

Z 7625 F

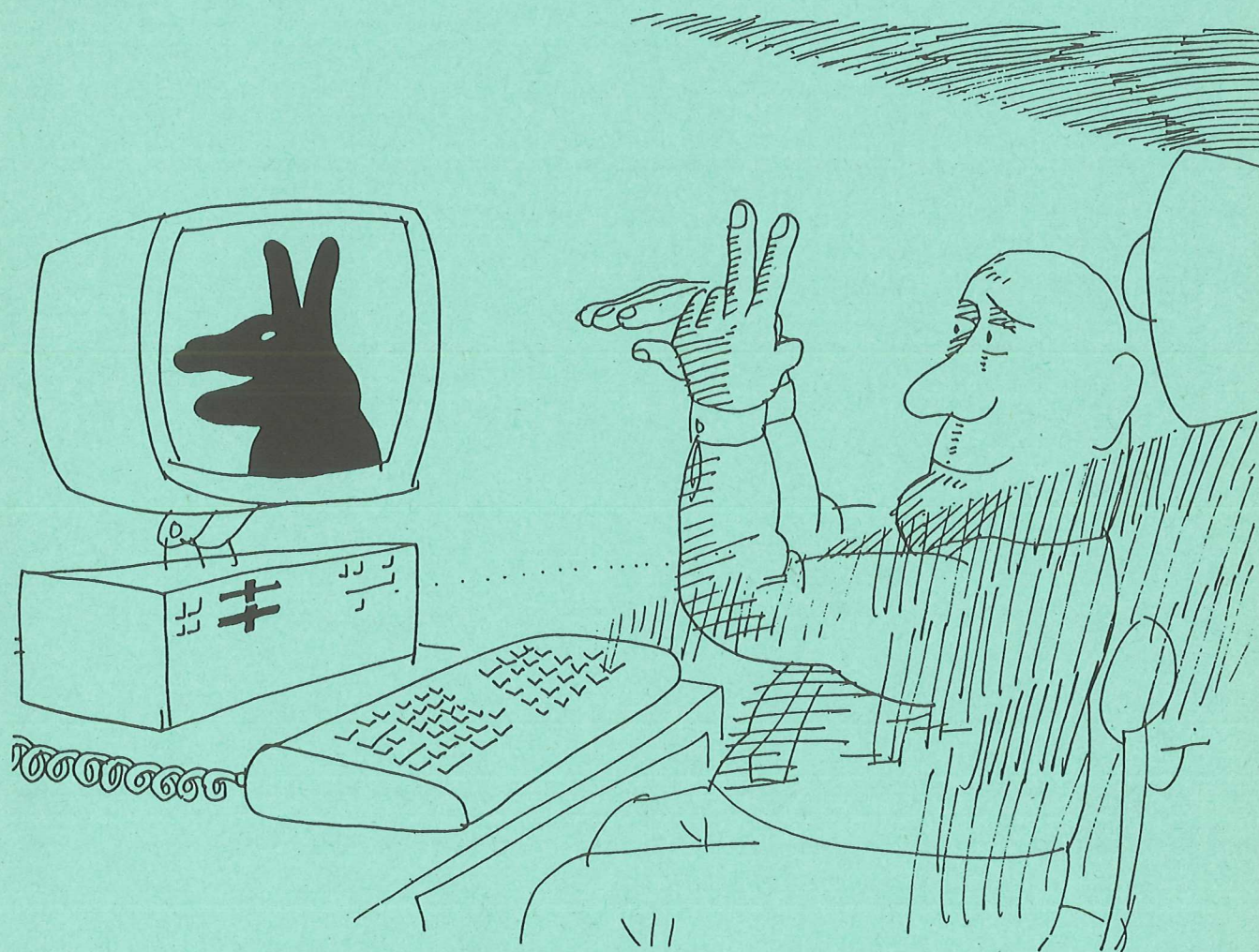
K O M M U N I K A T I O N

Forum InformatikerInnen
für Frieden und
gesellschaftliche
Verantwortung e.V.

7. Jahrgang
April 1990

Heft 2/90

Einzelpreis: 3.-- DM



(Jan Tomaschoff)

Thema: Datenschutz in der EG

Denkzeug Computer

JESSI im Kontext

Wie ein Geheimdienst zur obersten Bundesbehörde für Computersicherheit gemacht wird

Zum "Zukunftskonzept Informationstechnik"

INHALT

Nachruf auf Reinhold Franck	3
EDITORIAL	4
FORUM	5
AKTUELL	
• Die Aufrüstung geht weiter	8
• REFORGER als Simulation	9
• PSV abgerüstet?	9
• Softwarefehler läßt AT&T Telefonnetz zusammenbrechen	10
• Wählscheibentelefone stören ISDN	10
• Netzwerk Friedenskooperative	11
F!FF e.V.	
• Von der Klausurtagung des F!FF-Vorstands	11
MEDIENSPIEGEL	13
• Aberwitziger Wettlauf	13
Datenschutz in der EG: Grenzenlose Kontrolle	14
Vom Schlagbaum zum Datenverbund	17
Denkzeug Computer	21
JESSI im Kontext	25
Wie ein Geheimdienst zur obersten Bundesbehörde für Computersicherheit gemacht wird	29
Zum "Zukunftskonzept Informationstechnik"	36
F!FF ÜBERALL	44
LESEN?	
• DFKI - Gegensätzliche Interessen an der KI	46
TERMINE	48
VIELZWECKSCHNIPSEL	49
IMPRESSUM	50
ADRESSEN	51
SCHLUSS-PF!FF	
• Vom Fischernetz zum neuronalen Netz!	52

Nachruf auf Reinhold Franck

Reinhold Franck ist am 11. März 1990 bei einem Bergunfall in der Schweiz ums Leben gekommen. Er starb weit weg, hoch in den Bergen und war vielen Menschen sehr nah. Er wurde knapp 44 Jahre alt.

Reinhold Franck gehörte zur Generation jener Mathematiker, die als junge Assistenten wichtigen Anteil an der Formung der Informatik als Fachdisziplin hatten und die für einen neuen Begriff von Wissenschaft standen und daraus praktische Konsequenzen zogen. Für ihn war klar, daß Informatik keine "wertneutrale" Angelegenheit ist, bei der es lediglich um "wahr" oder "falsch" geht. Nicht im philosophischen oder soziologischen Seminar, sondern in der harten, drängenden Auseinandersetzung eines neuen Studienganges am Ausgang der sechziger Jahre konnte er jene Position erringen. Er ist ihr treu geblieben und hat sie entfaltet, als er industriell Software entwickelte, als er Professor wurde, als er den Vorsitz des FIFF übernahm.

Seit 1986 war Reinhold Franck im Vorstand des FIFF, zu dessen Gründungsmitgliedern er gehörte. 1987 wurde er zum Vorsitzenden gewählt. Im vergangenen Jahr begann er eine zweite Wahlperiode.

Innerhalb des FIFF steht Reinhold Franck für eine Phase der Konsolidierung nach teilweise euphorischem Beginn. Diese Phase ist intern geprägt durch die Hinwendung zu Fragen der Vernetzung weiterer Bereiche der Gesellschaft. Das FIFF hat sich damit einer Herausforderung gestellt, bei der die gesellschaftlichen Widersprüche sich komplexer schneiden als bei der militärischen Aufrüstung. In beiden Feldern hat Reinhold Franck Position bezogen. Tief von der Notwendigkeit radikaler Abrüstungsmaßnahmen überzeugt, hat er von Anfang an zu jenen Informatikern gehört, die warnend auf eine Beteiligung ihrer Disziplin beim Auftürmen unvorstellbarer Vernichtungsmittel und -strategien hingewiesen

haben. Es war ihm ein persönliches Anliegen, daß das FIFF sich auch weiterhin der militärischen Frage annimmt, weil sonst kaum jemand mehr dieses Thema behandelt. Als Verfechter breiter Demokratie, hat er nach Möglichkeiten gesucht, wie diese durch das technische Hilfsmittel der Netze unterstützt werden könnte.

Reinhold Franck hatte sein Mathematik-Studium an der freien Universität Berlin 1971 mit dem Diplom abgeschlossen. Schon in seiner Diplom-Arbeit wandte er sich Fragen der formalen Sprachen zu, einem Gebiet, das nun zum theoretischen Fundament der Informatik zählt. Von 1971 bis 1977 war er in der Informatik an der TU Berlin tätig. Dort gehörte er zu jenen, die das Curriculum der Informatik neu faßten und eine Prüfungsordnung ausarbeiteten, die in etlichen Teilen Beispielcharakter gewann. Sie war der politischen Seite nicht genehm, mußte jedoch alternativ zu einer konservativen genehmigt werden.

Im Jahr 1975 promovierte Reinhold Franck mit einer Arbeit über eine Klasse kontextfreier Graph-Grammatiken. Sie bildeten die Grundlage für eine Reihe von Veröffentlichungen (teilweise zusammen mit E. Denert und W. Streng) über zweidimensionale Programmiersprachen.

1977 ging Reinhold Franck in die "Praxis" der Software-Entwicklung und arbeitete sechs Jahre lang bei Softlab in München. Er war während dieser Zeit insbesondere im Großprojekt START - einem Buchungssystem für Reisebüros - tätig und leitete ein Projekt im Bereich der Rechnerkommunikation. Hatten die Programmiersprachen ihn zur Software-Technologie geführt, so diese nun zu seinem dritten fachlichen Schwerpunkt, den Rechnernetzen und der Datenkommunikation.

Nachdem Reinhold Franck 1978 von der TU Berlin die Lehrbefähigung erhalten hatte, kam er 1983 an die Universität Bremen als Professor für "Programmierung und Software-Engineering". Fragen der Validierung von Software durch Testen und der Rechnernetze prägten hier sieben Jahre lang seine fachliche Tätigkeit. Er hatte eine Gruppe von sieben WissenschaftlerInnen um

sich geschart, die von der Universität Bremen, der DFG und ESPRIT finanziert wurden.

Reinhold Franck gehörte zu jenen akademischen Lehrern, die ihre Studierenden ernst nehmen. Er hat mehrfach Lehrveranstaltungen neu konzipiert. Reformen in Lehre und Prüfung war er stets aufgeschlossen. In Bremen war er einer der wichtigen Träger des Projektstudiums. Wie in all seinen Arbeiten zeichnete er sich auch in der Lehre durch Genauigkeit, Sorgfalt und Übersichtlichkeit aus. Das Spontane und Assoziative waren weniger seine Haltungen als das Planvolle und Abgeleitete. Er liebte die abgerundete und klare Darstellung mehr als eine provozierende oder über-raschende, selbst wenn dieses Verlangen eine gewisse Sprödigkeit des Vortrages erzwang. Pathos lag ihm fern. Er zog die sachliche, aus kritischer Reflexion kommende Auseinandersetzung vor. Oft schien er dabei von inneren Zweifeln und Unzufriedenheiten über halsstarrige Positionen geplagt zu werden. Reinhold Franck zählte zu jenen, die einsprangen, wenn eine Aufgabe unbedingt zu erledigen war, auch dann wenn es über seine Kräfte ging. Hier, wie bei allem, was er anpackte, war er ein unerbittlicher Arbeiter. Seinen MitarbeiterInnen begegnete er lachend, freundschaftlich, kritisch und anregend. Sie wußten, daß er von Ihnen etwas verlangen konnte, weil er von sich selbst viel verlangte.

Obwohl sein Herz für die Lehre und die Hochschule schlug, hat Reinhold Franck sich der Industrie nicht versperrt. Auch nach seiner Rückkehr in die Hochschule hat er Fortbildungskurse für die Industrie durchgeführt. Er war Mitglied und Vorsitzender des Betriebsrates bei Softlab. Den Rektor der Universität Bremen hat er in den letzten Jahren hinsichtlich EDV-Ausbau beraten. In diesen Tagen sollte er zum Rechner-Beauftragten des Akademischen Senats gewählt werden. Das Konzept des campusweiten Netzes stammt von ihm. Lange Zeit war er verantwortlich für Beschaffung und Betrieb der Rechner im Studiengang Informatik.

Innerhalb der GI hat Reinhold Franck in den Programm-Ausschüssen mehrerer Tagungen mitgewirkt.

Er ist Mitverfasser von Empfehlungen für ein Industrie-Praktikum innerhalb des Informatik-Studiums. Zuletzt war er Sprecher der Fachgruppe Software-Engineering.

Neben vielen Beiträgen für Zeitschriften, Tagungsbände und Technische Berichte hat Reinhold Franck zwei Bücher geschrieben. Das 1977 erschienene "Datenstrukturen" (zusammen mit Ernst Denert) ging aus einer Lehrveranstaltung hervor. Es war ein Novum und eine Besonderheit im deutschsprachigen Raum, insofern es Algol68 und Lisp als Programmiersprachen stützte.

In einer für Praktiker bedeutsamen Reihe legte er 1986 das Buch "Datenkommunikation und Rechnernetze" vor. Es ist ein Musterbeispiel für die Genauigkeit und Übersichtlichkeit, mit der Reinhold Franck ein Thema behandelte.

Geist und Körper, Wille und Tat waren für Reinhold Franck nicht zu trennen. Seine Liebe zum Bergsteigen, zu seiner Familie sind Ausdruck davon. Er wurde aus einer Fülle sich entfaltender Arbeiten herausgerissen. Reinhold Franck hat Verantwortung und Verantwortlichkeit ernst und wahr genommen, er hat sie gelebt. Er wird uns an vielen Stellen fehlen.

(Frieder Nake)

EDITORIAL

Auch der Bundesregierung scheint langsam zu dämmern, wie verletzlich der gesamte Bereich der Informationstechnik ist und wie abhängig ein moderner Staat von dieser ist. Deshalb wurden flugs Fakten geschaffen mit der Einrichtung des 'Interministeriellen Ausschusses für die Sicherheit in der Informationstechnik' (ISIT) und der Erweiterung des Aufgabenbereichs der Zentralstelle für das Chiffrierwesen (ZfCh) um das Gebiet Computersicherheit. Folgerichtig wurde diese dann umbenannt in 'Zentralstelle für Sicherheit in der Informationstechnik' (ZSI). Die ZSI soll nun durch Gesetz in den Rang einer Bundesbehörde erhoben werden. (Die FIF KOMMUNIKATION berichtete in ihrer letzten Ausgabe ausführlich über die einschlägigen Pläne der Bundesregierung.)

Durch Hintergrund-Papiere Beteiligter für die Wissenschafts-Pressekonferenz anlässlich einer Anhörung zu dem entsprechenden Gesetzentwurf werden die geäußerten Befürchtungen bestärkt:

Nach Aussagen des Referatsleiters "Informationstechnik" beim Bundesbeauftragten für Datenschutz gegenüber der Wissenschafts-Pressekonferenz hat der Leiter der früheren ZfCh, und jetzige Leiter der ZSI, Dr. Otto Leiberich, damals in einem Gespräch mit dem Bundesbeauftragten für Datenschutz erklärt, er halte es nicht für sinnvoll, eine zu schaffende Instanz für Sicherheit in der Informationstechnik einem Ministerium zu unterstellen. "Die dazu notwendige Unabhängigkeit von ministeriellen Weisungen verträgt sich nicht mit den Aufgaben, die einer solchen Stelle gestellt werden müssen."

Wie bekannt, soll das zu errichtende Bundesamt für Sicherheit in der Informationstechnik (BSI) nun dem Bundesministerium des Inneren unterstellt werden.

Herr Dr. Leiberich hat sich wohl damit abgefunden, eine Bundesbehörde im Spannungsfeld zwischen Geheimdiensten und Wirtschaft zu leiten. Vielleicht macht gerade die-

ses Spannungsfeld den Reiz seiner neuen Aufgabe aus.

Seine Aussagen gegenüber der Wissenschafts-Pressekonferenz lassen an Deutlichkeit nichts zu wünschen übrig: Die ZSI hat "die möglichen Bedrohungen und Sicherheitslücken zu ermitteln und aufzudecken - bis hin zur Skizzierung von theoretischen Angriffsmodellen. Hierauf basierend hat sie Abwehrverfahren zu entwickeln bis hin zu arbeitsfähigen Programmen und Hardware-Komponenten." Analoges gilt für den Bereich der Fernmeldesicherheit: "Die ZSI hat Chiffrierverfahren und -geräte mathematisch und technisch zu entwickeln und die Verantwortung für die Sicherheit zu tragen. Die ZSI führt nur die Grundentwicklung durch, Produktion und Verkauf erfolgen durch die Industrie. Die ZSI hat Maßnahmen gegen die sog. bloßstellende elektromagnetische und akustische Abstrahlung von Klartext führenden Geräten zu ergreifen. Die ZSI arbeitet auf beiden Gebieten mit den Schwesterbehörden der befreundeten Länder zusammen." Für den Fall, daß die Industrie das Angebot immer noch nicht begriffen haben sollte, erinnert er daran, daß das von der ZSI entwickelte Telefon-Verschlüsselungsgerät soeben zum NATO-Standard-Gerät gekürt wurde.

Auch die sicheren Dienste werden an dem neuen Bundesamt ihre Freude haben: "Im Behördenbereich ist der ZSI eine Steuerungsaufgabe eingeräumt. ... darf eine Behörde nur solche Geräte beschaffen und einführen, die von der ZSI zugelassen sind" und nach ZSI-Entwicklungen von der Industrie produziert werden. Wenn man die Ausstrahlung von Anforderungen staatlicher Stellen und des entsprechenden Angebotes in Rechnung stellt, kann man davon ausgehen, daß in nicht allzu ferner Zukunft alle Daten nach Verfahren verschlüsselt werden, mit denen sich das zukünftige Bundesamt genau auskennt. Und das nicht nur bundesweit, denn: "Die Kenntnis von Abwehrmaßnahmen gegen

Computer- und IT-Kriminalität und -Spionage setzt die genaue Kenntnis der Angriffsverfahren voraus. Nur eine Behörde gelangt durch Zusammenarbeit mit den Ermittlungs- und Sicherheitsbehörden des eigenen Landes und mit den Schwesterbehörden befreundeter Länder an die notwendigen Informationen." Die Europäische Integration muß auf allen Ebenen erfolgen.

Die Errichtung einer solchen zentralen Bundesbehörde bedarf aus seiner Sicht keiner Rechtfertigung: "Die Frage ist auch nicht, ob eine solche Behörde notwendig ist, denn sie ist für die Belange des Staates bereits da, kein moderner Staat kann auf eine Fernmelde- und Computer-Sicherheitsbehörde verzichten. Die Frage ist vielmehr, ob die ZSI ihre Erkenntnisse und Möglichkeiten auch für die Wirtschaft nutzbar machen soll."

Ein Eindruck von Nachdenklichkeit könnte aufkommen bei seinen Schlußbemerkungen zur Zukunft der IT. Es lohnt jedoch, sie in voller Schönheit zu zitieren: "Die vergangenen Jahre waren durch ein unvorstellbares Wachstum der EDV-Möglichkeiten gekennzeichnet. Arbeitsprozesse, die man vor wenigen Jahren noch für unmöglich gehalten hat, sind heute Realität: Computerverbund und Datenfernverarbeitung, die Nutzung entfernter Datenbanken, Informationssammlungen und Computerkapazitäten, und wir sind vom Funktionieren dieses Systems in gefährlicher Weise abhängig. Denn: Sicherheitseinrichtungen sind bisher sträflich vernachlässigt worden. Unsere Systeme öffnen hochspezialisierten Datenspionen, Datenfälschern und -Erpressern Tür und Tor. Es ist ein Wunder, daß bisher nicht mehr passiert ist, und es ist m.E. nur eine Frage der Zeit, bis eine Welle der Computerkriminalität über uns hereinbrechen wird. "Das klingt schon fast wie Herr Herold, erinnern Sie sich?

Und weiter: "Noch gefährdeter sind unsere Fernmeldeverkehre. Z.Zt. wird zum Beispiel der gesamte kommerzielle Fernmeldeverkehr - auch über weite Strecken - unverschlüsselt abgewickelt. Industriespionage-Organisationen finden offene Türen zur Erlangung wichtiger Informationen im Konkurrenz-

kampf um Märkte und Produkte." Vollends klar wird sein Standpunkt am Ende seiner Ausführungen: "Gelingt es nicht, die Gefahren für die Sicherheit in der Informationstechnik in Grenzen zu halten, so werden wir für diese Akzeptanz-Probleme bekommen, wie sie heute für die Atom-Technik bestehen."

In dem vorliegenden Hintergrundpapier der Wissenschafts-Pressekonferenz von Herrn Dr. Leiberich kommen die Begriffe 'Wirtschaft', 'wirtschaftlich' und 'Industrie' auf fünf maschinengeschriebenen Seiten insgesamt zwölf mal vor. Die Staatsbürgerin und der Staatsbürger werden nicht einmal erwähnt.

Demokratie lebt von der offenen, kontroversen, politischen Diskussion. Wenn die Bundesregierung ihre Bringschuld der Öffentlichkeit gegenüber nicht erfüllt, damit auch andere Meinungen zu Gehör kommen, ist es die Verantwortung einer jeden mündigen Bürgerin und eines jeden mündigen Bürgers, sich selbst zu informieren. 'Forum' zu sein für diese Diskussion ist der Anspruch des FIFF, tragen wir dazu bei, ihn einzulösen.

(Hellmut Weber)

FORUM

(Angeregt durch die Thesen 'Quo vadis FIFF?' von Eberhard Barth in der FIFF KOMMUNIKATION 2/90 stellen Ditz Schroer und Heidelotte Craubner Folgendes zur Diskussion)

Gesunder Widerstand ist Leben, Leben ist Widerstand

Wir haben Gedanken aus zahlreichen Diskussionen und Gespräche mit FIFFerlingen, FreundInnen und KollegInnen zur anstehenden Selbstverständnisdiskussion im FIFF zusammengeführt. Zur Formulierung unserer Gedanken in konkrete Aussagen und inhaltlichen Erweiterung haben wir Literatur herangezogen, die in unserer Selbstverständnisdiskussion von Wichtigkeit ist. Um ein flüssiges Lesen zu ermöglichen verzichten wir auf einen Quellennachweis im Text. Die Zusammenfassung basiert im wesentlichen auf folgenden Quellen:

Thea Bauriedl: Das Leben riskieren. Psychoanalytische Perspektiven des politischen Widerstands. Pieper Verlag, 3-492-03204-4, 1988.

Das Ende der Geduld. Eine Diskussionsschrift bezogen auf - Die Zeit drängt C.F. von Weizsäcker. Hanser Verlag, 3-446-15015-3, 1987.

Horst E. Richter: Der Gotteskomplex und Leben statt Machen. Rowohlt Verlag, 3-498-05687-5, 1979.

Joseph Weizenbaum: Kurs auf den Eisberg. Pendo Verlag, 3-858-42087-5, 1984.

Günther Anders: Die Antiquiertheit des Menschen.

Zweiter Band: Über die Zerstörung des Lebens im Zeitalter der dritten industriellen Revolution. C. H. Beck Verlag, 3-406-07552-5, 1981.

In unserer Selbstverständnisdiskussion, dem sogenannten "Neuen Denken" im FIFF, geht es bei uns um Offenheit, um den täglichen persönlichen Mut, nicht stumm in einem Trend oder in einem Lager mitzuschwimmen, dessen Widersprüchlichkeit und oft Gewalttätigkeit (Arbeitsbedingungen, falsche fachliche Schwerpunkte usw.) wir erkannt haben oder erkennen können.

Durch unsere Technik sind wir in die Situation geraten, in der wir uns die Konsequenzen ihrer Anwendung nicht mehr vorstellen können.

Diejenigen, die die Folgen und die Verantwortung zu dieser Entwicklung tragen, müssen sich an den politischen Entscheidungen maßgeblich beteiligen. Das bewirkt zunächst Verunsicherung und Angst, da die Möglichkeit, sich an bisher bekannten Normen zu orientieren, abnimmt. Wenn wir erleben, daß wir selbst verantwortlich sind für alles, was wir tun, und auch für alles, was wir unterlassen, dann wünschen wir uns manchmal die Zeit zurück, in der wir dachten, unschuldig bleiben zu können, wenn wir nur gehorsam sind. Wir wünschen uns FührerInnen (FIFF-Vorstände), die uns sagen, was wir tun sollen, und die uns Rezepte dafür anbieten, wie das zu erreichen ist, was wir erreichen wollen.

Schon als kleine Kinder lernen wir, aufkommende Angst durch die Suche nach einem Schuldigen zu verdrängen. Wir schützen uns vor dem Überwältigtwerden durch unsere Gefühle, indem wir uns selbst oder andere beschuldigen oder entschuldigen. Wenn wir Angst bekommen, tendieren wir dazu, den Konsens mit dem Freund und der Freundin und den Dissens mit dem Feind zu suchen.

Wir lassen Zweifel nur noch uns selbst gegenüber zu. Wenn wir etwas nicht verstehen, oder gutheißen können, dann halten wir uns für dumm; wenn wir zögern, dann halten wir uns für träge. Autoritäre Behauptungen anzuzweifeln, Fragen zu stellen, sich nicht anzupassen, öffentliche Kritik und Auflehnung erfordern mehr Energie, Erfahrung und Zivilcourage, als die meisten von uns haben; und dies um so mehr, wenn sich die "anderen" auch anpassen und ebenso verhalten. Wir fürchten, das, was wir haben, zu verlieren, wenn wir die Mächtigen reizen. Der Störer/die Störerin zu sein, Widerstand zu leisten und nachdrücklich Fragen zu stellen ist oft schwer und macht Angst. Statt dessen halten wir lieber still und kooperieren, genauer gesagt: wir gehorchen.

Oder aber wir zeigen in dieser Situation zivilen Mut, d.h. wir verlassen die eigenen "Schlachtreihen", wir wagen es, unterschiedliche Gefühle und Überzeugungen gegenüber den Mitgliedern der eigenen Gruppe

(FIFF e.V. oder als Gesellschaft mit beschränkter Haftung FIFF GmbH & Co. KG.?) bei uns zu entdecken, was oft bedeutet, daß wir in bestimmten Punkten Ähnlichkeiten mit den Gefühlen und Überzeugungen der "anderen" bei uns bemerken.

Beobachtungen zeigen, daß die wirkliche Veränderung vom Widerstand in den eigenen Reihen ausgeht, daß sie nicht auf dem Kampf gegen die "anderen" beruht. Dies führt in eine ständige Konfliktsituation, die besonders dann ängstigend ist, wenn wir es nicht gewöhnt sind, uns in einem konflikthaften Spannungsfeld aufzuhalten. Aber die Größe der Angst hängt nicht nur von einem selbst und der eigenen Geschichte ab, sondern auch von dem Umfeld (am Arbeitsplatz, der Partnerbeziehung), indem wir uns bewegen.

Ziviler Mut wird von den "andern" oft mit zivilem Ungehorsam gleichgesetzt. Der zivile Ungehorsam hat aber sehr viel mehr Facetten, als im allgemeinen berücksichtigt werden, wenn dieses Schlagwort in fachliche



(Gerd Glück, Quelle: Cartoon-Caricature-Contor)

und politische Auseinandersetzungen gebracht wird. Ziviler Ungehorsam nach dieser weiten Sicht ist es, sich immer wieder die Frage zu stellen, ob die "Sachzwänge", in denen wir uns befinden, tatsächlich so bindend sind, wie sie zu sein scheinen.

Das Gefühl "ich muß ja, weil..." deutet oft Stellen an, an denen wir beginnen, uns nicht mehr nach den eignen Gefühlen und Wünschen zu richten, und statt dessen eine Begründung für ein der eigenen Person und der eigenen Verantwortlichkeit entfremdetes Verhalten suchen. Dagegen steht, daß ziviler Ungehorsam schon seit Jahrtausenden zu dem Stoff gehört, aus dem die Sternstunden unserer Geschichte gemacht sind.

Der Aufenthalt in einem solchen spannungsreichen Konfliktfeld von gelebtem zivilen Mut, hat allerdings auch eine angenehme Seite. Nur diese Seite kann einen FIFFerling dazu bewegen, dem jeweiligen Konflikt nicht auszuweichen. Wir können in dieser Situation das Gefühl haben, lebendig (pFIFFig) zu sein, uns verändern zu können, indem wir uns selbst und damit auch die "anderen" nicht verlassen.

Die Veränderung der Umwelt durch Lebendigkeit hängt von dem Grad ab, in dem wir in uns Lebendigkeit zulassen. Sobald wir die Umwelt verändern wollen, ohne uns selbst zu verändern, delegieren wir die Veränderung, die wir selbst nicht wagen, an andere und tragen so zur Entstehung und Aufrechterhaltung linearer, maschineller Beziehungsstrukturen bei.

Die Realität sieht folgendermaßen aus:

Zwischen denen, die heute schon "Auf neue Weise.... Dinge von morgen leben" und denen, die auf dem Weg dorthin weiter nach den herkömmlichen Vorstellungen leben, gehört es zum Charakter der Geschichte (der FIFF-Geschichte), daß auf dem Weg zu den Regeln von morgen zuerst immer noch die von gestern gelten, trotzdem aber einige vorangehen müssen.

Ein lebendiger Mensch, sprich FIFFerling, ist fähig, Freude und Leid, Genußmöglichkeiten und Bedrohung zu erleben, die in seiner und für seine Gemeinschaft entste-

hen. Er fühlt sich mitbetroffen von allem, was die Gemeinschaft betrifft. Er/Sie erlebt sich weder außerhalb der Gemeinschaft (d.h. darüber, darunter oder abseits stehend), noch identifiziert er/sie sich mit dem Ganzen der Gemeinschaft.

Gesunder Widerstand ist Leben, Leben ist Widerstand!

Das Ziel des FIFF:

Die systemverändernde Funktion unseres zivilen Mutes besteht darin, standzuhalten, Gefühle und damit unsere Verunsicherung und unsere Angst wahrzunehmen.

Jeder Versuch, durch Verdrängung von Angst und Gefahr, eine künstliche Lebendigkeit (heutiger FIFF-Zustand?) zu erzeugen, bringt eine psychische Totenstarre bei lebendigem Leibe mit sich und macht es dem derart lebendigen FIFFerling unmöglich, sich für sein Leben und für das seiner Nachkommen einzusetzen. Andererseits können wir besser mit unserem Leben umgehen, wenn wir es wagen, die Angst und auch die Lust zu erleben, die zu diesem Leben, (FIFF-Leben) gehören.

Für jeden von uns stellt sich im Moment die Frage, ob wir mit der scheinbaren Sicherheit und Zufriedenheit durch die "Beton-Informatik" leben oder ob wir uns auf die Unsicherheit und Lebendigkeit des "Grases" (FIFF-Mitgliedschaft) verlassen wollen, das immer noch, wenn auch sehr kümmerlich (Anzahl der FIFFerlinge bezogen auf die arbeitenden InformatikerInnen), unter dem Beton lebt.

Wir haben uns so sehr an die Sicherheit durch Beton gewöhnt, daß wir unsere Unzufriedenheit mit dem Beton vor allem in unseren sozialen Beziehungen nur sehr langsam entdecken. Zudem ist die Angst vor dem Verlust der Betonsicherheit so groß, daß wir uns im Konfliktfall doch lieber schnell wieder einbetonieren und es nicht riskieren, als Gras - unter den harten Schritten der "anderen" - zu leiden.

Ein ersten Schritt aus diesem Kreislauf auszusteigen kann nur die Aufgabe der Illusion sein, auf ein Ziel hinzuleben, eine Leistung zu erbringen, einen besseren Zustand herstellen zu müssen.

Ein Widerspruch?

Wenn wir uns nicht ständig bessere Sollzustände in der Informatik vorstellen, die wir erreichen oder herstellen müssen, dann merken wir, daß wir jetzt leben und weitergehende Bedürfnisse haben. Wenn wir diese Leistungsorientierung mit ihren vielfältigen Implikationen fallen lassen, riskieren wir das Bewußtsein und damit die Erkenntnis, daß wir uns in einem ständigen Veränderungsprozeß befinden. Und wir gewinnen dabei auch die Sicht auf die vielen kleinen Veränderungsschritte, die in jedem Moment möglich sind. Wir sehen die Möglichkeit, Schritte, die wir gestern nicht getan haben, heute zu tun.

Die Zeit drängt - Nehmen wir uns unsere Zeit!

Wir als FIFF-MitgliederInnen müssen heute zur Geduld aufrufen, zur Geduld der Vernunft in unserem Handeln und in unserer Politik. Die Summe der Themen, die jetzt in intellektueller Genauigkeit und gefühlsmäßiger Offenheit in Sachkunde und in der Mühsal der Details erarbeitet werden müssen, steht im Widerspruch zur Atemlosigkeit des Drängens der kurzen Fristen (millionstel Sekunden Zugriffs- und Verarbeitungszeit).

Wenn wir uns selbst verstehen als Menschen, die sich in einem ständigen Prozeß befinden, jederzeit abhängig von Prozessen und Situationen unserer Umwelt und jederzeit beteiligt an allen Veränderungen und Nichtveränderungen in dieser Welt, dann nehmen in gleichem Maße unsere irrationalen Größenphantasien ab und auch unsere ebenso irrationalen Ohnmachtsphantasien.

In diesem Augenblick sehen wir dann nicht nur den Punkt, an dem wir stehen, und nicht nur das Ziel, auf das wir zustreben, wir sehen den Weg, den wir in unserem Leben zurücklegen, den Ablauf unseres FIFF-Lebens.

(Ditz Schroer und Heidelotte Craubner, Seefeld-Meiling)

AKTUELL

Die Aufrüstung geht weiter

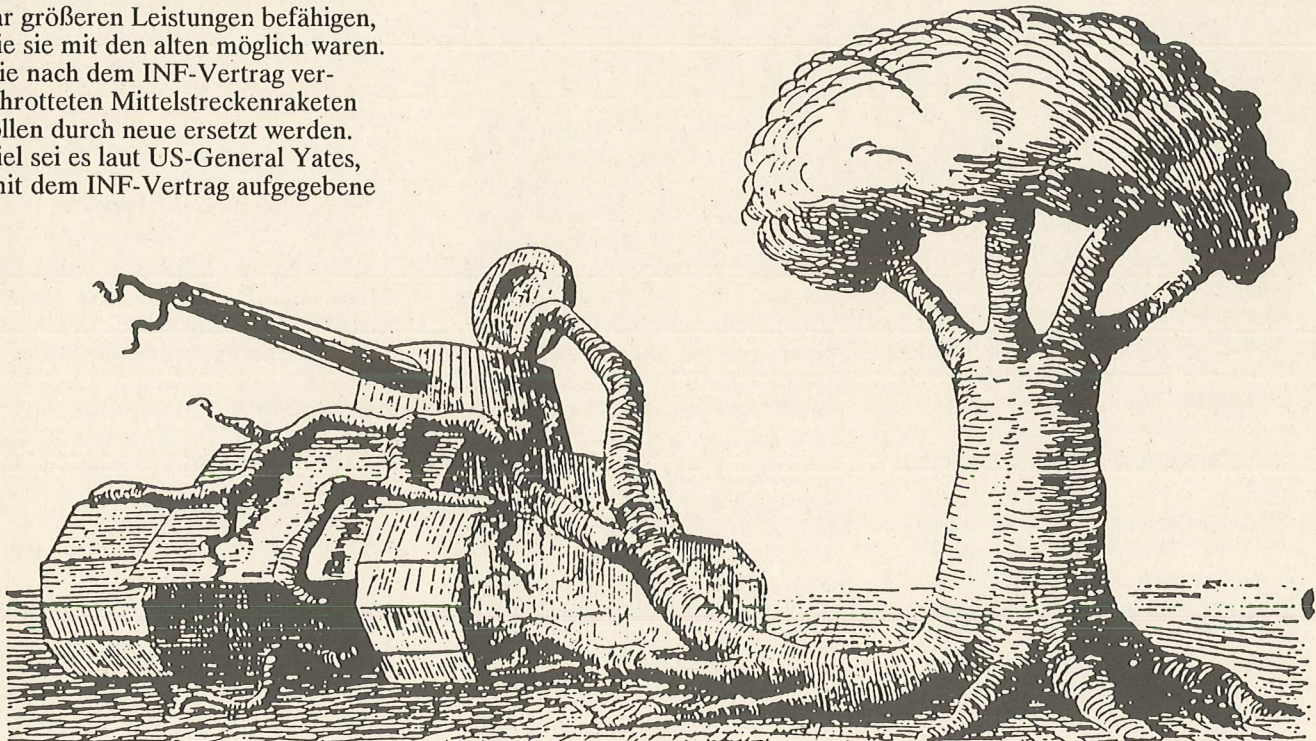
Die vielzitierten "Veränderungen im Osten Europas" haben auch für unsere Streitkräfte die Sinn- und Existenzfrage aufgeworfen. Während die Bundeswehr in dieser Phase allzu laute Querdenker wie Elmar Schmähling schnell kaltstellt, ist in den USA schon eine Neuorientierung des Wehrauftrages zu beobachten: die Stärkung der Weltpolizistenrolle. Wehretatkürzungen werden daher nur mager ausfallen.

Starr wird dort auch an der Modernisierung von Waffensystemen festgehalten. Mehr Informationstechnik soll die an Zahl abnehmenden Waffen zu denselben oder gar größeren Leistungen befähigen, wie sie mit den alten möglich waren. Die nach dem INF-Vertrag verschrotteten Mittelstreckenraketen sollen durch neue ersetzt werden. Ziel sei es laut US-General Yates, "mit dem INF-Vertrag aufgegebene

militärische Fähigkeiten wiederherzustellen". Die Stationierung neuer Atomgranaten wurde wegen der Bundestagswahl im Dezember vom August auf den Januar 1991 verschoben. Diese Atomwaffen mit einer Reichweite von 30 bis 50 Kilometern sind zwar - getreu der sprachlich zwar unschönen, doch korrekten Devise "je kürzer die Reichweite, desto toter die Deutschen" - mit den neu erwachenden deutschen Interessen nicht vereinbar. Ein um so besseres politisches Druckmittel könnten sie aber darstellen.

Fast unbemerkt blieb der Ausbau der Kommunikations- und Informationsinfrastruktur der Streitkräfte, die bei der Planung von Militäraktionen eine weiter zunehmende Rolle spielt. Nach dem Überfall auf

Panama wurde bekannt, daß das US-Militär ein Expertensystem entwickelt, das die Vorbereitungszeit für Militäraktionen von eineinhalb bis zwei Wochen auf nur noch 48 Stunden senkt. Damit korrespondiert die geplante Aufstockung der schnellen Eingreifverbände. Die künstliche Intelligenz macht es also bald möglich, den "big stick" des Weltpolizisten USA - wie ihn die US-Medien nennen - nicht nur zu schwingen, sondern auch im Bedarfsfall niedersausen zu lassen. Das vom FIFF schon lange kritisierte "Worldwide Military Command and Control System" (WWMCCS) wird seinem Namen eben voll gerecht.



REFORGER als Simulation - ein politischer Erfolg

Das REFORGER-Manöver, mit dem die USA die Verlegung von Truppenverbänden über den Atlantik in die Bundesrepublik proben, fand dieses Jahr erstmals mit einer Verringerung der Manövertruppen um 40 Prozent statt. Grund dafür war nicht die Senkung der Manöverkosten oder die Rücksicht auf die Natur, sondern die derzeitige politische Lage. Die Diskussion um die Rechte der Besatzungsmächte - vom unkontrollierten Telefonabhören bis zum Verhängen der Todesstrafe durch Militärgerichte -, um Tiefflüge und um das Ende des Kalten Krieges nötigen den US-Truppen erstmals eine Rechtfertigung für ihr Verhalten und ihre Präsenz ab. Mit festem Blick auf die Bundestagswahlen im Dezember äußern sich Beamte aus der US-Administration, die Situation sei derart, "daß wir uns gerade jetzt keine Unfälle oder Zwischenfälle leisten können".

Unter politischen Druck geraten, gehen die Militärs in den Publicity-Untergrund, weg von der Straße und zurück auf ihr eigenes Gelände. Die einfachen Soldaten üben auf Truppenübungsplätzen, die Stabs-ebene taucht ab vor die Computerbildschirme der Feld-Simulations-Zentren (FSC). Die Befehle der Kommandeure gehen nicht mehr an die Truppe, sondern werden in das Computersystem eingegeben. Die Auswirkungen der Befehle werden errechnet und auf den Bildschirmen wieder ausgegeben. Dabei werden Treffergenauigkeit, Truppenstärke, Kampfgerät, Benzinvorrat usw. berücksichtigt. Der Zweck der Übung wird damit ebenso erfüllt, Stabsübungen als Computersimulation können sogar noch häufiger durchgeführt werden.

Hier werden die undemokratischen Potentiale des Computereinsatzes deutlich: Computersimulationen bieten die Möglichkeit, den Übungsstand der Truppe zu erhalten, das Militär aber aus der Öffent-

lichkeit fernzuhalten, statt öffentlicher Debatte nun eine weitere nichtöffentliche Dunkelzone aufzubauen. Wir werden diesen Rückzug des Militärs ins Nichtöffentliche und Geheime nicht hinnehmen, sondern - so gut dies möglich ist - auch über weitere Computer-Manöver eine Öffentlichkeit herstellen.

PSV abgerüstet?

Nach Angaben des Springer-Flaggschiffs "Die Welt" sollen unsere alten Bekannten von der Psychologischen Verteidigung (PSV) zu den ersten Truppenteilen gehören, die von der Abrüstung getroffen werden. Laut Welt vom 19. Januar 1990 soll die PSV ihre bisherigen Propagandaarbeiten in Friedenszeiten aufgeben und gegen den Feind nur noch im Verteidigungsfall tätig werden. Dazu soll die PSV dem Heer unterstellt und das Referat PSV im Verteidigungsministerium aufgelöst werden.

Auch die PSV-Akademie in Waldbröl soll einen neuen "Auftrag für Informationsarbeit in Fragen der Sicherheit und Verteidigung" erhalten. Militärische Führungskräfte sollen hier fortgebildet werden. Wie bisher sollen dort aber auch Presse- und PR-Offiziere aus- und weitergebildet sowie Treffen zwischen Militärs und "zivilen Multiplikatoren" abgehalten werden. In diesen Offizierslehrgängen wurde anhand des Wissens der PSV über die "Bestrebungen gegen den Verteidigungsauftrag der Streitkräfte", die Friedensgruppen also, gelehrt, sich der Argumente zu wehren; bei den Treffen mit Zivilisten wurde dies dann ausprobiert oder beraten, je nachdem, welcher Couleur diese Gäste waren. Wenn die PSV also auch weiterhin die Schmiede für zuverlässige Bundeswehrkader bleibt, so wird sie auch weiterhin Informationen über Friedensbewegte sammeln müssen. Ob sie dazu wieder neue Dateien anlegt, bleibt abzuwarten.

Wie in der letzten **FIFF** KOMMUNIKATION berichtet, hat die PSV wenigstens die vom Datenschutzbeauftragten beanstandeten Dateien

vernichtet und hat auch in der zur PSV gehörenden "Gesellschaft für Zeitprobleme e.V." keine Daten über uns gespeichert.

Damit es aber nicht den Anschein hat, die PSV wolle sich nun dem äußeren Feind ab- und ganz dem inneren zuwenden, soll Waldbröl zu einer Stätte der Begegnung von Militärs und Zivilisten aus den In- und Ausland werden. So können abrüstungsgestreßte Militärs international Erfahrungen austauschen aber auch ängstliche Ausländer von der Harmlosigkeit der Bundeswehr - oder wie der Name in einem zusammenwachsenden Deutschland dann sein wird - überzeugt werden.

So gesehen, reicht ja die Beobachtung von "Wehrunwilligen" und "Wehrindifferenten" aus dem Inland gar nicht aus. Vielmehr müßten jedem bundesdeutsche Militärattaché ein PSV-Attaché zur Seite gestellt werden, der Daten über Ausländer sammelt, die sich gegen ein militärisch zu starkes Deutschland aussprechen. Francois Mitterand, Margaret Thatcher und und...

Verfassungsschützer ...

... tauchen derzeit offenbar bei ausgewählten Net-UserInnen auf und stellen ihnen Fragen. Angesichts der von der Bundesregierung u.a. mit dem ZSI/BSI (siehe Artikel "Wie ein Geheimdienst zur obersten Bundesbehörde für Computersicherheit gemacht wird" in dieser **FIFF** KOMMUNIKATION) eröffneten Jagdsaison auf Computerspione und -saboteure würde es uns interessieren, ob die Besuche dieser Herren zufällig oder Vorboten einer intensiveren "Bearbeitung" der Computer-Szene sind. Wir, Ute und Ingo aus dem FIFF-Büro, möchten deshalb alle Betroffenen bitten, uns über derartige Besuche und ihre Erfahrungen nach Möglichkeit zu informieren.

Softwarefehler läßt AT&T Telefonnetz zu- sammenbrechen

Der mit 70% Marktanteil größte Telefonnetz-Anbieter der USA, AT&T dürfte den Januar 1990 noch lange in Erinnerung behalten. Ausgehend von einem New Yorker Telefon-Vermittlungsrechner, den eine noch unbekannte Kombination von Telefonaten fälschlicherweise in einen Überlastzustand versetzt hatten, breitete sich der Fehler schnell über weite Teile des aus 114 Knotenrechnern bestehenden Long-Distance-Netzes aus. Für neun Stunden meldete das AT&T-Telefonnetz den Ferngesprächskunden: "all circuits busy". Das AT&T-Telefonnetz mit dem Namen "Die richtige Wahl" entpuppte sich so als die falsche.

Grund dieses bisher größten Ausfalls eines solchen Netzes war ein Softwarefehler in einem neuen Programm zum effizientesten Routing der Anrufe. Nachdem AT&T sein System so umgestellt hatte, daß Anrufrufen auf einem vom Gespräch selbst getrennten Kanal weitergegeben werden - ob es ein ISDN-System ist, oder eine Abart, wird nicht genau klar - führte die notwendige Anpassung der Steuerungssoftware zu dem jetzt aufgetretenen Fehler.

Der Schaden für AT&T allein beläuft sich auf knapp 70 Mill. Dollar, der von Telefonkunden - Banken, Hotelketten, Fluggesellschaften - ist nicht abzuschätzen. Immerhin hat der Schaden in den USA ein wenig zum Nachdenken über Softwarefehler geführt. Vom Telefon abhängige Firmen schaffen sich einen Backup-Anschluß bei einer zweiten Telefongesellschaft an.

Der Zusammenbruch des AT&T-Telefonnetzes, das etwa in den Hearings zur (Un-) Sicherheit der SDI-Software als Musterbeispiel eines sicheren, komplexen Softwaresystems gepriesen wurde, hat die Korrektheit des nicht zuletzt vom FIFF immer wiederholten Satzes

"Jedes Computerprogramm ist fehlerhaft" nachdrücklich ins öffentliche Bewußtsein gebracht. So macht sich in den USA die Einsicht breit, daß ein Softwarefehler weit mehr Schaden anrichten kann, als Hacker oder Viren. Hacker und Viren treten zudem selten und meist in öffentlich zugänglichen Computernetzen auf und richten nicht notwendigerweise Schaden an. Softwarefehler aber gibt es in allem möglichen Programmen und in allen möglichen Sicherheitsbereichen. Gerade dort, wo Hacker nie hinkommen, warten Softwarefehler auf ihre Entdeckung. Diese Fehler zu entdecken und zu korrigieren, ist zu teuer. Wie gut, daß es da als Sündenböcke wenigstens die Hacker gibt.

Wählscheiben- telefone stören ISDN

Mit einer Sonderumtauschaktion will die Bundespost/Telekom endlich ihre Wählscheibentelefone aus dem Verkehr ziehen. Die alten Geräte sind deshalb innerhalb des im Aufbau befindlichen ISDN (Integrated Services Digital Network, oder neudeutsch: Integriertes Sprach- und Daten-Netz) störend, weil sie keine unmittelbar geeigneten Wählpulse an die ISDN-Vermittlungsstellen schicken können und so zusätzlichen Aufwand provozieren, den sich die Post gerne sparen möchte.

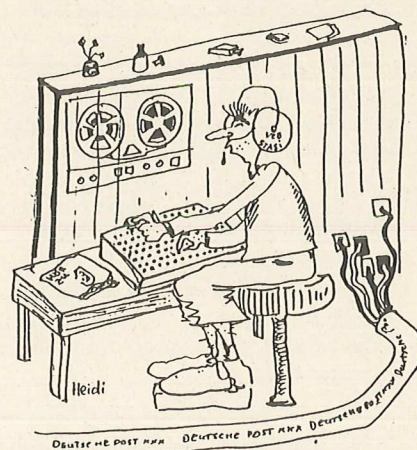
Bei der Aktion werden Wählscheibentelefone kostenlos gegen Tastatur-Telefone ausgetauscht. Seltsamerweise werden gerade jene besonders problematischen Wählscheibenapparate vom Umtausch ausgeschlossen, die im Gehäuse einen Gebührenzähler haben. Diese Apparate, noch häufig in WGs zu finden, haben die Eigenschaft, daß sie Wellen ("Kompromittierende Strahlung") aussenden, die mit einem Langwellen-Radio abgehört werden können. Das geht zum Beispiel durch Wände und Decken hindurch. Im 10. Bericht des Bundesbeauftragten für Datenschutz ist

zwar nur von 2 m Reichweite die Rede, mit entsprechend empfindlichen Empfängern dürften jedoch auch im weiteren Abstand die Telefongespräche abzuhören sein. Im Datenschutzbericht heißt es u.a.: "Die Deutsche Bundespost hat mir nach entsprechenden Untersuchungen diesen Sachverhalt bestätigt, einen generellen Austausch der Geräte jedoch abgelehnt."

Protestiert man/frau nun etwa beim Personal der "Telefonläden" gegen diese Praxis, so bekommt man zu hören, daß die erste Generation der Tastentelefone mit integriertem Zähler die gleiche Eigenschaft des "Langwellensenders" aufweist.

Trotzdem sollten Teilnehmer, die ihr Wählscheibentelefon mit Gebührenzähler gegen ein "abhörsicheres" ISDN-Tastentelefon austauschen lassen wollen, versuchen, diesen Austausch kostenlos vornehmen zu lassen.

(aus: Informationsdienst COMPUTER und MEDIEN 1/90, Herausgegeben von DIE GRÜNEN - Bundesarbeitsgemeinschaft Computer und Medien, siehe auch unter **LESEN** in dieser **FIFF** KOMMUNIKATION)



Heute horch ich
morgen schleich ich
übermorgen sitz ich am ISDN



Netzwerk Friedens- kooperative

Nach der Selbstauflösung des "Koordinierungsausschuß der Friedensbewegung" im Oktober 1989 hat sich ein neues Netzwerk konstituiert, das als erstes eine große Anzahl von Initiativen (mit der Bitte um Mitarbeit) angeschrieben. Dieses "Netzwerk Friedenskooperative - Förderverein Frieden e.V." arbeitet finanziell mit den JUSOs zusammen, so sind die Briefe auf deren Kosten verschickt worden. Zielsetzung ist "... als unabhängiger und überparteilicher Dachverband zur Verbreitung der Informationen und der Vernetzung der politischen Initiativen beizutragen"

Daß ein übergeordnetes bundesweites Organ der bundesrepublikanischen Friedensbewegung eine wichtige Funktion übernehmen könnte, ist offensichtlich, deshalb ist dieser Initiative viel Erfolg zu wünschen. Dieser Erfolg hängt natürlich davon ab, ob es gelingt, die mißliche Entwicklung des aufgelösten Koordinierungsausschusses zu vermeiden und ob sich das ganze Spektrum der Friedensbewegung darin wiederfindet.

Als Organ dient das Magazin "Friedensforum", das bei folgender Adresse bestellt werden kann:

Netzwerk Friedenskooperative
Förderverein Frieden e.V.
Römerstraße 88
5300 Bonn 1

FIFF e.V.

Von der Klausur- tagung des FIFF- Vorstands

Vom 25. bis 27. Februar 1990 hat sich der FIFF-Vorstand im Heinrich Fabri-Institut in Blaubeuren zu seiner diesjährigen Klausurtagung zusammengefunden. Geplante Programmpunkte waren

- Selbstverständnis von FIFF und Vorstand,
- Berichte und Organisatorisches,
- Vorstrukturierung der Jahrestagung
- Verantwortung und Ethik

Selbstverständnis von FIFF und Vorstand

In einem ersten Brainstorming sind folgende Gedanken zum Selbstverständnis von FIFF zusammengetragen worden: Gegenöffentlichkeit; FIFF-Ideen am Arbeits-

platz leben und weitergeben können; Widersprüchlichkeit unserer Arbeitssituation; Verständnis von Frieden; FIFF-spezifische Themen; Meinungsvielfalt; FIFF ist kein alternativer Arbeitgeber; "gleichgesinnt sein" als Basis; Netz von Gleichgesinnten; inhaltliche Anregungen an die Wissenschaft; Veränderung der Lebenssituation vom Studium zum Beruf; interessante Menschen; Katalysator; weg von Oberflächlichkeit.

Mehr die Arbeit des Vorstands betreffende Punkte waren: Mehr inhaltliche Arbeit; effektiver und professioneller; in der Öffentlichkeit Akzeptanz erreichen; Projekte, Stellen, Fördermittel; normales Leben widerspiegeln; Gefahr des "Abhebens"; Politik stellvertretend für andere machen; Organ zur Koordinierung der Arbeit, nicht Ideenfinder; Ideen aufnehmen und Anregungen geben; keine Vordenkertätigkeit, Struktur vermitteln; "gegenseitiges von-einander-wissen" organisieren; Menschen anregen, für eine gewisse Zeit (auch) etwas zu tun; Kommunikationszentrale Vorstand.

Helga berichtete in diesem Zusammenhang, daß im Bonner Büro durch die Arbeit von Ingo und Ute bereits einiges mehr an Professionalität eingezogen ist. Kritisiert wurde, daß der Beirat als Kontroll-



(Oswald Huber)

organ des Vorstands nicht funktioniert, da nicht regelmäßig Vertreter aus den Regionalgruppen zu den Sitzungen kommen. Die Beirats-tätigkeit beschränkt sich im wesentlichen auf einen Informationsaus-tausch.

Jahrestagung 1990

Einen breiten Raum während der Klausur nahm die Diskussion über die Gestaltung der nächsten Jahrestagung ein.

Der Vorschlag, Firmen anzusprechen, die die Jahrestagung sponsern, wurde im Vorstand kontrovers diskutiert. Dem Argument, daß es ein Erfolg für FIFF wäre, wenn sich Firmen bereit erklären, unsere Ideen zu unterstützen, stand die Meinung entgegen, daß wir uns auf keinen Fall von Sponsoren abhängig machen dürften. Als Konsens wurde beschlossen, daß die Vorbereitungsgruppe eine Liste von Firmen, die angeschrieben werden sollen, vorbereitet, die Thematik aber auf jeden Fall auch auf der Jahrestagung problematisiert werden muß.

Einige Vorschläge für das Thema der Jahrestagung wurden im weiteren intensiv diskutiert. Insbesondere wird, wie die bisherigen Reaktionen auf Beiträge in der letzten FIFF-Kommunikation gezeigt haben, von vielen FIFF-Mitgliedern eine Selbstverständnisdiskussion, d.h. eine Beschäftigung mit sich selbst, zum Teil vehement abgelehnt. Die Diskussion drehte sich im weiteren um das Problem, weshalb wir Berührungängste haben, über unsere Organisation zu reden. "Unser Problem ist die Organisation des FIFF." "Wenn die FIFF-Mitglieder sich nicht mit der Organisation auseinandersetzen wollen, dann wird FIFF im Sande verlaufen."

Die Diskussion über das Motto der Jahrestagung wurde schließlich mit folgendem Kompromiß abgeschlossen: "Wort und Tat - Jahrestagung der InformatikerInnen für Frieden und gesellschaftliche Verantwortung"

Für die Arbeitsgruppen wird eine interdisziplinäre Gestaltung durch die Regionalgruppen angestrebt. Dazu sollten bereits bestehende Kontakte zu befreundeten Gruppen ausgenutzt werden. Einige Themen-

vorschläge waren: Familie, Betrieb/Industrie, Parlament, Öffentlichkeit, Forschung, Ausbildung, soziale Bewegung, Solidaritätsfonds, FIFF-Kontakte in die DDR. Zur Erfassung von Themen formuliert die Vorbereitungsgruppe einen Fragebogen, der über das Büro an die Regionalgruppen verschickt werden soll. Befreundete Gruppen und relevante Vereinigungen sollen eingeladen werden, sich an der Gestaltung der Arbeitsgruppen zu beteiligen: Gewerkschaften, BdWI, Friedensinitiativen, GCN, Frauengruppen, IKÖ, AKWs und Müslis, DFG-VK, WSI, STEIG, IPF; IHK, GI, GI der DDR, Kirchen, VDI, ZVEI, IFIP.

Berichte und Organisatorisches

Auf eine Anzeigenaktion, die Ingo und Ute in der TAZ gestartet hatten, sind bisher etwa 50 Anfragen im Büro eingegangen, hauptsächlich von Leuten, die bereits im Berufsleben stehen.

Es wurde beschlossen, die Aufnahme von FIFF in die Liste der Verbände und Vereine beim Deutschen Bundestag zu beantragen. Dieses ist Voraussetzung z.B. für die Einladung zu Bundestagsanhörungen, begründet jedoch keinen rechtlichen Anspruch darauf.

Der derzeitige Mitgliederstand ist 910 ordentliche und 59 fördernde Mitglieder und 37 Abonnenten der FIFF KOMMUNIKATION. In der Zahl der Mitglieder sind 88 Nichtzahler enthalten, die bisher trotz Mahnung nicht bezahlt haben. Der Vorstand wird diese Mitglieder über das Büro anschreiben und ihnen eine Frist setzen, nach der die Mitgliedschaft erlischt, wenn bis dahin keine Reaktion erfolgt. Der Versand soll nach der nächsten Vorstandssitzung erfolgen.

Für den Reader der Jahrestagung 1989 in Frankfurt hat die Regionalgruppe Frankfurt eine ISBN beantragt und bekommen. Der Umschlagentwurf ist fertiggestellt. Das Buch wird voraussichtlich etwa 300 Seiten dick und im Offsetdruck von der Papiervorlage in Bonn erfolgen. Im Bonner Büro fehlen z. Zt. noch etwa 140 Seiten Druckvorlage.

Ralf berichtet über eine Initiative "Verpflichtungserklärung/Hilfsfonds

für Naturwissenschaftler". Mit Unterzeichnung der Verpflichtungserklärung treten Wissenschaftler einem Fonds bei, der bei beruflichen Schwierigkeiten finanzielle Unterstützung bietet. Gerhard bemerkt dazu, daß rechtliche Unterstützung und finanzielle Hilfe die ureigenste Aufgabe der Gewerkschaften ist. Die Verpflichtungserklärung der Naturwissenschaftler müsse also von den Gewerkschaften anerkannt und akzeptiert werden.

Weiter wurde diskutiert, daß die in der Erklärung enthaltene Einschränkung auf Wissenschaftler für FIFF-Mitglieder herausgenommen werden müsse, da im FIFF auch andere DV-Fachkräfte Mitglied sind. Für FIFF-Mitglieder müsse eine spezifische Erklärung evtl. basierend auf den von der UNESCO herausgegebenen "Rechten und Pflichten von Naturwissenschaftlern" formuliert werden. Es wurde beschlossen, daß die FIFF KOMMUNIKATION für die Verbreitung der Verpflichtungserklärung zur Verfügung gestellt werden sollte ebenso wie die nächste Jahrestagung. Das Thema soll bei der nächsten Vorstandssitzung noch einmal diskutiert werden.

(Hellmut Weber)

Aus dem Büro

Wir möchten alle Mitglieder und AbonnentInnen nochmals darauf hinweisen, daß Postvertriebsstücke wie die FIFF KOMMUNIKATION auch mit einem Nachsendeantrag von der Post nicht an die neue Adresse nachgesandt werden. Daher möchten wir Euch bitten, uns alle **Adressänderungen** rechtzeitig bekannt zu geben.

Und noch etwas: alle, die aus dem Büro für einen bestimmten Termin Materialien o.ä. haben möchten, möchten wir dringend bitten, die Postlaufzeiten zu berücksichtigen. Für Pakete und größere Sendungen heißt das, uns mindestens 14 Tage vorher bescheid zu geben, da wir sonst für nichts garantieren können.

Mit FIFFigen Grüßen
Ute und Ingo

MEDIEN- SPIEGEL

(Der folgende Artikel erschien in der ZEIT Nr. 6 vom 2. Februar 1990.)

Aberwitziger Wettlauf

Die Stärke der japanischen Unternehmen bei Microchips zwingt Siemens und IBM zur Kooperation

Noch ist nicht entschieden, wer am Ende den Weltmarkt beherrscht - Japan ist jedenfalls auf dem besten Wege dorthin. Zunächst geht es nur ums Geschäft mit den Microchips. Um im Rennen zu bleiben, schlossen Siemens und IBM jüngst einen transatlantischen Pakt. Gemeinsam wollen sie die übernächste Generation von Speicherchips entwickeln. Allein fühlen sich die beiden starken Weltkonzerne zu schwach.

Zwar ist der Wert der weltweit produzierten Chips im Vergleich zu allen anderen Gütern verschwindend gering, doch ihre Bedeutung erklärt sich anders: Die Bausteine wurden zum Antrieb jeder modernen Industriegesellschaft. Die Siliziumplättchen sind der Rohstoff, ohne den - wie beim Öl - in vielen Branchen nichts mehr geht. Sie stecken nicht nur in Computern, sondern auch in Autos, Raketen und Waffen, Waschmaschinen oder Musikinstrumenten. Wer das Chip-Geschäft beherrscht, hat auch andere Märkte unter Kontrolle.

Kein Wunder, daß es die amerikanischen und europäischen Industrie mehr als stört, daß auf der Welt-rangliste der Chip-Hersteller japanische Unternehmen dominieren. Die Angst vorm japanischen Weltmonopol geht um. Und die kommt nicht von ungefähr.

Die Konkurrenz im Osten hat die strategische Bedeutung der elektro-

nischen Ware rechtzeitig erkannt. Im Gegensatz zu ihren amerikanischen Wettbewerbern ließen sie sich auch von zeitweise horrenden Verlusten nicht irritieren - sie machten beharrlich weiter. Die meisten Amerikaner stiegen hingegen aus dem Geschäft mit der Massenware, den Speicherchips, aus. Und weil die Europäer lange Zeit glaubten, in diese Technologie gar nicht erst einsteigen zu müssen, hängen heute viele Branchen von der Versorgung aus Japan ab.

Viel Geld und Zeit hat es Siemens und andere dann gekostet, mit einem enormen Kraftakt nur die unteren Plätze auf der Hersteller-Liste zu erobern. Doch langfristig kann die europäische Industrie gegen die riesigen Konglomerate des Inselreiches, die unter der Rückendeckung des mächtigen Handelsministeriums MITI agieren, nicht durchhalten. Und in den USA platze jüngst der Plan, eine Gegen-offensive zu starten. Die zunächst unternehmungslustigen US-Computerkonzerne verzichteten am Ende darauf, die verlorene Bastion zurückzuerobern. Das gemeinsame Unternehmen, das fortan die Versorgung mit Chips aus heimischer Produktion sichern sollte, scheiterte am Geld.

Auch beim finanzstarken Konzern Siemens drohen die Kosten des technischen Fortschrittes unherrschbar zu werden. Die Bereitschaft zur Kooperation wuchs auch bei IBM nur, weil selbst der größte Computer-Konzern der Welt nicht verkraften kann, Hunderte von Millionen Dollar dafür auszugeben, ein kleines Plättchen namens 64-Mega-bit-Chip zu entwerfen, um - wie bisher - einen Teil der Eigenversorgung sichern zu können.

Das brutale Prinzip für Verkäufer in diesem Geschäft: Nur der erste Anbieter kann mit einem neuen Chip Geld verdienen, der zweite geht schon leer aus und der dritte schreibt Verluste. Dafür sorgt regelmäßig ein abenteuerlicher Preisverfall. Der Grund: Kaum ist eine neue Chip-Generation auf dem Markt, wird die nächste angekündigt. Das Tempo bestimmen allein die Japaner. Wer nicht mithält, gerät in Abhängigkeit.

Diese Hetze kostet Europas Industrie und Steuerzahler mittlerweile

Milliarden. Und der Preis dafür, zum exklusiven Club derjenigen zu gehören, die die Technologie beherrschen, wird weiter steigen, die Zahl der Konkurrenten sinken. Auf diese Weise erreicht der Wettbewerb in absehbarer Zeit sein Endstadium. Geht diese Entwicklung mit gleichem Tempo weiter, bleiben immer weniger Weltkonzerne übrig, die dann mit Milliardensummen Technik zur Selbsterhaltung weitertreiben müssen - ein aberwitziger Wettlauf.

(Gunhild Lütge, Wirtschaftsredakteurin der ZEIT)

Sogar **schlechte Software**
bringt man an den Mann:

Durch **gute Präsentation!**

Wir bieten Ihnen den Rahmen für Ihre Präsentationen/Seminare:

- Seminarräume auf Bodensee-Insel
- PCs, Overh.proj. usw.
- techn. Support in SW u. HW
- Hotels u. Restaurants ganz nah
- Freizeit: Weinproben, Bootsfahrt usw.

Rufen Sie uns an: 0 71 41 11 11 11

Datenschutz in der EG:

Grenzenlose Kontrolle

von Dagmar Boedicker

Dieser Beitrag beschreibt des europäischen Kaisers neue Kleider: den Datenschutz. Neben dem Artikel von Ingo Ruhmann speziell zum Schengener Abkommen soll er Hintergrund-Information zu der FIFF-Resolution bieten, die im Heft 1/90 der **FIFF** KOMMUNIKATION veröffentlicht wurde.

Der grenzüberschreitende Datenverkehr nimmt zu ...

Immer mehr Daten bewegen sich im Binnenmarkt und wandern über die Grenzen: für Kreditauskünfte, in Marketing- und Adressdateien, um Ansprüche auf Sozialleistungen zu wahren, ... Sie wandern in öffentlichen oder privaten Netzen, zu denen der Zugang durch die Open Network Provision (ONP) gefördert wird. Die Netze werden immer weiter ausgebaut und immer einfacher und billiger zu nutzen sein. Von 393 000 im Jahr 1979 ist die Zahl der Anschlüsse an west-europäische Netze auf über 1,5 Millionen 1987 nach einer UN-Untersuchung gestiegen.

Die EG-Kommission fordert in ihrem Grünbuch einen Ausbau der Netze und ihre Standardisierung.

Das große Projekt einer wirtschaftlichen und politischen Gemeinschaft erfordert Grundlagen für die Planung und Gesetzgebung, wie zum Beispiel für die gemeinsame Agrarpolitik. Die Menge der zu diesem und anderen Zwecken erhobenen und verarbeiteten Daten nimmt ständig zu.

Immer mehr Daten fallen an - auch jetzt schon - und wollen von den Konzernen genutzt sein. Grenzen spielen in transnationalen Konzernen kaum noch eine Rolle, grenzüberschreitender Datenverkehr findet statt, auch wenn er de

jure in etliche Länder verboten wäre.

... und führt in die Illegalität

"Hinreichende Lösungen werden vom Gesetzgeber derzeit weder national noch international noch supranational angeboten; mit Regelungen ist in absehbarer Zukunft nicht zu rechnen. Damit besteht die Gefahr, daß die Wirtschaft entweder auf wesentliche Verarbeitungsvorgänge verzichten muß, oder in die Illegalität getrieben wird." Soweit eine Erklärung der Gesellschaft für Datenschutz und Datensicherung.

Nur sieben der zwölf EG-Mitgliedstaaten haben ein Datenschutz-Gesetz. Zwar sollte man die Bedeutung dieser Gesetze nicht überschätzen, es wird aber kaum bestritten, daß grenzüberschreitender Datenverkehr in Länder ganz ohne Datenschutz-Gesetz nicht zulässig sein kann, weil schutzwürdige Belange der Betroffenen verletzt werden.

Für die Arbeitnehmerinnen und Arbeitnehmer wird es bei Datentransfers ins Ausland so gut wie unmöglich, selbst Auskunft über Inhalt und Umfang der über sie gespeicherten Daten zu erhalten; Sperrungs- oder Löschungsrechte auszuüben wird genauso erschwert, wie Beteiligungsrechte der Betriebsräte wahrzunehmen. Die ohnehin schon dürftigen Kontrollen durch die Aufsichtsbehörden können im Ausland natürlich nicht ausgeübt werden: Sie gelten nur für das nationale Hoheitsgebiet.

Wen kümmert das?

Woran mag es liegen, wenn sich trotzdem außer einigen Datenschutz-Beauftragten und nationalen

Juristen kaum jemand kritisch mit diesem Thema zu befassen scheint? Vor allem nicht die EG-Kommission, deren bisherige Aktivitäten sich darauf beschränkt haben, bisweilen zu empfehlen, die Mitgliederstaaten mögen doch die Datenschutz-Konvention des Europarates unterschreiben. Diese Konvention strebt einen uneingeschränkten Informationsfluß über die Grenzen an und setzt dazu voraus, daß die Unterzeichnerstaaten über gleichwertige Datenschutzregelungen verfügen. Obwohl diese Voraussetzung keineswegs erfüllt wird (Spanien beispielsweise hat unterzeichnet, es gibt dort aber kein Datenschutz-Gesetz), haben sich bisher nur sechs der EG-Staaten zur Ratifizierung entschlossen.

Regelrechte Datenschutzregelungen sind also nicht gegeben, es sieht vielmehr traurig aus. So stellt der hessische Datenschutz-Beauftragte, Spiros Simitis, über den gegenwärtigen Zustand fest, daß die Appelle des Europaparlaments folgenlos gewesen sind, daß aber die fehlenden Datenschutz-Regelungen weder Behörden noch Industrie daran hindern, Daten zu speichern. Er erklärt, daß Italien und Belgien fleißig Daten verarbeiten, ohne ein Datenschutz-Gesetz zu haben, und daß die supranationale Zielsetzung der EG zwangsläufig zu einer Erweiterung des grenzüberschreitenden Datenverkehrs führen wird. Als einer von wenigen warnt er vor einem Informations-Markt, in dem die von den öffentlichen Verwaltungen gespeicherten personenbezogenen Daten kommerzialisiert werden sollen. Dies stelle einen eindeutigen Verstoß gegen die Zweckbindung dar. Auch für die von der EG selbst verarbeiteten Daten, deren Umfang zunehmen wird, seien gesetzliche Regelungen notwendig.

Arbeitnehmer(innen)- und Sozialdatenschutz

Sozialdaten sollen im Binnenmarkt zukünftig im Online-Verfahren zwischen Sozialversicherungen ausgetauscht werden. In der BRD genießen diese Daten einen besonderen Schutz durch das Sozialgeheimnis, das im Sozialgesetzbuch verankert ist. Durch die internationale Zusammenarbeit ist dieser Schutz allerdings bereits gefährdet.

Die rechtmäßige Wahrung von Leistungsansprüchen der Arbeitnehmer, so erwünscht ihre Freizügigkeit im EG-Binnenmarkt sein mag, darf nicht dazu führen, daß der Datenschutz der Mitgliedstaaten, also auch der BRD, aufgeweicht wird. Hier fordern die holländische Stichting Waakzaamheid Persoonsregistratie (SWP) und die Deutsche Vereinigung für Datenschutz (DVD) mehr Transparenz und die Weiterentwicklung nationaler Datenschutz-Gesetze.

Kann der Verbraucherschutz helfen?

Nicht nach Ansicht der DVD/SWP: "Gegenüber internationalen Auskunftsteilen, Versicherungsgesellschaften und Banken sind selbst Verbraucherverbände machtlos. Um die 'informationelle Vermarktung' der Verbraucherinnen und Verbraucher zu verhindern, bedarf es europäischer Verbandsklage-Befugnisse und der Einführung einer Datenschutz-Verträglichkeitsprüfung."

Gesetzliche Grundlagen für den Datenschutz in den Europäischen Gemeinschaften

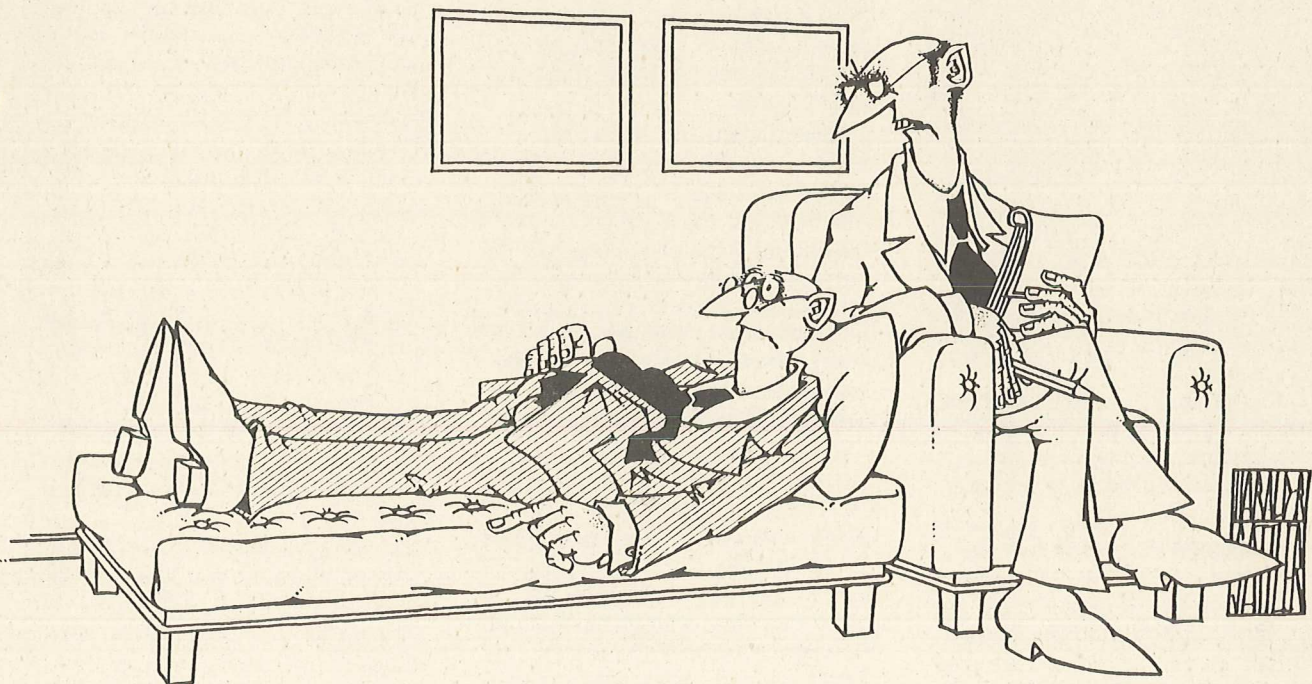
Wie bereits erwähnt, haben nicht alle Länder in der EG ein Datenschutz-Gesetz. Vorhandene Gesetze beruhen aber außerdem auf sehr unterschiedlichen Grundlagen. Ich möchte aus einer vergleichenden Zusammenfassung der DvD zum Datenschutz im öffentlichen Bereich

einige Grundsätze anführen. Die Zusammenstellung beantwortet drei Fragen:

- Wann ist eine Datenerhebung in den Ländern rechtmäßig (Legitimität)?
- Wieviel erfahren die Bürger(-innen) über die Datenerhebung und welche Ausnahmen zu Auskunftsrechten gibt es (Transparenz)?
- Wer kontrolliert wie die Praxis der Behörden (Kontrollmöglichkeiten)?

Legitimität: In allen angeführten EG-Ländern (Dänemark, Frankreich, Bundesrepublik Deutschland, Luxemburg) gibt es eine gesetzliche Grundlage: in der Bundesrepublik und Dänemark hat eine Abwägung zwischen Notwendigkeit der Erhebung und persönlichen Interessen der Betroffenen stattzufinden, in Frankreich und Luxemburg ist eine Verordnung oder ein Gesetz über die Erhebung von einer Kommission zunächst zu prüfen.

Transparenz: Nicht überall besteht eine Informationspflicht, in manchen Ländern ist sie nicht ausrei-



"Ganz minderwertig können Sie nicht sein: immerhin sind Sie bei der Volkszählung miterfaßt worden, oder?"

(Harald R. Sattler)

chend. In der Bundesrepublik wird die erste Einspeicherung nicht den Betroffenen mitgeteilt, sondern im Blatt für amtliche Bekanntmachungen veröffentlicht, das wohl kaum zur bevorzugten Lektüre gehört. In Dänemark legt eine Kann-Bestimmung fest, daß die Betroffenen benachrichtigt werden können, um sie auf ihr Auskunftsrecht hinzuweisen. Frankreich hat eine erheblich günstigere Regelung: Die Betroffenen müssen erfahren, ob es sich um obligatorische oder freiwillige Angaben handelt, welche Folgen es hat, wenn sie nicht antworten, für wen die Daten bestimmt sind, und daß ein Auskunfts- und ein Berichtigungsrecht besteht. Auch in Luxemburg erfolgt eine solche umfangreiche Information der Betroffenen.

Deutschland, Frankreich und Luxemburg haben ein öffentlich zugängliches Register der behördlichen Datenverarbeitung, Dänemark nicht. In Deutschland und Dänemark berichten die für den Datenschutz Zuständigen an das Parlament, in Luxemburg und Frankreich werden die Berichte veröffentlicht.

Ausgenommen von der Auskunftspflicht (auch gegenüber dem Datenschutz-Beauftragten) sind in der Bundesrepublik Deutschland: Behörden des Verfassungsschutzes, BND, MAD, andere Sicherheitsbehörden des Verteidigungsministeriums, Bundes- und Landes-Finanzbehörden, Behörden der Polizei und der Staatsanwaltschaft, gesetzlich vorgeschriebene Register. Außerdem bestehen Ausnahmen bei Gefährdung der öffentlichen Sicherheit und Ordnung oder des Wohles von Bund und Land, bei Gefährdung der rechtmäßigen Aufgabenerfüllung, bei Geheimhaltung aufgrund Rechtsvorschrift oder ihrem Wesen nach überwiegendem berechtigtem Interesse einer dritten Person. Es gibt neben dem DSG verschiedene Verwaltungsgesetze, die ein Auskunftsrecht gewähren.

Frankreich und Dänemark sehen eine Auskunft über medizinische Daten nur auf dem Weg über den Arzt vor. In Frankreich können sich die Bürger(innen) mit einem Auskunftsbegehren zu Sicherheitsrelevanten Belangen an die Commission Nationale de l'Information et des Libertés (CNIL) wenden, die eines

ihrer Mitglieder zur Überprüfung einsetzt. Auf Antrag der Dateiverantwortlichen kann die CNIL maßvolle Einschränkungen des Auskunftsrechts einräumen. Dänemark schränkt das Auskunftsrecht ein bei überwiegendem öffentlichem oder privaten Interesse an der Geheimhaltung und bei Daten, die ausschließlich zu statistischen Zwecken gespeichert werden. Luxemburg sieht Einschränkungen vor, wenn die Herausgabe der Daten durch ein Gesetz oder eine Verordnung untersagt ist, und bei Daten, die bereits übermittelt worden sind, oder wenn sie in einer anderen Form als der hier vorgesehenen übermittelt werden können und dies durch Gesetz, Verordnung oder Vertrag vorgesehen ist (!).

Kontrollmöglichkeiten: Sie wurzeln in den Auskunftsmöglichkeiten, denn: Wer kann Kontrollrechte wahrnehmen, ohne zu wissen, auf welche Sachverhalte sie sich erstrecken? Beanstandungen sind gesetzlich vorgesehen in Deutschland, Frankreich und Luxemburg. In Dänemark sind sie beschränkt auf Streitigkeiten, deren Gegenstand die Ausübung des Auskunftsrechts ist. Für die Löschung und Berichtigung sind die Behörden selbst zuständig, oder die "Registertilsynet" (Data Surveillance Authority - DSA). In Frankreich liegt die Beweislast grundsätzlich bei der Stelle, der gegenüber das Auskunftsrecht ausgeübt wurde.

Eine Sperrung ist nur in der Bundesrepublik vorgesehen, Berichtigung und Löschung ermöglichen alle vier Staaten, wenn auch ohne besondere Regelungen (bis auf die Bundesrepublik). Auf Antrag erhalten die Betroffenen in Frankreich und Luxemburg eine Abschrift der vorgenommenen Änderung. - Alle vier Staaten sehen ein Beschwerderecht der Betroffenen vor.

(Um eine einigermaßen lesbare Länge (bzw. Kürze) dieses Beitrags zu erreichen, war ich gezwungen, manche Nuance zu streichen. Diese Zusammenfassung ist also nicht ganz so präzise, wie Sie sich das möglicherweise wünschen. Auch die Beschränkung auf EG-Staaten wurde dadurch leider notwendig, ist aber für eine Betrachtung des Themas an sich nicht wünschenswert.)

Harmonisierung des Datenschutzes in der EG

Datenschutz-Gesetze anderer Länder sind in diversen Aspekten unserem Datenschutz-Gesetz überlegen, in anderen hat dagegen die Bundesrepublik die besseren Regelungen. So sieht beispielsweise Norwegen einen Schutz auch für Personengruppen vor. Dem liegt die Überlegung zugrunde, daß auch politische Gruppierungen, Wohngemeinschaften oder andere Personenvereinigungen in eigenen Rechten genauso verletzt werden können wie die Personen, die sich in ihnen zusammengeschlossen haben.

Daher unsere Forderung, den Datenschutz EG-weit durch eine Richtlinie zu harmonisieren, die sich an den jeweils weitestgehenden nationalen Regelungen orientiert. Wir würden es außerdem begrüßen, wenn die EG-Kommission bei ihrem Vorschlag über den eigenen Teller rand schauen und Empfehlungen, Konventionen und nationale Regelungen von Drittländern (d.h. Staaten außerhalb der EG) berücksichtigen würde.

Harmonisierung: Das ist die Formel, nach der sich nationales Interesse, wie beispielsweise die größtmögliche Erhaltung von einzelstaatlicher Souveränität, wahren, und trotzdem eine Vereinheitlichung im EG-Rahmen erreichen läßt. Richtlinien stecken einen Rahmen für die nationale Gesetzgebung ab. Sie erlauben den Mitgliedstaaten eine Umsetzung in nationales Recht innerhalb eines vernünftigen Zeitrahmens und vermeiden weitgehend eine Anpassung "nach unten", also in Richtung auf den niedrigsten Standard. Zwar wäre eine Verordnung vorzuziehen (sie wird in den Mitgliedstaaten sofort und unmittelbar wirksam), die Chancen, daß sich alle Staaten darauf einigen, sind aber gleich Null.

(Dagmar Boedicker, 37, ist Übersetzerin für Englisch und Spanisch und schreibt Software-Handbücher.

Gemeinsam mit Stefan Huber koordiniert sie die Aktivitäten des überregionalen Arbeitskreises "FIF euro-pawelt".)

Datenschutz in der EG:

Vom Schlagbaum zum Datenverbund

Schengen und die Folgen

von Ingo Ruhmann

Europa '92 bedeutet nicht nur das Ende der Binnengrenzen, sondern nach Meinung von Kritikern auch ein Ende der Bindung der Polizei an das Recht und an nationale Errungenschaften wie den Datenschutz und das informationelle Selbstbestimmungsrecht. Ein entfesselter Kommissar Computer wird zum Grundstein einer europäischen Polizeibehörde.

Die deutsch-nationale Wallung brachte auch ein wenig bekanntes Nebenprodukt von Europa '92 in die Schlagzeilen. Am 15. Dezember 1989 wollte die Bundesregierung den Schengen-Vertrag ratifizieren, in dem zum Ausgleich für den Abbau der Grenzkontrollen eine stärkere polizeiliche Zusammenarbeit vereinbart werden sollte. Im letzten Moment zuckte die Bundesregierung jedoch zurück, weil die Vertragspartner, die BeNeLux-Länder und Frankreich, es nicht hinnehmen wollten, daß nach der Einigung, alle Menschen aus Nicht-Schengen-Staaten als Drittausländer zu betrachten und für sie z.T. neue, strenge Visabestimmungen zu erlassen sowie scharfen Grenzkontrollen zu unterziehen, ausgerechnet die sechzehn Millionen DDR-Bürger und die deutschstämmigen Übersiedler davon ausgenommen werden sollten.

Die Bonner Regierung zeigte damit erstmals eine Reaktion auf die eigentliche Bedeutung des Schengener Abkommens: die Auf-

gabe einer eigenständigen nationalen Innenpolitik und deren Ersatz durch eine Innenpolitik der Schengen-Staaten, später dann der europäischen Staaten. Und einen solchen Schritt wollte Bonn dann doch nicht tun. Kaum, daß der neue Traum von der deutschen Großmacht begonnen hat, wäre er durch Schengen schon wieder zu Ende gewesen.

Doch nicht nur in Bonn gibt es Probleme, sich an den Gedanken zu gewöhnen, nationalstaatliche Gesetzesentwicklungen und Gewohnheiten ebenso wie Erfahrungen aus der Geschichte über den Haufen zu werfen. Die Niederlande, Belgien und Frankreich sträuben sich, dem starken Verlangen der bundesdeutschen Polizei nach grenzübergreifender Tätigkeit, der sogenannten "Nacheile" über die Grenze hinter Flüchtenden her und dem Observieren in anderen Schengen-Mitgliedsländern, nachzukommen. Auch die 45 Jahre seit dem zweiten Weltkrieg haben bei den Opfern noch nicht ausgereicht, all das zu vergessen, was deutsche Polizeikräfte anstellen können.

Frankreich und die Niederlande würden gern den Strömen von Schwarzgeld nachforschen, die ihre Bürger in luxemburgischen Banken deponieren, doch Luxemburg will sich weder dieses Geschäft noch das mit der Geldwäsche durch die Lockerung des Bankgeheimnisses verderben lassen. Der Ausbau von Amsterdam-Schipol zu einem bedeutenden Duty-Free-Zentrum

hätte schließlich wenig Sinn gehabt, wenn durch Schengen schon vor dem europäischen Binnenmarkt Flüge nach Paris, Frankfurt und München durch gemeinsame Visa- und Zollbestimmungen zu Inlandsflügen würden. Und auch außerhalb der Bundesrepublik besteht die Angst vor dem Supranationalen Überwachungsstaat, die sich vor allem am geplanten Schengen-weiten Polizeicomputer-Verbund, dem Schengen-Informationssystem (SIS), entzündet.

So berechtigt diese Vorbehalte im Einzelnen auch sein mögen, haben sie für unbefangene Betrachter doch den Anschein, als ob hier überkommenes nationalstaatliches Denken dem Gedanken der europäischen Einigung im Wege steht. Probleme auf dem Weg zu einer einheitlichen europäischen Innenpolitik ließen sich schließlich durch eine Ausweitung der Rechte der demokratischen Vertretung der Europabürgerinnen und -Bürger, des Europaparlaments also, lösen. Das Europaparlament zu stärken, wäre für das Problem Schengen wie für die gesamte europäische Innenpolitik allerdings keine Lösung, denn europäische Innenpolitik wird an allen Parlamenten vorbei gemacht.

Den im europäischen Kontext ins Leben gerufenen polizeilichen Organisationen auf übernationaler Ebene ist gemein, daß sie neben den politischen Strukturen der EG etabliert wurden.

TREVI

Die älteste Keimzelle einer europäischen Polizeiorganisation ist die auf der EG-Ratssitzung am 2. Dezember 1975 zum besseren Informationsaustausch eingerichtete Arbeitsgemeinschaft TREVI ("Terrorisme, Radicalisme, Extremisme et Violence International"), der mittlerweile neben den EG-Ländern auch die USA, Kanada, Australien, Norwegen, Schweden, Österreich, Schweiz, Marokko, Jugoslawien und Malta angehören. TREVI ist jedoch keine EG-Institution und entzieht sich so der Kontrolle durch das EG-Parlament.

Das Gremium teilt sich in drei Arbeitsebenen auf: Innen- bzw. Justizminister, hohe Beamte dieser Ministerien und Arbeitsgruppen mit Polizeiexperten. Solche Arbeitsgruppen bestehen zu drei Themen:

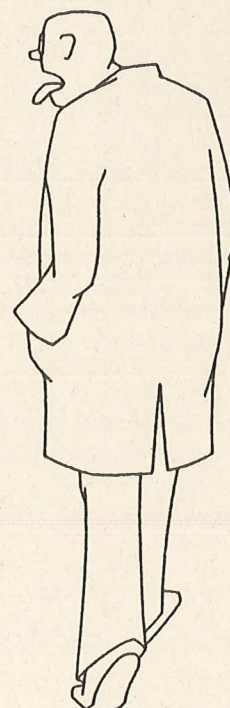
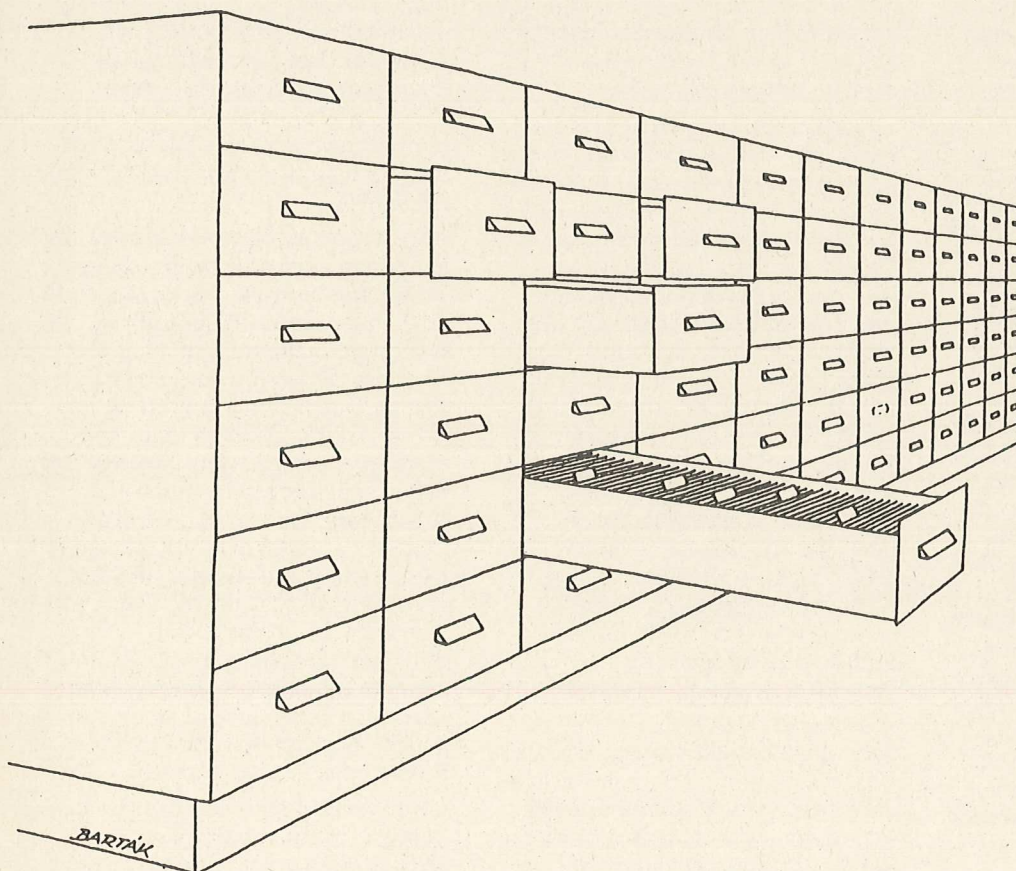
Terrorismus (TREVI I), Ausbildung und (Kommunikations- und DV-) Technologie (TREVI II) und die AG TREVI III, die sich mit Schwerverbrechen, organisierter Kriminalität und "Störungen der öffentlichen Sicherheit" auseinandersetzt. Geplant ist eine AG TREVI IV zu Maßnahmen gegen nukleare und nichtnukleare Katastrophen und deren Vorsorge. In TREVI-Gruppen wurden Asyl- und Ausländerrechtsfragen ebenso beraten wie die Gestaltung maschinenlesbarer Ausweispapiere. Die Kommunikation über Vorfälle geht über ein abhörsicheres Spezialnetz. TREVI ist also ein bedeutendes europäisches Koordinationsinstrument polizeilicher Arbeit.

Schengen

Im Mosel-Örtchen Schengen wurde am 14. Juni 1985 zwischen

den Niederlanden, Belgien, Luxemburg, Frankreich und der Bundesrepublik der sog. Schengener Vertrag abgeschlossen. Sein Ziel ist es, die Grenzkontrollen zu reduzieren und dafür als Kompensation:

- Asylanträge in nur einem Schengen-Vertragsstaat zu erlauben und alle einmal abgewiesenen Asylanten Schengen-weit abzuweisen,
- Polizeiaktionen auf dem Gebiet anderer Vertragsstaaten zu regeln, insbesondere die Verfolgung über die Grenze hinweg ("Nacheile") und die Observation,
- Rechtsnormen, vor allem aber die Rauschgiftpolitik der Schengen-Staaten, an die strengsten Normen - das sind zumeist die der Bundesrepublik - anzugleichen,
- Auslieferung und Amtshilfe zu erleichtern, die nicht mehr unter



(Barták)

Kontrolle der Außenministerien, sondern der Staatsanwaltschaften, z.T. aber auch der Polizeidienststellen möglich sein sollen,

- Zusammenarbeit bei der "präventiven Verbrechensbekämpfung" zu vereinbaren,
- ein Informations- und Kommunikationssystem (Schengen Informationssystem, SIS) zur Schengen-weiten Fahndung, Ausschreibung abzuweisender Ausländer sowie zur beobachtenden Fahndung aufzubauen.

Die Bundesregierung hat zwar inzwischen erklärt, sie wolle die Grenzkontrollen nicht völlig wegfällen lassen¹, dies ist jedoch noch lange kein Grund, die aus polizeilicher Sicht auch ohne Europa '92 überfälligen "Kompensationsmaßnahmen" aufzugeben. Schengen ist ein einfach zu verlockendes Mittel, um die alten Träume einer europäischen Polizei umzusetzen. Das sagt eleganter Bundesinnenminister Schäuble: "Dies ist eine wesentliche Bedeutung des Abbaues von Grenzkontrollen: Sie stellen für die Menschen eine psychologische Barriere dar, die ihnen ein Gefühl der Sicherheit verleiht, wenn dieses Gefühl der Sicherheit auch zum Teil trügerisch ist. Dies gilt es für die zukünftige Sicherheitspolitik nutzbar zu machen: Wer Grenzen abbaut, der muß Ersatz schaffen, einen Ersatz, für den schon lange die sachliche Notwendigkeit besteht. Doch nun kommt der psychologische Druck hinzu"². Ein psychologischer Druck, den das Innenministerium bisher kräftig geschürt hat.

Bei diesen polizeilichen Zielen zur Erreichung von Recht und Ordnung spielen die rechtlichen Probleme kaum noch eine Rolle, obwohl sie noch gar nicht vollständig zu übersehen sind. Schengen in der gegenwärtigen Form verletzt jedenfalls eine Reihe von Grundrechten:

1. Einer Schengen-weiten Asylpolitik müßte der Artikel 16 des Grundgesetzes weichen: das Asylrecht wird durch Schengen ausgehebelt und der ebenfalls zum Artikel 16 gehörende Satz "Kein Deutscher darf an

das Ausland ausgeliefert werden" wird ebenso zur Makulatur.

2. Polizeiaktionen in anderen Ländern setzen u.U. voraus, sowohl klare Normen zur Vermeidung einer Doppelbestrafung zu schaffen, als auch z.B. zu regeln, mit welchen Mitteln eine Observation geschehen darf: dürfen bundesdeutsche Polizisten in Belgien mehr als zu Hause? Für Polizeiaktionen ausländischer Polizeibehörden gegen Bundesbürger gilt gleiches; was deren rechtliche Überprüfbarkeit angeht, so ist es fraglich, ob die Rechtsweggarantie des Grundgesetzes gewährleistet ist.

3. Die Rauschgiftpolitik vor allem zwischen den Niederlanden und der Bundesrepublik anzugleichen soll bedeuten, daß Holländer nicht mehr an Bundesbürgerinnen und -bürger verkaufen dürfen, und daß Bundesbürgerinnen und -bürger, die Rauschgift in den Niederlanden erwerben, von der dortigen Polizei festgenommen und nach Aufnahme eines Protokolls an eine deutsche Grenzstelle abgeschoben werden. Dies wiederum wäre juristisch der Entzug des gesetzlichen Richters.

4. Ein letzter juristische Streitpunkt um Grundrechte ist die Länderhoheit in Polizeiangelegenheiten, die durch den von der Bundesregierung für die Länder abgeschlossenen Vertrag umgangen wird.

Der dickste Brocken im Schengen-Vertrag ist allerdings der Computerverbund SIS. Dieses Informationssystem ist das Pilotprojekt einer internationalen Polizeiorganisation. So kann jede bundesdeutsche Staatsanwaltschaft Datenbestände in das SIS einstellen und alle Polizeibehörden der Schengen-Vertragsländer genauso zu ihrem Hilfsorgan machen, wie dies bisher nur für inländische Polizeidienststellen galt - zusätzliche nationale Kontrollen über die Berechtigung des Ersuchens entfallen.

Das Resultat sind allerdings neue Probleme: Politiker aus dem Nahen Osten, nach denen etwa die Bundesrepublik fahnden läßt, sind in

Frankreich durchaus respektierte Verhandlungspartner der Regierung. Die französische Regierung hat bereits signalisiert, daß sie sich ihre Außenpolitik durch eine derartige unkontrollierte Übernahme von Fahndungsersuchen in SIS nicht beeinträchtigen lassen will.

Damit stellt das SIS den größten bisher bekannt gewordenen Datentransfer von äußerst sensiblen Daten aus der Bundesrepublik heraus dar. Liefere alles nach Recht und Datenschutzgesetz, so hätte dies zu unterbleiben, da in Belgien keinerlei Datenschutzregelungen existieren. Das SIS wird dennoch munter weitergeplant und realisiert. Auf einer gemeinsamen Tagung der Deutschen Vereinigung für Datenschutz (DVD) und ihrer holländischen Schwesterorganisation Stichting Waakzaamheid Persoonsregistratie (SWP) kamen zu diesem Thema einige Einzelheiten zur Sprache.

Die Planungen gehen von zunächst 800.000 Datensätzen aus, davon sind 15% personenbezogene Daten, 55% Sachdaten und zunächst 30% Reserve. Insgesamt wird mit 5,5 Millionen Datensätze in der Ausbauphase gerechnet. Die Zugriffszeiten sind auf 8-12 Zugriffe pro Sekunde ausgelegt, die Übertragung auf dem speziellen SIS-Netz läuft mit X25-Protokoll bei 9600 Baud. Die SIS-Infrastruktur sieht einen Zentralrechner (ZSIS) und in allen Schengen-Vertragsstaaten nationale Knotenrechner (NSIS) vor. Dabei wird auf die bereits bestehende Infrastruktur nationaler polizeilicher Computersysteme - in den Niederlanden PODACS, in der Bundesrepublik INPOL - zurückgegriffen. Ersten Gerüchten zufolge soll eine Zusage für die Lieferung des Zentralrechners an die Firma Siemens gegangen sein, die beim BKA schon genügend Erfahrungen gesammelt habe. Wiesbaden und damit das BKA zur SIS-Zentrale zu machen, stößt jedoch auf Widerstände.

Gerade das BKA zeigt, wohin die Richtung mit SIS geht: das BKA hat ebenfalls Anfang der siebziger Jahre als zentrale Informationsstelle der bundesdeutschen Polizeibehörden

angefangen und sich erst über sein Informationsmonopol zum "deutschen FBI" entwickelt. Mit SIS wird wie bereits beim BKA ein Computersystem zum Rückgrat polizeilicher Kontroll- und Überwachungstätigkeit.

Und dies wird nicht auf Schengen begrenzt bleiben: "Die Ergebnisse der Verhandlungen über das Schengener Informationssystem werden neben ihrer Bedeutung für die Vertragspartner zudem Grundlage für die ebenfalls geplante Errichtung eines Informationssystems der 12 EG-Mitgliedsstaaten sein", so Bundesinnenminister Schäuble im BKA am 7. November 1989³. Aber nicht nur die EG sieht den Erfahrungen mit SIS mit Interesse entgegen, sondern auch die gerade gegründete TREVI-AG "1992", die sich mit genau denselben "Kompensationsmaßnahmen" befaßt, wie sie in Schengen geregelt wurden. Dazu Schäuble am 16. November 1989 in Den Haag: "Damit werden die TREVI-Kompetenzen praktisch auf alle Bereiche der grenzüberschreitenden Zusammenarbeit im Sicherheitsbereich erweitert". So bildet Schengen die Grundlage für eine gemeinsame Polizeipolitik der EG-Staaten wie auch der restlichen TREVI-Länder von den USA über Australien bis hin zu Jugoslawien und Malta.

Was schließlich das Grundrecht auf informationelle Selbstbestimmung angeht, so ist damit zu rechnen, daß sich in einem im Moment weder durch Parlamente noch durch Datenschützer kontrollierbaren System wie SIS ein noch schlimmerer Daten-Wildwuchs entwickeln wird, wie in den Anfangszeiten des BKA. Mit Hilfe des SIS lassen sich schließlich auch nationale Einschränkungen umgehen, die gerade dem BKA immer ein Dorn im Auge waren. Der BKA-Präsident Boge ließ bereits verlauten, der Datenschutz sei ein "Problem der Deutschen". Schengen bietet da Abhilfe.

Datenschutz ist jedoch nicht das Problem der Deutschen sondern das des BKA. Diese unter Horst Herold um Computer herum aufgebaute Polizeiorganisation setzte weltweit

führend jede Art der Technik ein, nicht nur um Verbrechen aufzuklären, sondern auch, um Verbrechen durch eine umfassende Verdattung der Gesellschaft nach Möglichkeit zu verhüten. Auch, wenn die Verhütung versagt hat, so sind Raster- und Schleppnetzfahndung, "elektronische Notizblöcke", aber auch automatische Videobildauswertung und Sprechererkennung zu gern genutzten Mitteln polizeilicher Arbeit geworden. Und das BKA ist es, das seit Jahren bereits die treibende Kraft hinter dem Wunsch nach einer Euro-Polizei darstellt. Was in bilateralen Polizeikooperationen mit verschiedensten Ländern bisher versucht wurde, soll in großen Stil nun mit Schengen und TREVI europaweit Einzug halten.

Schengen wird also ohne parlamentarische Beratung über die zuständigen Bundesländer hinweg unterzeichnet, setzt Grundrechte außer Kraft und überträgt unzulässigerweise Rechte an eine supranationale Organisation, die keinerlei demokratischer Kontrolle unterliegt. Damit dies nicht vor der Zeit ruchbar wird, bleiben die Schengen-Vertragsentwürfe offiziell geheim, ebenso wie die Ergebnisse von TREVI-Arbeitsgruppen. Zusammenfassend bedeutet dies einen Grundrechtsabbau ohne irgendeine Notwendigkeit und all dies unter konspirativen Umständen - oder, wie sich staatliche Stellen ausdrücken dürfen: unter Ausschuß der Öffentlichkeit.

Wie ist dies nun zu bewerten? Dazu der Rechtsanwalt und Polizeixperte Thilo Weichert: "Man kann zu Europa stehen, wie man will. In jedem Fall ist das, was demokratisch gewählte Regierungen derzeit im Bereich "Innere Sicherheit" planen, mit den minimalsten Standards der eigenen nationalen Rechtssysteme nicht vereinbar. Europa war und ist derzeit nichts anderes als ein Europa der Unternehmer und Bürokraten. Ein Europa der Menschen oder der Menschenrechte ist nicht in Sicht. Ein "Europa der Inneren Sicherheit", wie es derzeit geplant ist, darf es nicht geben"⁴.

Während also andererseits selbst von unserem Innenminister Schäuble eine "Renaissance der Freiheit" geortet wird, sollten wir uns unsere Grundrechte nicht still und heimlich nehmen lassen. Organisationen wie DVD und SWP wollen grenzübergreifend gegen ein "Europa der Polizei und der Konzerne und für ein Europa der Informationsfreiheit" zusammenarbeiten. Das FIFF sollte da nicht zurückstehen.

¹ Die Grenzkontrollen fallen nicht völlig weg, in: Die Woche im Bundestag, 17/89, S. 33

² BMI Schäuble am 16. November 1989 in Den Haag: Europa ohne Grenzen - Eine sichere Gemeinschaft; in: Innere Sicherheit, 5/89, S. 11

³ BMI Schäuble am 7. November 1989 im BKA: Technik im Dienst der Strafbekämpfung; in: Innere Sicherheit, 5/89, S. 19

⁴ Thilo Weichert: Europolizei. Die Entfesselung der Exekutive vom Recht; in: Forum Recht, 3/89, S. 21-26

(Eine Kurzinformation zu Ingo Ruhmann befindet sich am Ende des Artikels "Wie ein Geheimdienst ...".)

WERKZEUG - BENUTZEN
MASCHINE - BEDIENEN
COMPUTER - ??

Denkzeug Computer

Ein Zeug ist ein Mittel zum Zweck

von Bernhard Steiner

In letzter Zeit ist ein neuer Begriff entstanden, der helfen soll, den Computer in das Begriffsschema technischer Geräte einzugliedern - *Denkzeug*. Damit soll ausgedrückt werden, daß uns Computer in ähnlicher Weise helfen sollen unsere 'geistigen' (besser: kognitiven) Fähigkeiten auszuweiten und zu ergänzen, wie dies Werkzeuge im körperlichen Bereich tun. Gerade der Begriff *Zeug* drückt wie kein anderer aus, wie eine Technik beschaffen sein müßte, die menschengerecht (I. Illich¹) benützt dafür den Begriff *konvival*) genannt werden will. Heidegger etwa definiert den Begriff 'Zeug' so: "Zeug ist wesentlich 'etwas, um zu ...'. Die verschiedenen Weisen des 'Um-zu', wie Dienlichkeit, Beiträglichkeit, Verwendbarkeit, Handlichkeit konstituieren eine Zeugganzheit. In der Struktur des 'Um-zu' liegt der Verweis von etwas auf etwas."²) Das Zeug ist also Mittel zum Zweck. Jegliche Bedeutung darüber hinaus verstellt diesen Zweck und läßt das Mittel selbst zum Zweck werden. Dies läßt sich etwa beim Auto zeigen: Für manchen Autobesitzer ist das Auto nicht (Fortbewegungs-) Mittel, sondern Statussymbol. Es nimmt einen zentralen Platz in seinem Leben ein und der Verlust des Autos führt nicht selten zu existenziellen Krisen, die sogar einen Selbstmord auslösen können.

"Fertigsein des Zeugs heißt, daß dieses über sich selbst hinweg entlassen ist, in der Dienlichkeit aufzugehen."³) Dort, wo das Zeug nicht

mehr nur-dienlich ist, ist es auch nicht mehr Zeug. Daran ist nun der Computer zu messen.

Welche Rolle und welcher Stellenwert wurden dem Computer (oder allgemeiner: der Datenverarbeitung) in unserer Gesellschaft zugewiesen? Hilft er uns, Probleme zu lösen, oder verschärft er nicht vielmehr bereits bestehende Probleme? Nach I. Illich¹ "definieren wir uns durch die Grundstruktur der Werkzeuge, die wir verwenden": in welcher Form hat uns der Computer verändert?

Der Computer verhindert die lebendige Erneuerung erstarrter Strukturen

Bevor ich nun versuche, die Struktur des Computers und die Auswirkungen, die sein Einsatz in allen menschlichen Lebensbereichen hat, zu analysieren, um von daher beantworten zu können, ob der Computer ein Zeug, ein Mittel zum Zweck ist, muß ich mich doch fragen, ob ich mich hier nicht weltfremd mit unrealistischen Spekulationen abgebe. Eine Kritik, die sich folgendermaßen äußert: "Ende des 20. Jahrhunderts hat sich nun einmal die Diskussion pro und contra Computer erledigt. Die digitale Maschine ist ein Faktum. Wir müssen damit leben, und das einzige, worüber wir uns Gedanken machen sollten, ist, wie wir am besten damit leben."⁴

Eines ist gewiß, gäbe es plötzlich keine Computer mehr, so würde wohl unsere Zivilisation zusammenbrechen, so sehr ist die Datenverarbeitung bereits in alle Lebensbereiche eingedrungen: wir sind momentan ohne Computer nicht lebensfähig. 1976 hat Joseph Weizenbaum diese Situation noch sehr milde beschrieben: "Der Computer wird zum unentbehrlichen Bestandteil jeder Struktur, sobald er so total in die Struktur integriert ist, so eingesponnen in die verschiedensten lebenswichtigen Substrukturen, daß er nicht mehr herausgenommen werden kann, ohne unweigerlich die Gesamtstruktur zu schädigen."⁵ Daraus könnte nun irrtümlich die Schlußfolgerung abgeleitet werden, daß wir ohne die Erfindung des Computers schon längst zugrundegegangen wären, oder doch große Einbußen unseres Lebensstandards hätten hinnehmen müssen. Ohne auf die Frage einzugehen, auf wessen Kosten wir in unserer Gesellschaft diesen sogenannten 'hohen Lebensstandard' erreicht haben, würde ich eher das Gegenteil vermuten. Denn vieles spricht dafür, daß unser Leben ohne Datenverarbeitungstechnik menschlicher/menschengerechter gestaltet sein könnte.

Der Computer wurde - und wird - dort eingesetzt, wo eine Struktur so komplex geworden ist, daß sie uns (als Individuum oder als Gruppe) überfordert. Hier kann diese Struktur durch den Einsatz von Datenverarbeitung 'gerettet' oder

sogar weiter ausgebaut werden. Ohne Computer wäre es notwendig, diese Struktur zu verändern, umzugestalten. "Dann hätte vielleicht der Anreiz, der durch die Unfähigkeit der Militärs geschaffen wurde, mit der wachsenden Komplexität der Luftkriegsführung in den 50er Jahren fertig zu werden, nicht mehr darin bestanden, nach Techniken zu suchen, mit denen das Militär seine traditionellen Aufgaben gerecht werden könnte, sondern neue menschliche Organisationen mit neuen Aufgaben zu erfinden, und zwar in Bezug auf die grundsätzlichere Frage, wie nämlich Völker mit unterschiedlichen Interessen miteinander auskommen können.⁵ In allen anderen menschlichen Lebensbereichen könnten ähnliche Beispiele angeführt werden, wie durch den Computer verhindert wird, daß Strukturen, die uns zu entgleiten drohen, in neue, lebendige Strukturen umgewandelt werden. Ich möchte dabei besonders auf den Zusammenhang zwischen *Komplexität* und *menschengerecht* hinweisen: Wenn eine soziale Struktur, also eine Struktur, an der Menschen beteiligt sind, in ihrer Komplexität menschliches Fassungsvermögen übersteigt, so muß sie entweder umgeformt werden, oder es werden Hilfsmittel zur Bewältigung dieser Komplexität verwendet (z.B. ein Computersystem). Diesem 'Hilfsmittel' muß nun die Kontrolle über diese Struktur überantwortet werden, und damit wird auch die Verantwortung abgegeben. Das bedeutet, daß die Gestaltung (d.h. lebendige Verwirklichung und Veränderung) dieser Struktur sich den in ihr lebenden Menschen entzieht und auf den Computer übergeht. "(Denn) der Mensch, der das Problem seiner Verantwortung blindlings auf die Maschine abwälzt, sei sie nun lernfähig oder nicht, streut seine Verantwortung in alle Winde und wird sie auf den Schwingen des Sturmwindes zurückkommen sehen."⁶

Der Computer beherrscht die, die ihn verwenden, ebenso wie die, die von ihm verwendet werden

Ich möchte nun die Rolle und den Stellenwert des Computers in unserer Gesellschaft und die Veränderungen, die er - z.B. in der zwischenmenschlichen Kommunikation - bewirkt, von der Struktur des Computers her untersuchen.

Der Computer verändert die Daten, die ich ihm gebe (Eingabedaten) zu anderen Daten, die ich wiederum von ihm zurückerhalte (Ausgabedaten). Diese Veränderungen vollzieht er nach genau festgelegten Regeln (Programm oder Befehlssatz).

Mit diesen kurzen Angaben habe ich im wesentlichen die Funktionsweise und Struktur eines Computers beschrieben. Auffallend ist hier die Ähnlichkeit mit militärischen Strukturen. So läßt sich auch die hervorragende Eignung des Computers in der Militärtechnik oder in ähnlichen Institutionen erklären. Umgekehrt ist der Computer eine Entwicklung der Rüstungsindustrie, denn vielleicht mehr noch als für andere Hochtechnologien gilt für die Datenverarbeitung, daß die Forschung überwiegend - direkt oder indirekt - von der Rüstungsindustrie finanziert wird.

Welche Auswirkungen hat nun diese Struktur des Computers auf die Verwendung eines Computers?

In der Datenverarbeitung gibt es den Begriff 'Schnittstelle'. Er bezieht sich dort auf jene Bereiche von zwei Systemen, wo sie miteinander verbunden sind (ungebräuchlicher, aber anschaulicher ist die umgekehrte Betrachtungsweise, nach der die Schnittstelle jener Bereich eines Systems ist, wo dieses in zwei *vollständige* (Sub-)Systeme unterteilt werden kann.). An dieser Stelle müssen diese beiden System aneinander angepaßt werden.

Andererseits gilt für zwei Menschen, die miteinander kommunizieren wollen, daß sie eine gemeinsame Basis brauchen - das kann die gemeinsame Sprache sein, ein

gemeinsamer kultureller Hintergrund oder Erlebnishorizont, ...

Bei der Verwendung eines Gerätes handelt es sich nun eigentlich um eine Mischform: auf der einen Seite ein Mensch, auf der anderen Seite ein System. Auch für diese Mischform gilt, daß Mensch und Gerät in der Verwendung aneinander angepaßt sein müssen (genauer: *aufeinander hin* angepaßt sein müssen). Bezüglich der strukturellen Anpassung sind aber Computer völlig starr, ihre Struktur, wie ich sie oben kurz skizziert habe, ist unveränderlich. Daher muß sich der Mensch, der einen Computer verwendet, strukturell an ihn anpassen, und dies umso mehr, je besser er ihn beherrschen will: er muß ebenso in Regeln denken und befehlen bzw. Befehlen gehorchen. Dabei wird ihn der Computer in *dieser* Hinsicht unterstützen und *diese* seine 'Fähigkeiten' verstärken. Also: je besser ich meinen Computer beherrschen will, desto mehr muß ich mich ihm unterwerfen.

Weshalb hat nun diese Anpassung beim Computer so starke Auswirkungen auf den Menschen?

Bei einer mechanischen Maschine beschränkt sich diese Anpassung vor allem auf körperliche Eigenschaften. Andere Eigenschaften (geistige, seelische,...) werden entweder unterdrückt oder bleiben unberücksichtigt, sofern sie sich nicht 'störend' auf die Tätigkeit auswirken. Anpassung an einen Computer beinhaltet nun auch die geistigen Fähigkeiten - die allerdings auf kognitive reduziert werden. Unterdrückt wird dabei die emotionale Ebene.

So bewirkt der Computer eine starke Einbindung und Anpassung des Menschen an ihn, durch die er der Freiheit seines Mensch-Seins beraubt wird. Er verhält sich wie eine Maschine - er wird zur Maschine. Seine Fähigkeiten werden verwendet - nicht mehr er kann darüber 'verfügen'. Eine Unterdrückung läßt immer noch die Chance zu einer Rebellion offen, oder zumindest die Schaffung 'illegaler' Freiräume. Aber in der Verwendung des Computers akzeptiere ich die 'Spielregeln', die diese Anpassung (Unterwerfung) beinhalten; diese Unterwerfung erfolgt also ebenso *freiwillig* wie die Verwen-

dung des Computers (nicht selten wird diese Verwendung aber aufgezwungen).

Ich habe mich hier nur mit dem Verhältnis Benutzer/Bediener beschäftigt. Ebenso werden natürlich auch die Betroffenen einer Computerverwendung von der Struktur des Computers erfasst: Jedes technische Gerät hat starken Einfluß auf die mit ihm ausgeführte Tätigkeit. Somit erstreckt sich der (strukturelle) Einfluß (z.B. Befehlscharakter) auch auf das 'Objekt' der Tätigkeit. Das gilt eben aus diesen strukturellen Gründen nicht nur für Systeme wie etwa ein Polizeiinformationssystem, sondern auch für *alle* anderen Computerverwendungen.

Der Computer macht jeden Menschen in seiner Umgebung zu seinem Subsystem

Ich will nun veranschaulichen, weshalb der Computer immer als System und nicht als Gerät existiert; als System, das die Menschen in seinem Wirkungskreis zu seinen Systemteilen reduziert. Das kann ich am besten anhand der Veränderungen zeigen, die ein Computer in seinem Wirkungsbereich (z.B. Arbeitsplatz, privater Bereich) mit sich bringt, und der Form der Verwendung, die dabei entsteht.

Die Situation vor einer Computerverwendung ist meist die, daß es mehrere Arbeitsbereiche gibt, die oft nicht klar voneinander getrennt sind oder lose miteinander verknüpft sind. Seine Struktur erhält der Arbeitsplatz erst durch mich, der ich in diesem Bereich verschiedene Tätigkeiten ausführe. Ich verwende dabei auch verschiedene Mittel, angefangen von Schreibgeräten bis hin zum Telefon. Auch für diese Geräte ist es charakteristisch, daß sie nur über mich miteinander verbunden sind.

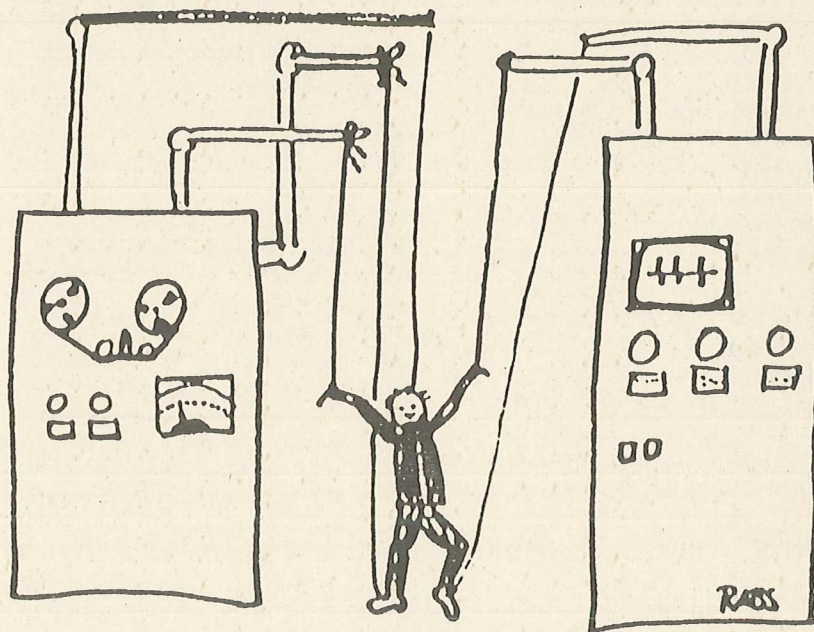
Wie sehr ich meine Tätigkeiten nach fixen Regeln ausführe, liegt an mir, ebenso, wie starr mein Tätigkeitsbereich ist, ob ich verschiedene Tätigkeiten flexibel ändere usf. Aber der Arbeitsbereich ist erst durch mich und ohne mich ist er nur eine mehr oder weniger zusammenhang-

lose Ansammlung von verschiedenen Utensilien. Soll jetzt in diesem Bereich ein Computer eingesetzt werden, so müssen verschiedene Voraussetzungen erfüllt werden, denn der Computer hat bestimmte Anforderungen an den Bereich, in dem er arbeiten soll. Dabei möchte ich grundsätzliche Anforderungen, die durch die Struktur des Computers bestimmt sind, von solchen unterscheiden, die durch die speziell verwendete Software (Anwendungsprogramme) bedingt sind. Häufig wird es sich aber dabei um fertige Softwarepakete handeln, die nur noch geringen Gestaltungsspielraum für den Benutzer übriglassen (vor allem Parameterfestlegung).

Welche Tätigkeiten (oder Teile davon) kann der Computer über-

Algorithmisiert bedeutet (u.a.) Formalisierung, und diese beinhaltet Normierung, weitgehende Fixierung und Ausschluß von Mehrdeutigkeiten.

Nun müssen diese Tätigkeiten in algorithmische und andere Teile getrennt werden, oder nicht-algorithmisierbare Teile werden entfernt. Die Verbindungen zwischen diesen, dem Computer zu übergebenden, und den anderen Teilen werden festgelegt. Da der Computer ein Datenverarbeitungsgerät ist, müssen die realen Situationen, die bearbeitet werden, an dieser Schnittstelle auf Objekte und deren Wechselbeziehungen reduziert werden, und diese Objekte und Informationen werden zu Daten reduziert. Diese Daten haben lediglich bestimmte Formate und Typen, eine



ICH BIN HIER DER CHEF!

nehmen? Das erfordert zuerst eine grundlegende Analyse des gesamten Tätigkeitsbereiches. Der Computer kann nur solche Prozesse bearbeiten, die seiner Struktur angepaßt sind (das sind regelgeleitete oder *algorithmisierte* Prozesse): daher müssen die verschiedenen Tätigkeiten auf algorithmische oder zumindest algorithmisierbare Bereiche untersucht werden.

bestimmte Anzahl von 'Eigenschaften' (Parametern) und sind eine diskrete Abbildung (Reduktion, Modell) dieser Objekte und Informationen. All dies erfordert eine grundlegende Umstrukturierung des gesamten Tätigkeitsbereiches einschließlich der Funktionen, die der Mensch nun in diesem Bereich zu erfüllen hat. Der Arbeitsbereich wird zu einem klar definierten System mit verschiedenen Kompo-

nenten (Moduln), mit klar definierten Schnittstellen, auch (oder vor allem) zum Menschen hin.

Ich bin somit Teil des Systems, dessen Zentrum der Computer ist. Lag das Zentrum also zuerst im Menschen, bestimmte der zuvor seinen Arbeitsbereich, so liegt das Zentrum, die Kontrolle nun im Computer.

Die Delegation der Verantwortung an den Computer

Diese Veränderungen, die durch die Verwendung von Datenverarbeitung bewirkt werden, haben natürlich weitreichende Konsequenzen. Ich will mich hier auf den Aspekt der *Verantwortung* beschränken. Wer handelt? Wer trägt die Verantwortung für dieses Handeln?

Bis jetzt habe ich versucht, zu veranschaulichen, wie in einem (lokalen) Bereich durch die Verwendung eines Computers die Macht und damit die Verantwortung für die Tätigkeit in diesem Bereich an den Computer übergeben wird. Denn, Macht beinhaltet Verantwortung, und ohne Macht gibt es auch keine Verantwortung.

Doch in größeren Dimensionen, bei Managern größerer Konzerne, beim Militär - ist es dort nicht so, daß der Computer als Werk-(Denk)zeug verwendet wird, um deren Interessen durchzusetzen? Gibt es nicht hier noch *persönliche* Verantwortung, Menschen, die entscheiden und die für diese Entscheidungen zur Verantwortung gezogen werden können?

Günther Anders bezieht zu diesen Frage sehr eindeutig Stellung: "... wir haben uns als die Subjekte der Geschichte entthront (oder entthronen lassen) und an unseren Platz andere Subjekte der Geschichte, nein: ein einzelnes Subjekt gesetzt: die Technik ...".⁷ Diese Behauptung will ich nun anhand der Verwendung der Datenverarbeitung unterstützen und bestätigen.

Der Mensch ist in quantitativer Hinsicht beschränkt, sowohl in seinen rezeptiven als auch in seinen aktiven Fähigkeiten (Arnold Gehlen spricht sogar vom *Mängelwesen Mensch*). Mit Hilfe der Technik versucht der Mensch nun, diese

'Beschränktheit' (allerdings um den Preis der Abhängigkeit von der Technik) zu überwinden: schneller, stärker, ... sind die Komparative, die diese Versuche kennzeichnen; ebenso der Wunsch, die Abhängigkeit von Zeit und Raum zu sprengen, also die Distanzen in räumlicher und zeitlichen Hinsicht mit technischen Mitteln so weit wie möglich zu eliminieren.

Technische Hilfsmittel, die den Menschen in quantitativer Hinsicht (bedeutend) übertreffen, *sind* Subjekte in dem Sinn, daß der sie 'verwendende' Mensch ihnen Aufgaben überträgt, die seine Fähigkeiten, die Ausführung dieser Aufgaben 'geistig' nachzuvollziehen und seine Konsequenzen abzuschätzen, übersteigt. Für solche von technischen Systemen durchgeführte Handlungen gilt, daß der Mensch mit der Auslösung der Handlung (z.B. der Inbetriebnahme von Datenverarbeitungssystemen) auch die Verantwortung dem technischen System übertragen hat.

Ich möchte das an einem Beispiel veranschaulichen: Bei Prozessen, bei denen die Zeit für Handlungsentscheidungen unter ein menschenmögliches Maß gesunken ist (z.B. Fertigungsprozesse, bei denen beim Auftreten von Fehlern in Sekunden schnelle entschieden werden muß, oder militärische Frühwarnsysteme, bei denen die Interpretation der empfangenen Daten und die damit verbundenen Entscheidungen, etwa über Vergeltungsschläge, im Minuten- oder gar Sekundenbereich liegen), muß die Entscheidung bereits vor dem Auslösen der Primärhandlung - also der Handlung, innerhalb der dann Entscheidungen getroffen werden müssen, die jenseits der menschenmöglichen Grenze liegen - getroffen oder delegiert werden.

Getroffen wird die Entscheidung dort, wo es lediglich einige klar begrenzte Entscheidungsmöglichkeiten gibt.

Delegiert wird die Entscheidung und mit ihr gleichzeitig die Verantwortung dort, wo es unvorhersehbare Möglichkeiten gibt, also überall dort, wo es sich um Handlungen in der realen Welt handelt - und in irgendeiner Weise haben wohl alle eingesetzten Computersysteme mit der Realität zu tun.

Delegation der Verantwortung bedeutet auch Delegation der Macht. Den Menschen bleibt die Bedienung der technischen Entscheidungsträger in der Form, daß sie deren 'fehlerloses' Funktionieren und deren Sicherheit (z.B. gegen terroristische Anschläge) zu gewährleisten versuchen. Diese Menschen begeben sich in eine (zum Teil lebensbedrohliche) Abhängigkeit von diesen technischen 'Objekten'. Die wahren Subjekte unserer Gesellschaft (im Sinne von *autonom*) sind damit diese technischen Systeme. Wir Menschen sind deren Bediener und von ihnen Beherrschte.

Computer sind also (von ihrer Struktur her) in *jeglicher* Form der Verwendung (sowohl im Kleinen als auch im Großen) Subjekte der Macht, die die Menschen zu beherrschten und angepaßten *Objekten* reduzieren. Ob sich diese 'Objekte' dieser Tatsache bewußt sind, ist zweifelhaft - das widerspricht dem Wesen des 'Objekt-Seins'.

Sicher ist diese Veränderung nicht erst durch den Computer entstanden. Aber die Datenverarbeitung hat diese Entwicklung in dramatischer Weise verschärft. Martin Heidegger⁸ hat diese Entwicklung schon 1949(!) beschrieben und als Hoffnung Hölderlin zitiert:

Wo aber Gefahr ist, wächst
Das Rettende auch.

¹ Ivan Illich: 'Selbstbegrenzung', Rowohlt Hamburg 1980

² Martin Heidegger: Sein und Zeit, Klostermann Tübingen 1984

³ Martin Heidegger: Der Ursprung des Kunstwerkes, Reclam Stuttgart 1960

⁴ Oberösterreichische Nachrichten, 27. November 1987

⁵ Joseph Weizenbaum: Die Macht der Computer und die Ohnmacht der Vernunft, stw Frankfurt 1977

⁶ Norbert Wiener: Mensch und Maschine, Berlin 1964

⁷ Günther Anders: Die Antiquiertheit des Menschen, Bd. 2, Über die Zerstörung des Lebens im Zeitalter der dritten technischen Revolution, Beck München 1980

⁸ Martin Heidegger: Die Technik und die Kehre, Neske Pfullingen 1962

(Bernhard Steiner ist Diplom-Ingenieur in Rofleithen, Österreich)

JESSI im Kontext

Ein Beispiel für Großindustrie-Subventionen und verdeckte Rüstungs-Haushalte

von Manfred Domke

Die Weiterentwicklung der Siliziumtechnik in Europa ist für die Wettbewerbsfähigkeit Europas von zentraler Bedeutung, so heißt es im Zukunftskonzept Informationstechnik der Bundesregierung (S. 88). JESSI (Joint European Submicron Silicon), ein Acht-Milliarden-Projekt (1990-1996) der Länder Frankreich, England, Italien, Niederlande und Bundesrepublik (Anteil ca. 2,8 Milliarden DM), zielt auf die Sicherung einer eigenständigen Position Europas bei der Basistechnologie Mikroelektronik. "Im Rahmen von JESSI muß den Chip-Anwendern in aller Breite die Nutzung der technologischen Möglichkeiten eröffnet werden."

Im folgenden sollen die Interessen, die mit diesem Programm verknüpft sind, näher betrachtet werden.

Das JESSI-Programm

Das komplexe Forschungs- und Entwicklungsprogramm von JESSI ist in vier Teile gegliedert¹:

- Der **Technologieteil** umfaßt 41 % des JESSI-Haushalts. Die Zielsetzung besteht in der wettbewerbsfähigen Herstellung von Chips mit Anschlüssen von 0,3 Mikron und 64 Millionen Informationseinheiten pro Speicherchip. "Der zukünftige Markt erfordert dies."
- Im Teil **Geräte und Materialien** (Equipment, 13 %) sollen die beiden nächsten Generationen von Chip-Herstellungstechniken entwickelt werden.
- Der **Anwendungsteil** (32 %) zielt auf ASIC-Chips (Application Specific Integrated Circuit), die den spezifischen Bedürfnissen der Benutzer angepaßt sind, und

auf CAD-Werkzeuge für die Entwicklung von chip systems.

- Im vierten Teil (14 %) geht es um die Stärkung der **Grundlagenforschung** für die 3 genannten Teilbereiche im Vorfeld der industriellen Entwicklung. Dazu gehört auch der Aufbau neuer Forschungskapazitäten.

Das Bundesministerium für Forschung und Technologie (BMFT) und das Land Schleswig-Holstein wollen im Rahmen von JESSI in Itzehoe ein Institut für Silizium-Technologie mit 400 Millionen DM fördern. Das Institut soll von einem europäischen Konsortium großer Firmen wie z.B. Siemens und Philips betrieben und genutzt werden. Unter einem Dach sollen Grundlagenforschung ($\frac{2}{3}$) und anwendungsorientierte Forschungsarbeiten ($\frac{1}{3}$) durchgeführt werden.

Die JESSI Initiatoren

Initiiert wurde JESSI 1986 zunächst von Siemens und Philips (Niederlande), später kam auch SGS-Thomson (Frankreich) hinzu. Heute ist JESSI ein Eureka-Projekt, erhält aber auch ESPRIT II- und BMFT-Fördergelder. Das BMFT hat für die gesamte Laufzeit des Programms bis 1996 ca. 1 Milliarde DM Fördermittel eingeplant.

SGS-Thomson ist ein Konzern französischer und italienischer Firmen. Das französische Rüstungsunternehmen Thomson-CSF stellt als **viertgrößte Elektronik-Firmengruppe** der Welt große Verteidigungs- und Infrastruktur-Systeme für den militärischen Einsatz zu Land, im Wasser und in der Luft her. Umfangreiche Erfahrungen existieren auf den Gebieten Radartechnik, Sonartechnik, Optoelektronik

und Kommunikationstechnik. Systeme von Thomson befinden sich heute weltweit im Einsatz. Die Fähigkeiten des Unternehmens reichen von der Grundlagenforschung bis zur Herstellung operationeller Geräte für die Ausrüstung moderner Streitkräfte, und zwar unter Verwendung eigener - und somit ohne Einschränkung verfügbarer - Schlüsselkomponenten². Die Thomson-CSF, **weltweit zweitgrößter Hersteller von Rüstungselektronik**, strebt über die Kooperation bei bestimmten Waffentypen hinaus eine engere Zusammenarbeit mit europäischen Partnerfirmen an, z.B. mit Siemens³.

Siemens hat ein Programm für Verteidigungselektronik. Die Entwicklung elektronischer Bauelemente gehört dazu.

Siemens und General Electric (GEC) haben inzwischen Plessey übernommen. GEC ist einer der weltweit führenden Hersteller in der **Rüstungselektronik**. Plessey ist ein weitgefächter Konzern für Telekommunikation, Elektronik und Luftfahrt. Seine **besondere Stärke liegt im Rüstungsgeschäft**. Die Übernahme von Plessey ist Teil einer breit angelegten Zusammenarbeit zwischen GEC und Siemens in der **Verteidigungselektronik** und Telekommunikation. Sie wird als Vorbereitung für den geplanten europäischen Binnenmarkt deklariert⁴.

Philips International NV geht den entgegengesetzten Weg und ist dabei, seine Rüstungselektronik-Anteile abzustößen. Der Konzern verhandelt gerade über einen Transfer seiner Rüstungsaktivitäten an Thomson-CSF. Laut Philips geschieht dies im Interesse der europäischen Integration und der Konzentration der europäischen

Rüstungsindustrie. Verhandelt wird über die von Philips gehaltenen Anteile an Hollandse Signaalapparaten NV (radar and fire-control systems, military equipment and networks, and command and control systems), MBLE (Belgien), TRT (Frankreich)⁵ und Usfa (Niederlande) mit Ausnahme deren Bereich Verschlüsselungstechnik⁶.

Philips gehört neben Thomson und Siemens zu den großen Chip-Produzenten in Europa. Mit dem Mega-Projekt haben Philips und Siemens technologisch Anschluß an die führenden japanischen Unternehmen gewonnen. Philips ist zusammen mit Thomson, Bosch und Thorn EMI (Großbritannien) führend im Eureka-Projekt HDTV (high-definition television, Großbildfernsehen). Die militärischen Interessen an HDTV liegen vor allem in den extremen Gewichts- und Raum-Anforderungen an Bildschirme für Flugzeug- und Panzer-Führer sowie Kommandozentralen. Thorn EMI Electronics setzt im Bereich Militärtechnologie ("battlefield sensors, radar and communications, sonar, airborne-surveillance and missile-guidance systems, and bomb fuses") jährlich etwa 470 Millionen US-Dollar um⁷. Es wird erwartet, daß HDTV zu einem Zusammenwachsen der Fernseh-, Computer- und Telephon-Industrien führen wird, was einen qualitativen Sprung in der technologischen Entwicklung bedeuten würde.

Am JESSI-Geschäft beteiligen sich u.a. auch folgende Firmen aus der Rüstungsszene: Daimler-Benz, AEG, Telefunken, Bosch, Alcatel, Matra, Plessey, Selenia.

"Die Hersteller werden die ersten Anwender sein", sagte Prof. Junne (Universität Amsterdam) vor dem Ausschuß für Forschung und Technologie zu JESSI⁸.

Die Dual-Use-Technologie Mikroelektronik

Im Zukunftskonzept Informationstechnik⁹ wird die wachsende Rolle der Informationstechnik für das Militär beschrieben. **Militärische Anforderungen** sollen künftig ver-

stärkt schon bei der Entstehung neuer Informations-Technologien berücksichtigt werden. Das bedeutet, daß zivile Informationstechnik künftig sogar **gewollt** militärische Elemente enthält.

"Die Informationstechnik spielt für die Verteidigung eine wachsende Rolle. ... Die Bundeswehr versucht, den Anteil der spezifisch militärischen Informationstechnik möglichst gering zu halten und sich weitgehend auf Entwicklungen für

den zivilen Bereich abzustützen. Dies gilt insbesondere für die Bereiche Führungs- und Informationssysteme sowie Mikroelektronik. ... In Zukunft wird auch verstärkt darauf hinzuwirken sein, sogenannte Dual-Use-Technologien intensiver zu nutzen, d.h. zu versuchen, **militärische Forderungen bei zivilen Entwicklungen frühzeitig mitberücksichtigen zu lassen.** ... Aus der Analyse dieser Gesamtaspekte lassen sich ... u.a. folgende für die Bundeswehr notwendigen Grundla-

Ausschuß

Eindrücke von der Anhörung "Zukunftskonzept Informationstechnik - Forschungs- und industriepolitischer Handlungsbedarf für eine Weiterentwicklung der Informationstechnik unter Berücksichtigung der internationalen Zusammenarbeit" im Ausschuß für Forschung und Technologie des Deutschen Bundestags am 13. Dezember 1989

- Die Großindustrie hat die Forschungs- und Technologiepolitik zur Informationstechnik fest im Griff. Vertreter der kleinen und mittleren Unternehmen, der Wissenschaft und Gewerkschaft spielen nur die Rolle von Statisten. Das Motto lautet: Die Gesellschaft als 'Testbett' für die Informationstechnik nutzen. Die Technik als Hilfsmittel zur Reduzierung drängender gesellschaftlicher Probleme wird nicht debattiert.

Entsprechend orientieren sich auch alle Ansätze zur Technologie-Folgen-Forschung an den Interessen der großen Industrie. Handlungsbedarf wird in einer verstärkten Abstimmung der langfristigen Forschungs- und Entwicklungsprogramme des BMVg mit dem Zukunftskonzept gesehen. Innovative Beschaffungen der öffentlichen Hand sollen zuerst die informationstechnische Industrie stärken.

- Der Ausschuß für Forschung und Technologie ist kein adäquates Kontrollgremium für die Forschungs- und Technologiepolitik der Bundesregierung. Die fünf bis sieben Abgeordneten der Opposition sind trotz redlicher Mühe restlos überfordert, die vorgeschlagenen Milliarden-Programme der Industrie zu durchschauen, angemessen zu bewerten und zu diskutieren. Diese Anhörung war eine reine Alibiveranstaltung.

- Die Leerformel "Internationaler Wettbewerb" öffnet als Universal-schlüssel die öffentlichen Förderkassen und dient unhinterfragt zur Legitimation weiterer wirtschaftlicher Machtkonzentration über nationale Grenzen hinaus. Der technologische Wettlauf zwischen Japan, den USA und Europa wird von Seiten der Politik als gegeben und notwendig begriffen, obwohl faktisch kooperiert und arbeitsteilig geforscht und entwickelt wird.

- WissenschaftlerInnen aller Fachrichtungen, Parteien, Gewerkschaften, Kirchen, Medien, Schulen, Frauenbewegung, Bürgerinitiativen sind aufgerufen, sich künftig mehr mit der Forschungs- und Technologiepolitik zu befassen und sich in sie einzumischen, weil "die Informationstechnik wie kaum eine andere technische Entwicklung zu tiefgreifenden strukturellen Veränderungen in allen Lebensbereichen führt" (Riesenhuber). Neue demokratischere und pluralistische Entscheidungsstrukturen für die Festlegung von Forschungs- und Entwicklungsschwerpunkten sind dringend erforderlich.

(Manfred Domke und Helga Genrich, FIFF-Regionalgruppe, Bonn)

gen auf dem Sektor der Verfahren/Techniken definieren, auf denen, aufbauend auf bestehenden zivilen Ergebnissen, ressortspezifische Ausprägungen notwendig sind: **Mikroelektronik, Bildverarbeitung, Computer Aided Engineering, Software-Engineering, Rechnerstrukturen, Kommunikationstechnik, Künstliche Intelligenz.** Die genannten Teilgebiete stellen langfristige **Schwerpunkte des Bundesministers der Verteidigung** im Rahmen der Informationstechnik dar ... wichtige Teilgebiete militärischer Aufgaben ..., für deren technische Lösung der Einsatz und die Weiterentwicklung der Informationstechnik unabdingbar sind. Hierzu gehören

- Aufklärung ...,
- Kommunikation ...,
- Führung ...,
- Waffensysteme, die eine verstärkte Automatisierung der komplexen Teilsysteme beinhalten und eine Erhöhung der Intelligenz erfordern.

Diese Teilbereiche sollen verdeutlichen, daß der Beitrag der Informationstechnik zur Verteidigungsfähigkeit der Bundeswehr in seiner Bedeutung noch steigen wird.
(Hervorhebungen durch den Verfasser dieses Papieres)

Fragen zur militärischen Verwendbarkeit der JESSI-Produkte

- Sollen die JESSI-Chips so entwickelt werden, daß sie auch in feindlicher Umgebung, im Kampf, zuverlässig arbeiten? Werden im Rahmen von JESSI gehärtete Chips entwickelt?
- Wird im Rahmen von JESSI **Fertigungstechnologie** so entwickelt, daß die Chips den militärischen Zuverlässigkeits-Anforderungen in Kampfsituationen genügen? Wenn ja, soll diese JESSI-Technologie auch den USA zu Verfügung stehen? Wenn nein, in welchem anderen Rahmen wird die Fertigungstechnologie für militärisch zuverlässige Chips entwickelt?

Prof. Heuberger (Fraunhofer-Institut für Mikrostrukturtechnik Berlin) unterstrich in der oben erwähnten Anhörung, daß aus finan-

ziellen Gründen in JESSI militärische Anforderungen nicht berücksichtigt würden, obwohl die Verteidigungstechnik von der Mikroelektronik abhängig sei. Dagegen würde das amerikanische SEMATECH "brutal unter den Prämissen der Verteidigung" stehen.

JESSI und SEMATECH

SEMATECH (Semiconductor Manufacturing Technology Institute) ist ein vom Department of Defense (DoD) und der Industrie gebildetes Konsortium, in dem AT&T und IBM treibende Kräfte sind¹⁰ und das in 1990 über ca. 100 Millionen US-Dollar verfügen soll. Ein Ziel von SEMATECH ist die Entwicklung von hochgradig zuverlässigen Produktionsmitteln.

Noch ist SEMATECH den Europäern verschlossen, aber nicht-europäischen Partnern wird schon die Mitarbeit in JESSI angeboten. Bieten die Europäer Firmen wie IBM Deutschland eine Mitarbeit in JESSI an, um den Einstieg in SEMATECH zu schaffen?¹¹

Heuberger und Weinerth (Philips Hamburg) bestätigten in der Anhörung vom 13. Dezember 1989, daß es über IBM zu einer Kooperation zwischen JESSI und SEMATECH kommen werde, insbesondere auf dem "Equipment-Gebiet".

Wiegt der strategische Wert einer Kooperation bei der Entwicklung militärisch relevanter Technologien eventuelle Wettbewerbsnachteile auf? Viele amerikanische und japanische Experten beantworten diese Frage mit "ja".

Im MMST (Microelectronics Manufacturing Science and Technology) - Programm, das von DARPA (Defense Advanced Research Projects Agency) und U.S. Air Force gefördert wird, soll eine futuristische papier- und menschenlose Produktionstechnologie für militärische ASIC - Chips entwickelt werden¹³.

Im Pentagon bestehen offensichtlich Zweifel an der Fähigkeit der US-Industrie, eine Spezial-Fertigungstechnologie für Chips entwickeln zu können, die den besonderen Zuverlässigkeits-Anforderungen in feindlicher Umgebung genügen:¹⁴

"Microelectronics technology encompasses a range of fabrication technologies used to manufacture miniaturized electronic devices mainly on silicon or gallium arsenide substrates. The components of microelectronics fabrication technology may be divided into the following categories:

- Wafer Preparation: ...
- Wafer Fabrication: ...
- Mask Making and Design: ... CAD design hardware and software ...
- Assembly and Test: ...
- **Radiation Hardening:** Hardening microelectronics against damage caused by high energy electrons, neutrons, protons, heavy particles, x-rays, and gamma radiation is vital to system performance in hostile radiation environments. Techniques used to accomplish that goal include special circuit designs, application of silicon-on-insulator (SOI) and silicon-on-sapphire (SOS) technology, and processing techniques to reduce radiation sensitivity of the silicon/silicon dioxide interface.

This fabrication technology has widespread use in both military and commercial applications, including computing, communications, and digital electronics. Many special manufacturing problems remain from a military point of view, however. The most important of them involves microcircuit reliability in hostile (i.e., combat) environments. **Reliability problems caused by hostile environments often demand specialized manufacturing solutions that may not be available from US industry.** Solving this problem remains a critical aspect of DoD fabrication efforts.

...

Important as microelectronics circuits are today, future weapons systems will rely even more so upon advances in their fabrication techniques. In addition, the ability to design and integrate new microelectronic components into weapons systems is an essential corollary to the device fabrication technology. **The success of our future defense posture relies in part on our ability to rapidly exploit advances in microfabrication technology at the**

systems level." (Hervorhebung durch den Verfasser)

Sollen die beiden Mikroelektronik-Initiativen JESSI und SEMATECH etwa verbunden werden, weil die USA nicht in der Lage sind, Fertigungstechnologien für Chips zu entwickeln, die auch in Kampfsituationen zuverlässig arbeiten?

Im Dezember 1989 soll in München (Standort des JESSI-Büros) mit den USA über Kooperationsmöglichkeiten bezüglich Standards, Universitätsprogramme, Geräte- und Materialprogramme beraten worden sein. Feststeht allerdings, daß ohne Zustimmung des amerikanischen Kongresses kein SEMATECH-Know-How nach Europa fließen wird¹⁵.

Befindet sich Europa nun mit JESSI im Wettbewerb mit den USA oder wird eine arbeitsteilige Kooperation mit SEMATECH angestrebt?

Diese Frage ist inzwischen beantwortet. Ende Januar 1990 beschloßen das JESSI-Board und die EG-Forschungsminister, die europäische IBM-Tochter zur JESSI-Mitarbeit einzuladen. Gleichzeitig wurde bekannt, daß Siemens und IBM die 64-Megabit-DRAM gemeinsam in USA entwickeln wollen. Der Forschungsbereich dynamische Speicherelemente (DRAM) soll nun aus JESSI herausgelöst werden. Nach der Chip-Kooperation von Siemens und IBM kommen nun auch JESSI und SEMATECH zusammen. Unter der Überschrift Bündnis gegen Japan heißt es in der WirtschaftsWoche: "Beide Initiativen wurden gegründet, um die Abhängigkeit von Japan zu verringern. Zusammenarbeit und Arbeitsteilung hätten sich schon lange angeboten. ... Die JESSI-Mitgliedschaft von IBM-Deutschland und die gemeinsame Entwicklung kommender Generationen hochintegrierter Speicherchips mit Siemens sind klare Indizien dafür, wie sehr das amerikanische Management auf das Können der Europäer baut."

Die Kooperationen im Rahmen von JESSI hielt Junne in der bereits zitierten Anhörung für die Eintrittskarte Europas in eine Kooperation mit den USA und Japan.

Welche Rolle spielt Japan?

Nach dem oben zitierten DoD-Plan für kritische Technologien ist Japan u.a. auf dem Gebiet Mikroelektronik (microelectronic circuits and their fabrication) den USA voraus. SEMATECH, die Semiconductor Research Corp. und U.S. Memories Inc. sollten den Rückstand der USA wieder wettmachen. Derartige Berichte sind allerdings mit Vorsicht zu genießen, wenn sie primär an den Kongress gerichtet sind. Die Bewilligung zusätzlicher Gelder steht dabei im Vordergrund. Das Buzzword 'Wettbewerb' wird von der Großindustrie in den USA und in Europa mit Erfolg als Vehikel zur Beschaffung öffentlicher Fördergelder benutzt.

Japan hat laut Chen¹² nach den Vereinigten Staaten und der Sowjetunion den drittgrößten Rüstungshaushalt der Welt, wenn die Pensionen einbezogen werden. Im Haushaltsjahr 1989 stieg der Etat um 5,9 % auf 27 Milliarden US-Dollar an. Für das Fiskaljahr 1990/91 haben Japans Streitkräfte eine Erhöhung ihres Etats um 6,35 % auf 4,16 Trillionen Yen oder umgerechnet 58,2 Millionen DM beantragt¹⁶. Die Forschungsaufwendungen sollen um 13,2 % auf umgerechnet rund 1,5 Milliarden DM steigen. Durch Kooperationsprojekte wird Rüstungstechnologie auch von Japan in die USA transferiert (Beispiel: F-16/FSX). Statt Lizenzverträgen ist heute ein Austausch von Technologien gefragt. Das generelle Waffenexportverbot Japans aus dem Jahr 1976, wurde 1983 durch eine Vereinbarung zwischen den USA und Japan eingeschränkt. Seitdem ist der Transfer von militärischem Know-How ausschließlich in die USA gestattet.

"In the project, Japan will develop on its own the avionics, including the active phased-array radar, inertial navigation system, integrated electronic warfare system, and mission computer hardware. U.S. companies will not participate in the avionics development, but results from the project will be available to them."

Japanese development of an efficient, reliable, and low-cost manufacturing method for gallium arse-

nide (GaAs) receiver-transmitter modules to be used in the active phased-array antenna would greatly interest the United States, but the method does not exist yet. ...

Because the semiconductor industry is vital to the defense, computer, and communications industries, it is just as vital to a nation's technology base. ...

Ironically, while Japan depends on the United States for military weapon systems and technology, some U.S. experts see increasing U.S. dependence on semiconductor technology from Japan.¹² (Hervorhebung durch den Verfasser)

Der JESSI-Initiator SGS-Thomson hat sich über die USA einen Weg nach Japan eröffnet. Im Jahr 1988 hat SGS-Thomson Microelectronics mit Standard Microsystems, Hauppauge, N.Y. einen Lizenzvertrag auf fünf Jahre mit dem Ziel abgeschlossen, für eigene Chips und Signalverarbeitungsprozessoren einen Zugang zum US-Markt zu schaffen. Über Toyo Corp., ein Joint Venture zwischen Standard Microsystems und Sumitomo Metal Industries Ltd., Tokio, hat Thomson auch Zugang nach Japan¹⁷.

Der internationale Wettbewerb entpuppt sich schließlich als Kooperation.

Merke:

- Dual-Use-Technologien sind nicht nur Technologien, die sowohl zivil als auch militärisch genutzt werden können. Viel wichtiger ist die Tatsache, daß bereits bei der Erforschung und Entwicklung neuer Technologien, die später auch zivil genutzt werden können, militärische Anforderungen berücksichtigt werden müssen.
- Ein Exportverbot für Waffensysteme kann durch den Verkauf von Dual-Use-Technologien umgangen werden. (vgl. auch Japan)
- Industriekooperationen einerseits, Forschungs- und Technologie-Politik andererseits sind gut aufeinander abgestimmt und zielen in erster Linie auf eine Stärkung der Rüstungsindustrie.

Wie ein Geheimdienst zur obersten Bundesbehörde für Computersicherheit gemacht wird

von Ute Bernhardt und Ingo Ruhmann

(In der FIFF KOMMUNIKATION 1/90 berichteten Ute Bernhardt und Ingo Ruhmann zum Thema Computersicherheit über die Zentralstelle für das Chiffrierwesen (ZfCh) und die Zentralstelle für Sicherheit in der Informationstechnik (ZSI). Im folgenden dokumentieren und kommentieren sie den Entwurf des geplanten Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI).)

"Nun, da die Gefahr der Bespitzelung aus dem früheren Ostblock gesunken ist, will sich die Bundesregierung offenbar auf die Sicherheitslücken im Inland konzentrieren". So beschreibt die Presse die Aufgaben der Zentralstelle für Sicherheit in der Informationstechnik (ZSI), die der Staatssekretär im Bundesinnenministerium (BMI), Neusel, am 6. Februar 1990 auf der Wissenschafts-Pressekonferenz vorstellte. Dabei bestätigte Neusel auch Dinge, die er vorher nur unter dem Siegel der Verschwiegenheit dem Innenausschuß des Bundestages anvertrauen mochte: daß nämlich die Bundesrepublik seit den fünfziger Jahren einen Chiffrier-Geheimdienst, die "Zentralstelle für das Chiffrierwesen (ZfCh) beim Bundesnachrichtendienst (BND)", hatte. Dieser Zentralstelle der "Codebreaker und Code-maker" (Neusel) wurde bereits 1987 der "Aufgabenbereich Computersicherheit übertragen". Mit Wirkung vom 1. Juni 1989 ist die ZfCh in die ZSI umgewandelt worden.

Die aus ihrer Herkunft resultierende organisatorische Verbindung der ZSI zum BND soll mit einem am 21. Februar 1990 vom Bundeskabinett verabschiedeten "Gesetz über die Errichtung des Bundes-

amtes für Sicherheit in der Informationstechnik (BSI)", das noch vor der Sommerpause durch den Bundestag gebracht werden soll, beendet werden. Aus der ZSI soll dann zum 1. Januar 1991 eine Bundesoberbehörde unter der Aufsicht des BMI werden. Doch auch mit dem weiteren Namenswechsel - von ZSI in BSI - endet die Verbindung zu den Geheimdiensten keineswegs, die ZSI wechselt nur den Partner der Zusammenarbeit. Im BMI hat die Abteilung IS 4 (Innere Sicherheit 4), zuständig für Geheimschutz und Sabotageschutz, Geheimschutzbeauftragter, nationale Sicherheitsbehörde (sprich: Bundesamt für Verfassungsschutz) die Fachaufsicht über die ZSI übernommen. Wegen ihrer Bedeutung wird die BSI ein eigenes Referat im BMI erhalten, was jedoch im gleichen Zuständigkeitsbereich liegen wird.

Wegen der vom BMI betriebenen Geheimniskrämerei war eine Vorstellung des ebenso umfangreichen wie erhellenden Aufgabenkataloges der ZSI von Neusels Pressekonferenz nicht zu erwarten. Grundlage des BSI-Gesetzes ist das "Rahmenkonzept zur Gewährleistung der Sicherheit bei Anwendung der Informationstechnik (IT) - IT-Sicherheitsrahmenkonzept", das vom Bundeskabinett am 23. November 1989 beschlossen wurde. Dieses Rahmenkonzept wurde vom "Interministeriellen Ausschuß für die Sicherheit in der Informationstechnik (ISIT)" entwickelt und vom darin federführenden BMI vorgelegt. Die im BSI-Gesetz genannten Oberbegriffe gehen auf dieses Rahmenkonzept zurück; das Rahmenkonzept ist der eigentliche und ausführliche Leitfaden der Arbeit der ZSI und des späteren BSI.

¹Eureka News, 19. Oktober 1989, S. 8 und Zukunftskonzept Informationstechnik, S. 88-89.

²Handbuch der Bundeswehr und der Verteidigungsindustrie, Bernhard&Graefe Verlag Koblenz, 1987/1988, S. 601.

³General Anzeiger vom 3. Juni 1989.

⁴General Anzeiger vom 18. November 1989.

⁵Does Europe need to concentrate its defense industry?, Electronics, October 1989, p. 44.

⁶Wehrtechnik 10/89, S. 25.

⁷Peter Fletcher, Thorn faces the music on defense unit, Electronics/July 1989, p. 36.

⁸Anhörung "Zukunftskonzept Informationstechnik - Forschungs- und industriepolitische Handlungsbedarf für eine Weiterentwicklung der Informationstechnik unter Berücksichtigung der internationalen Zusammenarbeit" am 13. Dezember 1989.

⁹Zukunftskonzept Informationstechnik, 10.2 Wehrtechnik und Landesverteidigung S. 120 ff

¹⁰vgl. Tobias Naegle, Why Sematech picked two technology drivers, Electronics, February 4, 1988, pp. 31-32.

¹¹"Will JESSI open its doors to U.S. companies?", Electronics, April 1989, p. 17.

¹²Katherine T. Chen, The state of Japan's military art, IEEE Spectrum September 1989, p. 29.

¹³Electronics/February 18, 1988, p. 108.

¹⁴The Department of Defense Critical Technologies Plan for the Committees On Armed Services United States Congress, 15 March 1989, p. A-3/4.

¹⁵Steven Dickman, 'JESSI enters critical phase', Nature, Vol. 341, 19 October 1989, p.559.

¹⁶WirtschaftsWoche Nr. 6 vom 2. Februar 1990 (S.135-138).

¹⁷Wehrtechnik 10/89, S. 45.

¹⁸Electronics, February 4, 1988, p. 142.

(Manfred Domke ist Mitglied der FIFF-Regionalgruppe Bonn)

Die Ziele der ZSI

Das IT-Sicherheitsrahmenkonzept der Bundesregierung hat als Ziel, Bedingungen festzulegen, um

- IT-Anwender in die Lage zu versetzen, system- und anwendungsbezogen Risikoanalysen zu erstellen und angemessene Sicherheitskonzepte zu entwickeln und zu realisieren,
- IT-Systeme/-Komponenten mit einem ausreichenden Sicherheitsstandard zur Verfügung zu stellen,
- die internationale Wettbewerbsfähigkeit deutscher/europäischer IT-Hersteller unter dem Aspekt eines hohen Sicherheitsstandards zu stärken.

Das Sicherheitsinteresse

Ausgerichtet sind die Sicherheitskriterien des Rahmenkonzeptes am sogenannten öffentlichen Sicherheitsinteresse, das definiert wird als Sicherheitsaspekte

- des Datenschutzes nach dem Bundesdatenschutzgesetz,
- der Wirtschaft und Wissenschaft,
- des staatlichen Geheimschutzes und
- der Verteidigung.

Die Frage, welche Sicherheitsaspekte hier Vorrang haben, läßt sich ohne große Mühen ableiten.

Der §6 des Bundesdatenschutzgesetzes (BDSG) verpflichtet den Bund wie auch die Wirtschaft, bei der Verarbeitung personenbezogener Daten Sicherheitsmaßnahmen zu ergreifen, die dem technischen Standard entsprechen. Die im Rahmenkonzept vorgestellten Sicherheitsmaßnahmen entsprechen jedoch weitgehend dem heute gebräuchlichen Stand der Technik. Nicht-personenbezogene Daten aus Kosten- oder aus anderen Gründen nicht dem Stand der Technik entsprechend zu schützen, ist eine Anwenderentscheidung. Schäden, die durch solche Sparmaßnahmen entstehen, werden auch nicht vom Gesetzgeber anerkannt: Die Hackerparagraphen gehen beim Hacken vom Eindringen in hinreichend geschützte Systeme aus.

Ungeschützte Systeme kann man nach juristischer Lehrmeinung nicht erhacken² und auch die Versicherungen, die gegen Computersabotage angeboten werden, werden Schäden bei ungeschützten Systemen nicht ersetzen.

In Wirtschaft und Wissenschaft ist der Aufwand der Datensicherheit eine Anwenderentscheidung, der Datenschutz schreibt den Stand der Technik als Maß für Sicherheitssysteme vor. Übrig bleibt vom "öffentlichen Sicherheitsinteresse", das das Rahmenkonzept für sich in Anspruch nimmt, also der staatliche Geheimschutz und die Verteidigung.

So sieht der GRÜNEN-MdB Manfred Such in der ZSI auch keinen "Beitrag zum Datenschutz und zur Verbesserung des informationellen Selbstbestimmungsrechts, sondern ein neues Amt mit Kompetenzen zur Kontrolle und Überwachung von BürgerInnen". Auch der Referatsleiter für Informationstechnik beim Bundesdatenschutzbeauftragten, Schmidt, bedauert, "daß die Beteiligung der nachrichtendienstlichen Zentralstelle für das Chiffrierwesen dann doch viel intensiver war als zunächst gewollt". Dies, so Schmidt, "liegt wie so vieles am Geld, das für die Aufgabe der Datensicherung zunächst nicht locker zu machen war, und am Fehlen anderweitig verfügbarer Experten". Unter diesen Umständen hält Schmidt das Konzept für "noch das beste, das erreichbar war".

Für welche Arbeit die ZSI im Bereich der öffentlichen Verwaltung zur Erhaltung des staatlichen Geheimschutzes geschaffen wurde und welche Einstellung zur Datensicherheit als lästigem Kostenfaktor dort bislang existiert, zeigt das Projekt PARLAKOM, die Vernetzung des Bundestages mit Datenverarbeitung. Trotz der Verarbeitung von hochsensiblen Informationen existiert bislang kein Datensicherheits- und Datenschutzkonzept³. Nicht nur Geheim-, sondern auch sensible Abgeordnetendaten werden dort bestenfalls - aber auch das nicht überall - mit einem Paßwort geschützt. DV-Experten bezeichnen diesen Umgang mit Daten übereinstimmend als fahrlässig. Die einzige Ausnahme stellt die Fraktion der GRÜNEN dar, die sich schon vor ihrer Beteiligung an PARLAKOM

von mehreren Beratergruppen ein Datenschutz- und Datensicherheitskonzept erarbeiten ließ.

Die Lage bei DV-Einführung und -Nutzung und damit auch der Sicherheit in den Bundesministerien, die vor allem vom preisgünstigen Einsatz von PCs ausgehen, bewertete der Haushaltsausschuß des Bundestages 1988 so, daß er eine vorübergehende 20%-ige Mittelsperre "wegen deren Konzeptionslosigkeit in der DV verhängte"⁴. Die ZSI soll nun das Auswärtige Amt als Pilotprojekt für ein sicheres Inhouse-Netz unterstützen, das zu einem Maßstab für die Umsetzung der "Richtlinien für den Einsatz der IT in der Bundesverwaltung" werden soll.

Die Sicherheitsinteressen der Verteidigung schließlich nimmt das Militär bereits selbst in die Hand. Die Abteilung Fernmeldetechnik und Elektronik (FE) des Bundesamtes für Wehrtechnik und Beschaffung (BWB) erarbeitet selbst - nur in "Abstimmung mit der ZSI" - "Grundlagen und Vorgaben für die Entwicklung von DV-Systemen und deren Software, sowie für die zugehörigen Prüfungen, Erprobungen und Evaluierungen"⁵. Die Bundeswehr setzt im Bereich der Rüstung also eigene Maßstäbe.

Die Aufgaben der ZSI

Trägt man alle Punkte zusammen, so hat die ZSI/BSI folgende Aufgaben:

- Analyse und Darstellung der Risiken bei der IT-Anwendung,
- Beratung in IT-Sicherheitsfragen,
- Entwicklung und Herausgabe von IT-Sicherheitskriterien,
- Prüfung von IT-Komponenten von Herstellern und - auf Antrag - bei und für Behörden,
- Zulassung von Systemen und Komponenten für den Einsatz in Behörden
- Entwicklung technischer Verfahren zur Sicherung der IT,
- Einwirkung auf und Begleitung von IT-Forschungsprogrammen,
- Einwirkung im Bereich nationale/internationale Normung,
- Zusammenarbeit im internationalen Bereich (EG, NATO),

Entwurf eines Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz, BSIG)

A. Zielsetzung

Viele Bereiche von Wirtschaft und Verwaltung sind bereits heute von dem einwandfreien Funktionieren der Informationstechnik abhängig. Mit dem zunehmenden Einsatz der Informationstechnik steigen auch die damit verbundenen Risiken durch unrichtige, unbefugt gesteuerte, fehlende oder rechtsgutgefährdende Informationen. Um die Verletzlichkeit der modernen Informationsgesellschaft zu begrenzen, muß bei der Entwicklung und dem Einsatz informationstechnischer Systeme oder Komponenten künftig die Sicherheit als gleichrangiges Ziel zu den Leistungszielen hinzukommen. Zu diesem Zweck sollen die Hersteller, Vertreiber und Anwender informationstechnischer Systeme oder Komponenten in Fragen der Sicherheit beraten und für geeignete Systeme oder Komponenten auf Antrag des Herstellers oder Vertreibers Sicherheitszertifikate vergeben werden. Neben Sicherheitsvorkehrungen in informationstechnischen Systemen oder Komponenten bedarf es - ergänzend oder alternativ - Sicherheitsvorkehrungen bei deren Anwendung.

Im übrigen müssen allgemein kriminell, extremistisch oder nachrichtendienstlich motivierte Einbrüche in informationstechnische Systeme rechtzeitig erkannt, ihre Auswirkungen bewertet und Möglichkeiten der sächlichen Beweisführung aufgezeigt werden. Zu diesem Zwecke soll für die Strafverfolgungs-, Polizei- und Verfassungsschutzbehörden des Bundes zentral der erforderliche Sachverstand bereitgestellt werden.

B. Lösung

Die schon bisher mit Fragen der Sicherheit in der Informationstechnik befaßte "Zentralstelle für Sicherheit in der Informationstechnik (ZSI)" - allerdings nur im Rahmen des staatlichen Geheimschutzes - soll künftig für alle sensitiven Anwendungsbereiche tätig werden, insbesondere auch für Zwecke des Datenschutzes. Nur sie verfügt bereits über die erforderlichen Erfahrungen und Kenntnisse sowie über das Fachpersonal und die Technik in diesem Aufgabengebiet. Als Behörde verfügt sie auch über die für die Wahrnehmung der Aufgabe erforderlichen Zugänge zu den staatlichen Sicherheitsinformationen.

Die vorgesehene Vergabe von Sicherheitszertifikaten stärkt auch die Wettbewerbsposition der auf dem deutschen Markt vertretenen Hersteller, soweit sie sich z.B. gegenüber US-Herstellern mit behördlichen US-Sicherheitszertifikaten international behaupten müssen.

Die neue Behörde ist zugleich dafür prädestiniert, die Strafverfolgungs-, Polizei und Verfassungsschutzbehörden mit ihrem Sachverstand zu unterstützen, soweit rechtswidrige Handlungen gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen.

C. Alternativen

Keine

D. Finanzielle Auswirkungen

...

Entwurf

Der Bundestag hat das folgende Gesetz beschlossen:

§ 1 Bundesamt für Sicherheit in der Informationstechnik

Der Bund errichtet das Bundesamt in der Informationstechnik als Bundesoberbehörde. Es untersteht dem Bundesminister des Innern.

§ 2 Begriffsbestimmungen

(1) Die Informationstechnik im Sinne dieses Gesetzes umfaßt alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen.

(2) Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen oder Komponenten oder
2. bei der Anwendung von informationstechnischen Systemen oder Komponenten.

§ 3 Aufgaben des Bundesamtes

Das Bundesamt hat zur Förderung der Sicherheit in der Informationstechnik folgende Aufgaben:

1. Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik, soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist,
2. Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten,
3. Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und Erteilung von Sicherheitszertifikaten,
4. Zulassung von informationstechnischen Systemen oder Komponenten, die im Bereich des Bundes oder bei Unternehmen im Rahmen von Aufträgen des Bundes für die Verarbeitung oder Übertragung amtlich geheimgehaltener Informationen (Verschlusssachen) eingesetzt werden sollen, sowie die Herstellung der Schlüsseldaten, die für den Betrieb zugelassener Verschlüsselungsgeräte benötigt werden,
5. Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen; soweit der Bundesbeauftragte für den Datenschutz unterstützt wird, geschieht dies im Rahmen der Unabhängigkeit, die ihm bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz zusteht,
6. Unterstützung der zuständigen Behörden des Bundes bei der Verhütung und Verfolgung von Straftaten sowie bei der Beobachtung der in § 3 Abs. 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes genannten Bestrebungen und Tätigkeiten, soweit dies erforderlich ist, um strafbare Handlungen, Bestrebungen oder Tätigkeiten, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen, zu verhindern oder zu erforschen,
7. allgemeine Beratung der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik.

§ 4 Sicherheitszertifikat

- (1) Hersteller und Vertreiber können für informationstechnische Systeme oder Komponenten bei dem Bundesamt ein Sicherheitszertifikat beantragen. Die Anträge werden in der zeitlichen Reihenfolge ihres Eingangs bearbeitet; hiervon kann abgewichen werden, wenn das Bundesamt wegen der Zahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an der Erteilung eines Sicherheitszertifikats ein öffentliches Interesse besteht. Der Antragsteller legt dem Bundesamt die Unterlagen vor und erteilt die Auskünfte, deren Kenntnis für die Prüfung und Bewertung des Systems oder der Komponente sowie für die Erteilung des Sicherheitszertifikats erforderlich ist.
- (2) Das Bundesamt kann im Einvernehmen mit dem Antragsteller sachverständige Stellen mit der Prüfung und Bewertung beauftragen.
- (3) Das Sicherheitszertifikat wird erteilt, wenn
 1. ein informationstechnisches System oder eine informationstechnische Komponente den vom Bundesamt festgelegten oder allgemein anerkannten Sicherheitskriterien entspricht und
 2. überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland der Erteilung nicht entgegenstehen.
- (4) Sicherheitszertifikate anderer anerkannter Prüfstellen aus dem Bereich der Europäischen Gemeinschaft werden vom Bundesamt anerkannt, soweit sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen.

§ 5 Ermächtigung

- (1) Der Bundesminister des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände durch Rechtsverordnung das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten nach § 4 und deren Inhalt.
- (2) Für Amtshandlungen nach diesem Gesetz und nach den zur Durchführung dieses Gesetzes erlassenen Rechtsverordnungen werden Gebühren und Auslagen erhoben. ...

§ 6 Änderung des Bundesbesoldungsgesetzes, Übergangsvorschrift

...

§ 7 Berlin-Klausel

...

§ 8 Inkrafttreten

Dieses Gesetz tritt am 1. Januar 1991 in Kraft

- Beratung bei Verbreitung bzw. Export von Sicherheitssystemen,
- Zusammenarbeit mit den Sicherheitsbehörden.

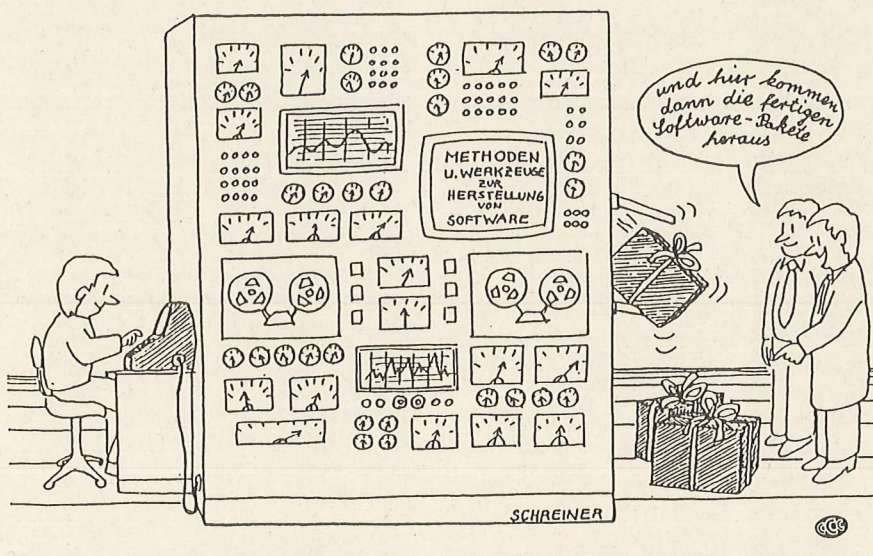
In der Aufklärung über Sicherheitsrisiken ist die ZSI bereits tätig geworden. Am 1. Juni 1989 veröffentlichte sie die IT-Sicherheitskriterien, eine "Fortentwicklung des in Fachkreisen bekannten "Orange Book" des US-amerikanischen Department of Defense (DoD)"⁶. Damit werden auch in der Bundesrepublik die Sicherheitsvorstellungen des Militärs zum Sicherheitsmaßstab im zivilen Bereich. Was für eine Organisation wie das Militär notwendig sein kann, ist in anderen Bereichen nicht ohne weiteres sinnvoll. Hierarchische Kommandostrukturen, die sich in der Datenweitergabe nach dem "need to know"-Prinzip niederschlagen, können kein Vorbild in einem demokratischen Rechtsstaat sein. Statt einer weiteren Militarisierung ziviler Bereiche wäre eine Trennung zwischen zivilen und militärischen Sicherheitsanforderungen notwendig.

Nach den IT-Sicherheitskriterien wird die ZSI/BSI Prüfungen von Produkten vornehmen und Sicherheitszertifikate vergeben. Die von ausländischen Anbietern geäußerten Befürchtungen, der Marktzugang werde über Sicherheitsfragen gesteuert, lassen sich nach § 4 des BSI-Gesetzes nicht von der Hand weisen. Die dort angeführten Veraberegelungen, die vom "öffentlichen Interesse" und "sicherheitspolitischen Belangen der Bundesrepublik Deutschland" abhängen, geben dem BSI ein neues marktpolitisches Instrumentarium. Geprüfte Produkte sollen nach Möglichkeit allen Anwendern zur Verfügung stehen, um so bei standardisierten Sicherheitssystemen die Voraussetzungen für hohe Stückzahlen und damit kostengünstige Lösungen zu schaffen. Es würde uns interessieren, seit wann im BMI standardisierte Sicherheitssysteme für besonders sicher gehalten werden.

Die mit den Prüfungen für Sicherheitszertifikate verbundenen Erwartungen dürfen allerdings nicht zu hoch angesetzt werden. Erstens gibt die ZSI zu, selbst mittelfristig nur beschränkte Kapazitäten zu Prüfungen

gen verfügbar zu haben. Zweitens muß nach den bisher bekannt gewordenen Kriterien das einem Stand-Alone-System erteilte Sicherheitszertifikat dann wieder aberkannt werden, wenn dieses System vernetzt wird. Drittens ist die Umsetzung der Sicherheitskriterien der ZSI auf die gebräuchlichsten Betriebssysteme nicht vor dem Jahr 2010 zu erwarten: "... bei Betriebssystemen wie MVS zum Beispiel,

Notstrom- und Wasserschutzmaßnahmen und zusätzlicher Backup-Kapazität auch Zutrittskontrollen, Verwendung vertrauenswürdiger Software, Maßnahmen gegen Diebstahl und Sicherheitsüberprüfungen von DV-Personal vor. Mit Kryptierverfahren für Software soll diese gegen Manipulationen gesichert werden, zwangsweise automatische Kryptierung von Datenübermittlungen soll diese gegen unerlaubten



(Hellmut Schreiner, Quelle: Cartoon-Caricature-Contor)

das auf die Mitte der sechziger Jahre zurückgeht, sowie bei BS2000 oder UNIX, die Ende der sechziger Jahre entstanden sind, ist so ein Modell allenfalls mit einem Aufwand von 12 bis 15 Jahren zu implementieren⁸. Damit dürften auch die mit diesen Betriebssystemen arbeitenden Rechner von BKA und Verfassungsschutz kein Sicherheitszertifikat erhalten. Trotz dieser Schwierigkeiten, die Grundlage der Sicherheit, das Betriebssystem, in den Griff zu kriegen, weitet die ZSI ihre Sicherheitsanalysen schon auf "die Sicherheit in Datenbanken und Expertensystemen"⁹ aus.

Die Sicherungsmaßnahmen

Als Sicherungsmaßnahmen sieht das Rahmenkonzept neben solchen Selbstverständlichkeiten wie Closed-Shop-Betrieb mit Brandschutz-,

Zugriff schützen. Paßwortschutz, z.T. mit Fingerabdruck als Authentifizierung, sowie die Protokollierung der Aktionen der DV-Benutzerinnen und -Benutzer sind ebenfalls vorgesehen. Alle im Rahmenkonzept vorgestellten Sicherheitsmaßnahmen sind nicht neu, sondern zumeist auf dem Markt verfügbar.

Nach § 3 BSI-Gesetz soll die BSI nicht nur Kryptiersysteme entwickeln, sondern auch die Schlüssel für diese Systeme an deren Benutzer vergeben. Wie schon in den USA mit der National Security Agency (NSA) geschehen, sollen auch hier die ehemaligen Code-Knacker die Verwalter der "sicheren" Codes werden. Diese Kontrolle über Codes und Schlüssel muß der ehemaligen ZfCh die Entschlüsselungsarbeit doch sehr erleichtern. Genausogut könnte man auch den Hackern die Verwaltung von Paßwörtern anvertrauen.

Eine weitere Aufgabe, die schon Innenminister Schäuble vorstellte, ist die Entwicklung "bestimmter technischer Sicherheitskomponenten". Die ZSI/BSI trägt die Kosten für Forschung und Entwicklung von Sicherheitskomponenten, deren Entwicklung im "öffentlichen Interesse" liegt. Entwicklungsaufträge darf die ZSI/BSI auch an andere vergeben. Damit erhält die ZSI/BSI im Sicherheitsbereich die Kontrolle über neue Forschungssubventionen. Die Herstellung der "allgemein" einzusetzenden Sicherheitskomponenten soll ausgewählten und auf ihre Zuverlässigkeit geprüften Firmen überantwortet werden.

Die ZSI/BSI legt auch die Richtlinien fest, nach denen Sicherheitsprodukte dem Geheimschutz unterliegen und nach denen diese Produkte exportiert werden dürfen.

Diese Sicherheitskonzepte und -produkte sollen, so Neusel, der Begrenzung der "Verletzlichkeit der modernen Informationsgesellschaft" dienen, da "andernfalls die Akzeptanz für die Informationstechnik gefährdet sei". Das IT-Sicherheitsrahmenkonzept nennt noch unterschiedliche Ausfallrisiken der DV:

- Defekte bei Hard- und Software bzw. der Infrastruktur,
- "höhere Gewalt" wie Blitz und Feuer,
- menschliches Versagen "(z.B. Fehlbedienung, Eingabe falscher Daten)",
- kriminelle Handlungen "(z.B. Computerkriminalität)".

Die in dieser Liste fehlende Abstrahlung von DV-Geräten wird an anderer Stelle angeführt.

Der seit 1974 amtierende Amtsleiter der ZfCh und jetzige Amtsleiter der ZSI, Leiberich, nennt den eigentlichen Grund für die Einrichtung der ZSI: "Wir haben es satt, uns immer von den Hackern überraschen zu lassen"¹⁰. Deswegen will er Sicherheitslücken in IT-Systemen "ermitteln und aufdecken - bis hin zur Skizzierung von theoretischen Angriffsmodellen". Hat denn Leiberich niemand gesagt, daß Hacken nichts mit Militärmanövern zu tun hat, sondern auf der Nutzung reicher praktischer Erfahrung beruht?

Während eine IBM-Studie die Häufigkeit des Eintretens von "Bedrohungen" der Informationstechnologie so beziffert, daß 54% von "normalen" Fehlern, 24% von Mitarbeitern, 17% von Feuer- und Wasserschäden und nur 3% von Externen herrühren¹¹, sind die Aufgaben der ZSI/BSI ausschließlich an der sogenannten Computerkriminalität ausgerichtet. Die Aufzählung von potentiellen Tätern läßt kein Feindbild-Klischee von Sicherheitsbeamten aus. Aufgezählt werden neben "kriminellen Insidern" nur noch "gegnerische Nachrichtendienste", "extremistische/terroristische Gruppierungen" und sogar das "organisierte Verbrechen".

Das Unvermögen, sich im BMI und anderswo neue, aus den Möglichkeiten der Informationstechnologie erwachsende Verbrechensformen - wie etwa solche, die die Löschung der Tat Spuren beinhalten¹² - vorzustellen, wird deutlich, wenn lediglich alte Verbrechensformen auf diese Technologie übertragen werden. So wird etwa als neue Form der "Datenerpresung" das Bitnapping erwartet¹³.

KGB-Hack

Diese fast ausschließlich auf Hacken als Grund eines DV-Ausfalls gerichtete Gewichtung der Risiken ist direkte Folge des inzwischen als "KGB-Hack" bekannt gewordenen Falles um vier Hacker, die Material an den KGB verkauft haben sollen, wobei nach Auffassung des Gerichts allerdings "kein nachweisbarer erheblicher Schaden für die Bundesrepublik und vermutlich auch nicht für NATO-Partnerländer entstanden" ist¹⁴.

Dieser Prozeß hat gezeigt, wie schwer die Beweisfindung in einem Hackerverfahren sein kann. Dies ist besonders für das BKA um so ärgerlicher, als dort parallel zur Einführung der "Hackerparagrafen" Kapazitäten für die Bekämpfung der "Computerkriminalität" aufgebaut werden sollten. Dafür seien nach Meinung eines BKA-Beamten "zentrale Spezialistenteams erforderlich, die die Ermitt-

lungsarbeit vor Ort unterstützen"¹⁵ - und mit dieser Zentrale war das BKA gemeint.

Um eine Wiederholung dieser und anderer Rückschläge der Sicherheitsbehörden zu vermeiden, soll mit der ZSI/BSI eine fachlich hinreichend qualifizierte Organisation geschaffen werden, die im Bedarfsfall allen Behörden des Sicherheitsbereichs - wie aus dem BMI zu hören war - zur "Bekämpfung von kriminellen oder verfassungsfeindlichen Aktivitäten, die gegen die Informationstechnik gerichtet sind oder unter deren Nutzung erfolgen" zur Verfügung steht. Damit soll die ZSI/BSI zur zentralen Anlaufstelle in Fragen der Computerkriminalität für Polizei und Verfassungsschutz werden.

Der Rekurs des BSI-Gesetzes auf den § 3 Bundesverfassungsschutzgesetz ist äußerst aufschlußreich. Die ZSI/BSI wird so unterstützen des Organ für alle Tätigkeiten des Verfassungsschutzes, bei denen Informationstechnik genutzt wird. Jetzt könnten z.B. Mailboxen auf deren - verfassungskonformen - Inhalt mit Hilfe der ZSI/BSI geprüft und überwacht werden.

Eine derartige Zentralisierung von Kompetenzen bei der Verbrechensbekämpfung ist in der Bundesrepublik nicht einmal mit dem Ausbau des BKA bei der Terrorismusbekämpfung zu vergleichen. Mangels fachlicher Kompetenz anderer Behörden ist die ZSI/BSI von der Software-Raubkopie über Hacken zu verschiedenen Zwecken bis zur Spionage für alles zuständig, was mit unbefugter Computernutzung zu tun hat. Die ZSI/BSI wird so zur Spezial-Eingreiftruppe für Computersicherheit.

Bewertung

Zentrum der Aufgaben der ZSI und ab 1991 des BSI bilden die Sicherheitsinteressen der Organisationen des Bundes, insbesondere die der Geheimdienste, des Militärs und der Polizei. Während die Bundeswehr eigene Standards entwickelt, werden für Wirtschaft und Verwaltung die vom US-Militär entwickelten Sicherheitskriterien vorgeschrie-

ben. Diese weitere Militarisierung von zivilen Bereichen ist weder sinnvoll noch hinnehmbar.

Das von der Bundesregierung für die ZSI definierte Ziel, mehr Sicherheit in der Informationstechnik zu schaffen, kann die ZSI auch mittelfristig nicht wirksam erfüllen. Die für die ZSI an zentraler Stelle stehende Aufgabe der Bekämpfung von Hackern und Computerkriminalität kann auch sie technisch kaum lösen. Um so wichtiger wird daher ihre Zusammenarbeit mit Polizei und Verfassungsschutz.

Die ZSI garantiert also nicht mehr Sicherheit, sondern mehr Sicherung im DV-Bereich - Sicherung vor den DV-BenutzerInnen. Zutrittskontrollen und Sicherheitsüberprüfungen von DV-Fachleuten und -BenutzerInnen müssen als Ersatz für die technisch und erst recht wirtschaftlich nicht herzustellende, aber gewünschte Sicherheit von DV-Systemen herhalten. Zutrittskontrollen gibt es mittlerweile an Uni-Rechenzentren¹⁶, Sicherheitsüberwachungen nehmen ständig zu: die Firma Siemens will, wie zu hören war, bis vor das Bundesarbeitsgericht ziehen, um die Zulässigkeit derartiger Überprüfungen ihrer Mitarbeiterinnen und Mitarbeiter klären zu lassen. In einem derartigen Klima der Hackerfurcht wird jeder neue Hackerfall strengere Sicherheitsrichtlinien nach sich ziehen, die immer mehr Individualrechte aller DV-BenutzerInnen den Sicherheitsinteressen der DV-Anwender unterordnen.

Nicht nur der Datenschützer Schmidt konstatiert, daß das Interesse der DV-Anwender vor allem darin besteht, möglichst kostengünstige Lösungen zu erhalten. Es kann ja wohl nicht wahr sein, daß den Sparwünschen der DV-Anwender zuliebe Individualrechte der BenutzerInnen, also letztlich der gesamten Gesellschaft, abgebaut werden.

Der Begriff der "Verletzlichkeit der Informationsgesellschaft", den Neusel anführt, bedeutet eben nicht allein die Sicherung des Funktionierens der Informationstechnik. Dieser Begriff ist vielmehr ein Synonym für unsere selbstverschuldete Abhängigkeit von einer Technik, deren Ausfall zum Teil lebensbedrohende Gefahren in sich birgt, ohne daß auf dem Weg dorthin

einmal über die Risiken nachgedacht worden wäre. Die einzige Lösung ist nicht die Sicherung unsicherer Systeme, sondern die Suche nach Alternativen, die den Technologieinsatz nicht auf Kosten unserer Freiheitsrechte betreiben.

Wie unterschiedlich unser Staat die Schutzinteressen der Bürgerinnen und Bürger und seine eigenen bewertet, zeigt allein die Aufzählung der Anwendungsbereiche für Sicherheit in der Informationstechnik: während die ZSI/BSI für sich in Anspruch nimmt, nicht nur Daten-, sondern auch Bild-, Sprach- und Textübermittlungen zu sichern, wird gerade dem Datenschutz mit dem Hinweis auf rechtssystematische Gründe¹⁷ die Erweiterung auf Bild- und Sprachverarbeitung verweigert.

Die ZSI/BSI hat Aufgaben in der Forschung und Entwicklung, der Normung, in der Kooperation mit Polizei und Geheimdiensten, in der Zusammenarbeit mit dem Militär und selbst in der Kontrolle über Exporte von Sicherheitssystemen. Eine derartige Konzentration von Aufgaben bei einer Behörde, die von den Interessen des staatlichen Geheimschutzes angetrieben wird, ist eine nicht hinnehmbare Machtzusammenballung in der Hand einer staatlichen Institution. Eine solche Behörde erst unter Ausschluß der Öffentlichkeit zu schaffen und dann bis zur Sommerpause das nötige Gesetz durch den Bundestag zu peitschen, erweckt kein Vertrauen in die mit der ZSI/BSI verfolgten Absichten.

"Das neue Bundesamt soll weder eine militärische noch eine nachrichtendienstliche, sondern eine zivile Behörde werden". Diese schönen Worte Neusels mögen formal korrekt sein. In der ZSI/BSI werden jedoch Beamte und Soldaten aus einem Geheimdienst Sicherheitsüberprüfungen und Sicherheitssysteme nach militärischen Kriterien entwickeln und durchführen - all dies in Zusammenarbeit mit Polizei und Verfassungsschutz.

Es ist bekannt, daß Geheimdienste das Hacken als neue Spionageform nutzen¹⁸. Nach eigener Einschätzung ist die ZSI/BSI die einzige Stelle in der Bundesrepublik mit den dazu notwendigen Experten. Die von Leiberich angekündigten "theoretischen Angriffsmodelle"

müssen nicht notwendigerweise nur der Hackerabwehr dienen. Dies zeigt, daß Aufgaben und Ziele der ZSI/BSI noch sehr ausbaufähig sind.

Es ist nicht einzusehen, warum für die Sicherheit der Informationstechnik in der zivilen Verwaltung und Wirtschaft statt der ZSI/BSI keine zivile Behörde mit ausreichenden Forschungs-, Entwicklungs- und Beratungskapazitäten geschaffen wird. Im militärischen und nichtmilitärischen Geheimbereich mit seinen besonderen Sicherheitsbedürfnissen können dann ZSI/BSI und das Bundesamt für Wehrtechnik und Beschaffung ungestört ihre Konzepte entwickeln und vorschreiben.

Computersicherheit darf Militär und Geheimdiensten nicht überlassen werden, sondern gehört in die Hände von zivilen und demokratisch kontrollierbaren Organisationen. Computersysteme sind fehlerhaft und werden es bleiben. Für Computerfehler kann man keine Hacker zu Sündenböcken machen, sondern ausschließlich diejenigen, die uns durch ihre Risikoblindheit in eine gefährliche Abhängigkeit von informationstechnischen Systemen gebracht haben. Und das sind dieselben, die jetzt Sicherheit in der Informationstechnik verwechseln mit der Sicherung der Informationstechnik vor ihren BenutzerInnen.

¹ Rhein-Sieg-Anzeiger vom 7. Februar 1990

² vgl.: Armin Leicht: Computersabotage - Die "besondere Sicherung gegen unberechtigten Zugang" (§202a StGB); in: Informatik und Recht, 2/87, S. 45-53

³ PARLAKOM: Sicherheitsbedürfnis erst nach Beschaffung entdeckt; in: Bonner Behörden Spiegel/Beschaffung Spezial, September, 1989

⁴ ebd.

⁵ Abteilung "Fernmeldetechnik und Elektronik" (FE); in: Wehrtechnik, 1/90, S. 55-60, S. 58

⁶ ZSI: IT-Sicherheitskriterien, 1. Fassung vom 11. Januar 1989; im Bundesanzeiger vom 1. Juni 1989

⁷ Dieses Prinzip besagt, nur die Daten weiterzugeben, die der Empfänger für seine Aufgabenerfüllung unbedingt braucht. Dies entspricht nicht der Zweckbindung beim Datenschutz.

⁸ Angelika Schrader: EDV-Sicherheit; in: Office Management, 7-8/89, S. 30-32, S. 31

⁹ Bonner Behörden Spiegel/ Beschaffung Spezial: Januar: taktische Einsatzsysteme, Mai: Sicherheitskonferenz; Heft Januar 1990, S. B IX

¹⁰ Rhein-Sieg-Anzeiger vom 7. Februar 1990

¹¹ zitiert nach: Roßnagel, Wedde, Hammer: Die Verletzlichkeit der "Informationsgesellschaft", Opladen, 1989, S. 106

¹² der Ordnung halber sei hier angemerkt, daß derartige Löschen nach den Hackerparagrafen natürlich verboten ist

¹³ vgl. die Presserklärung Neusels am 6. Februar 1990

¹⁴ General-Anzeiger vom 16. Februar 1990

¹⁵ Manfred Klink, BKA: Computerkriminalität - Eine neue Herausforderung an die Polizei; in: Die Polizei Heft 2, 1987, S. 37-39, S. 39

¹⁶ vgl. die F!FF-Kommunikation 1/90 zum RZ der Uni Oldenburg

¹⁷ BT-Drucksache 11/2108 vom 13. April 88

¹⁸ Ingo Ruhmann: KGB-"khaker" und CIA-Viren; in: F!FF-Kommunikation, 3/89, S. 28-29

(Ute Bernhardt und Ingo Ruhmann betreuen gemeinsam die F!FF-Geschäftsstelle in Bonn.)

Zum "Zukunftskonzept Informationstechnik"

Zwei Stellungnahmen aus kritischer Wissenschaft und interessierter Industrie

(In der letzten Ausgabe der F!FF KOMMUNIKATION hatten wir unter dem Titel "(K)ein Konzept" eine Stellungnahme des F!FF zum Zukunftskonzept Informationstechnik des Bundesministers für Forschung und Technologie abgedruckt.

Im folgenden sollen zwei Stellungnahmen zum Thema gegenübergestellt werden. Die eine stammt von Prof. Dr.-Ing. Alexander Wittkowsky, Universität Bremen, Technikgestaltung, Technologieentwicklung, Fachbereich Produktionstechnik, November 1989, die andere - in Kontrast dazu abweichend gesetzt - von Dr.-Ing. Hans Gissel, Direktion Konzernforschung, Daimler Benz, November 1989.

Die Texte sind leicht gekürzt abgedruckt, jedoch mit z.T. veränderten Überschriften. An einigen Stellen wurde die Aufeinanderfolge der Textteile etwas geändert, um eine bessere Gegenüberstellung der beiden Stellungnahmen zu erreichen.)

Allgemeine Stellungnahme

Wittkowsky: Das Konzept beansprucht, den generellen Rahmen für staatliches Handeln zur Förderung der Informationstechnik aufzuspannen, von der überdies angenommen wird, sie führe zu "tiefgreifenden strukturellen Veränderungen in allen Lebensbereichen". Diese Absicht der Bundesregierung ist zu begrüßen, da hiermit die Beweggründe für die Förderpolitik und die auf viele Programme verteilten Förderungsmaßnahmen einer vergleichenden Bewertung zugänglich werden. Auch hätte ich politische Aussagen dazu erwartet, wie dem

abschbaren Wandel von Arbeit und gesellschaftlichem Leben begegnet werden soll. Schließlich hätte begründet werden müssen, warum angesichts anderer drängender Zukunftsprobleme, wie Armut oder Umweltzerstörung, jährlich ca. 1,7 Mrd. DM staatliche Mittel für die Unterstützung der Entwicklung der Informationstechnik (IT) ausgegeben werden müssen.

Gissel: Das Zukunftskonzept Informationstechnik, das die Bundesregierung am 6. Juni 1989 als Nachfolgeprogramm des "Regierungsberichtes Informationstechnik 1984 bis 1988" verabschiedet hat, zeigt, daß die außerordentliche Bedeutung der Informationstechnik für die Weiterentwicklung der gesamten Volkswirtschaft von der Bundesregierung anerkannt wird.

Dies wird besonders deutlich durch die Hinweise, daß bis zur Jahrtausendwende die informationstechnische Produktion und Dienstleistung in ihrem Volumen die Automobilindustrie überflügeln wird, und daß darüber hinaus bis dahin zwei Drittel aller Beschäftigten neue informationstechnische Arbeitsmittel nutzen werden.

Die Darstellung der Position der deutschen informationstechnischen Industrie zum Weltmarkt zeigt indes, daß die deutsche und auch die europäische Industrie nach wie vor unterproportional an diesem Markt beteiligt sind.

Trotz der erheblichen Anstrengungen, die aufgrund des "Regierungsberichtes Informationstechnik 1984 bis 1988" von allen Beteiligten unternommen wurden, hat sich die Situation der deutschen informationstechnischen Industrie im Verhältnis zum Weltmarkt nicht wesentlich zu ihren Gunsten verändert.

Es ist daher zu fragen, ob die in dem neuen Zukunftskonzept Informations-technik aufgeführten Maßnahmen geeignet sind, die bestehenden Defizite nachhaltig im kommenden Jahrzehnt auszugleichen.

Ganz generell ist zu sagen, daß die Stärkung der Forschung weiterhin notwendig ist. In sehr viel stärkerem Maße jedoch als bisher ist der Schwerpunkt auf die Entwicklung der Anwendungen zu legen. Dabei kommt der Nutzung der Informationstechnik zur Lösung öffentlicher Aufgaben eine besondere Bedeutung zu. Die in dem Zukunftskonzept Informationstechnik aufgezeichneten Maßnahmen können als gute Ansätze bezeichnet werden, die aber zur Erreichung des Zieles nicht ausreichen werden.

Es wird erwartet, daß die Liberalisierung der Telekommunikation durch die Bundesregierung einen wesentlichen Beitrag zu einer verstärkten Entwicklung auf diesem Gebiet liefert. Dabei ist es notwendig, daß zunehmend private Anwender zur Nutzung der im staatlichen Monopol verbleibenden Dienstleistungen (z.B. ISDN) angeregt werden.

Zu begrüßen ist die Absicht der Bundesregierung, durch eine Verbesserung der steuerlichen Rahmenbedingungen die Attraktivität des Standortes Bundesrepublik für die Unternehmen zu erhalten.

Die Initiative, die Durchführung des Zukunftskonzeptes durch einen begleitenden Fachausschuß aus Wissenschaft, Industrie und Behördenvertretern begleiten zu lassen, wird begrüßt.

Der Mensch als Bezugspunkt der Technikentwicklung fehlt

Wittkowsky: Wenn das ZKI eine Art von "technischer Revolution" erwartet, wäre es oberste staatliche Maxime zu fragen, wie und wohin sich diese Entwicklung im Interesse der Menschen in der Bundesrepublik - aber auch außerhalb bis hin zur Dritten Welt - steuern läßt. Die Leitkriterien wären am Menschenbild des Grundgesetzes, insbesondere an der Entfaltung der Grundrechte auch in der industriellen Arbeit, zu orientieren. Die - an dieselben Freiheitsrechte der anderen gebundene - freie Entfaltung der Persönlichkeit und das Recht auf

körperliche Unversehrtheit zählen ebenso dazu wie das Recht auf informationelle Selbstbestimmung, die Sicherung der persönlichen Entfaltung durch Teilhabe an Entscheidungsvorgängen und die Gleichberechtigung von Mann und Frau.

Die Entwicklung der Informationstechnik wäre dann daran zu messen, inwieweit sie Menschen dient, die privat und im Beruf zielbewußt und sinnvoll im Sinne von Selbstverwirklichung handeln wollen und z.B. am Arbeitsplatz ausreichende Handlungs- und Entscheidungsspielräume - also Autonomie - benötigen. Jede Technikentwicklung muß sich daran messen lassen, inwieweit sie Mitbestimmung ermöglicht und Demokratie auch am Arbeitsplatz fördert.

Für Anwendungen in der Dritten Welt wäre die Richtschnur, inwieweit die Übernahme deutscher Technikkonzepte kulturelle Eigenständigkeit unbeschadet läßt und die Lebensbedingungen vor allem der ärmsten Bevölkerungsmassen fördert, also sozial und kulturell "angepaßt" ist.

Ebenso wichtig wie Handlungsautonomie sind der Informationshorizont und die Auswahlmöglichkeiten, die dem Menschen eröffnet werden. Technikentwicklung in einer Demokratie muß davon ausgehen, daß ihre Bürger ein grundlegendes Bedürfnis haben, sich ein zusammenhängendes, sinnvolles Verständnis ihrer Umwelt anzueignen, sich mit ihren Lebens- und Arbeitsbedingungen auseinanderzusetzen und sie gestalten zu können. Menschengemäße Gestaltung des Einsatzes der Informationstechnik in der Produktion z.B. muß also sowohl den einzelnen Beschäftigten als auch das Sozialgefüge von Betrieb, Unternehmen und Volkswirtschaft betrachten und die jeweils Betroffenen beteiligen, ehe Entscheidungen getroffen werden. Die Gestaltungsfelder, aber auch die Wirkungsbereiche, bilden einen viel komplexeren Zusammenhang für den Entwicklungs- und Einführungsprozeß, als das ZKI unterstellt. So beeinflussen hardwareorientierte Entwicklungsmaßnahmen die Arbeitssituation genauso, wie wirtschaftspolitische Maßnahmen auf

die Produktionskonzeptionen durchschlagen. Und auf allen Ebenen gibt es Handelnde und Betroffene. Notwendig ist ein andersartiger Prozeß der Technikentwicklung als in der Vergangenheit (...).

Weder eine in diesem Sinne soziale "Verträglichkeit" der Informationstechnik noch überhaupt eine arbeits- oder bedürfnisorientierte Entwicklung der Informationstechnik spielen im ZKI eine Rolle. Dabei kann die Bundesrepublik auf eine bald fünfzehn Jahre währende Tradition menschengerechter Gestaltung von Produktionssystemen und menschlicher Arbeit zurückblicken. Auch in England gibt es schon in den fünfziger Jahren und in den skandinavischen Ländern seit den sechziger Jahren erfahrungsreiche Bemühungen um eine Verbesserung der "Quality of Working Life". Das ZKI reiht sich dagegen ein in die rein techniklastige Fehlentwicklung auf EG-Ebene, in deren F+E-Programmen Ansätze humaner Technikentwicklung ebenfalls fast vollständig fehlen. Es sieht simplifizierend und von gesellschaftlichen Verhältnissen abstrahierend die Entwicklung der IT ausschließlich von ökonomischen und technischen Imperativen bestimmt.

Handlungsbedarf bei der Grundlagenforschung

Gissel: Die hohe Bedeutung der Grundlagenforschung für die Informationstechnik wird in dem Zukunftskonzept richtig gesehen.

Diese Grundlagenforschung ist künftig gekennzeichnet durch ein immer stärkeres Zusammenwachsen von Spezialdisziplinen wie Halbleitertechnik, Künstliche Intelligenz, Mikrosystemtechnik, Systemtechnik etc. Darauf geht das Zukunftskonzept nicht genügend ein.

Die Grundlagenforschung auf dem Gebiet der Informationstechnik findet in der Bundesrepublik verteilt auf eine Vielzahl von Hochschulen und Institute im wesentlichen unkoordiniert und ohne ersichtliche wesentliche Zusammenarbeit statt. Eine bessere Koordination und Schwerpunktbildung ist unumgänglich für den Erfolg des Zukunftskonzeptes.

Zur schnelleren Umsetzung der Ergebnisse der Grundlagenforschung ist eine enge und zielgerichtete Zusammenarbeit von Grundlagenforschung und Industrie notwendig. Dies umso mehr, als die Industrie heute aus Wettbewerbsgründen gezwungen ist, in erheblichem Umfang Anwendungsforschung zu betreiben. Es sollten Modelle unterstützt werden, wie dieser Prozeß verbessert werden kann.

Die Verlegung von sehr anwendungsorientierter Forschung oder gar Entwicklungen in Forschungsinstitute kann nur als ein Fehlweg gesehen werden. Dies führt unweigerlich zu Doppelarbeit in Forschung und Industrie.

An dieser Stelle sollte auch darauf hingewiesen werden, daß die Technologieprogramme der EC, wie z.B. ESPRIT, zunehmend über den vorwettbewerblichen (Forschungs-)Rahmen in Richtung Vorentwicklung und Demonstratoren erweitert werden.

Die stärkere Einbindung der bestehenden Großforschungseinrichtungen in die Forschung auf dem Gebiet der Informationstechnik wird mit Skepsis gesehen und nur in den Fällen für zweckmäßig erachtet, wo Forschungsaufgaben einen hohen apparativen Aufwand voraussetzen. Die deutsche Industrie ist dennoch bereit, in den Kontrollgremien der Großforschungseinrichtungen an deren Neuausrichtung mitzuwirken, um die notwendige Flexibilität dieser Institute zu fördern. Eine direkte Trägerschaft und Finanzierung werden nicht als ein Ansatz gesehen, der neue Perspektiven der institutionellen Forschung aufzeigen könnte.

Handlungsbedarf bei der Entwicklung von Basistechnologien

Gissel: Es wird richtig gesehen, daß Innovationen bei informationstechnischen Produkten und Leistungen auf der Verfügbarkeit weiterentwickelter oder neuer Basistechnologien aufbauen.

Der Bericht zeigt, daß in Teilgebieten eine deutliche Schwäche in der Eigenversorgung besteht, z.B. bei der Mikroelektronik.

Zu diesen notwendigen Basistechnologien gehören indessen nicht nur hardwareorientierte Technologien.

Zunehmend gewinnen auch Softwaretechnologien und Systemtechnik an Bedeutung.

Die Anstrengungen, bisher versäumte Entwicklungen aus der Vergangenheit nachzuholen, wie z.B. mit JESSI, sind zu begrüßen (*Anmerkung der Redaktion: In dieser FIFF KOMMUNIKATION befindet sich ein eigener Artikel zum Thema JESSI*). Es erscheint indessen ganz wesentlich, neue Basistechnologien, wie die Mikrosystemtechnik und die Software- und Systemtechnik, rechtzeitig und vor allem in ausreichendem Maße zu unterstützen.

Bei der Informatik muß darauf hingewiesen werden, daß hier die Entwicklung der Basistechnologien sich nicht nur auf die Felder der parallelen Verarbeitung und Künstlichen Intelligenz beschränken darf. Auch für die Peripheriegeräte sind weitere Innovationen notwendig.

Schließlich sollte darauf geachtet werden, daß Fördervorhaben nicht durch Übernahme von Entwicklungen, die im Ausland durch entsprechende Regierungsprogramme unterstützt wurden, unterlaufen werden.

Weltmarkt als Zwangsjacke

Wittkowsky: Das ZKI übernimmt kritiklos das Argument, nur durch forcierte Aufwendungen für F + E könne die internationale Wettbewerbsfähigkeit der IT-herstellenden und -anwendenden Industrie gesichert werden. Die "Zwänge" des Weltmarktes und dessen Wachstumsbedingungen werden umstandslos mit der Brille eines bestimmten Sektors der Großindustrie betrachtet.

Es wird nicht geprüft, inwieweit gerade eine regionale Orientierung der Entwicklung der IT unterschiedliche Bedürfnisse berücksichtigen, Potentiale nutzen und ausbauen und zu einer Vielfalt von Innovationen führen könnte, die vor allem die Eigenständigkeit von Klein- und Mittelunternehmen (KMU) sichern und entfalten hilft. Schon heute sind viele kleinere Software-Häuser von Konzentration oder Untergang bedroht.

Handlungsbedarf bei der Entwicklung von Halbleiterfertigungstechniken

Gissel: Bei den Halbleiterfertigungstechniken ist heute die Abhängigkeit der deutschen Industrie vom Ausland groß. Es kommt dabei vor allem auf die rechtzeitige Verfügbarkeit von Fertigungs- und Prüfgeräten an. Diese scheint heute durch die vielfältige Verflechtung der ausländischen Hersteller mit der Halbleiterkonkurrenz nicht gewährleistet. Diese Situation wird in dem Bericht nicht genügend dargestellt. Das JESSI-Programm kann hier für die deutsche und europäische Industrie wesentliche Fortschritte auch in dieser kritischen Frage bringen.

Handlungsbedarf bei der Entwicklung von Rechnern

Gissel: Seit mehr als zwanzig Jahren bemüht sich die Bundesregierung darum, die Rechnertechnik in der Bundesrepublik Deutschland international konkurrenzfähig zu machen. Der Vergleich des Erreichten mit den ursprünglichen Zielen zeigt, daß der Erfolg der Programme recht begrenzt ist und die angestrebte Konkurrenzfähigkeit nur in einigen wenigen Teilgebieten erreicht werden konnte.

Dies rührt daher, daß die Abdeckung der hohen Entwicklungskosten auf diesem Gebiet nicht auf nationaler Basis möglich ist, sondern nur auf europäischer oder internationaler Basis, und daß eine Beschränkung der Förderungsmaßnahmen auf die vorwettbewerbliche Forschung und Entwicklung angesichts der Aufwendungen des internationalen Wettbewerbs nicht zum Erfolg führen kann.

Der Bericht zeigt leider noch keinen Wandel in der grundsätzlichen Ausrichtung der Förderungsmaßnahmen.

Die Förderung konzentriert sich auch heute noch auf technologische Spitzenleistungen, für die nur ein begrenzter Markt vorhanden ist. Dabei werden durch moderne Technologien mögliche neue Anwenderstrukturen, die zu einer weitgehend dezentralen Informationsverarbeitung führen, übergangen.

Auf dem Gebiet der Peripheriegeräte für Rechner ist die Abhängigkeit vom Ausland, insbesondere von den USA und Japan, teilweise noch viel größer

als bei den Rechnern selbst (Beispiel Laserdrucker). Hier könnte insbesondere eine europäische Zusammenarbeit wirksame Abhilfe schaffen und zwar durch Entwicklung und Anwendung durchaus anspruchsvoller Technologien.

Handlungsbedarf bei der Entwicklung von Anwender-techniken

Gissel: Über die Entwicklung einer international konkurrenzfähigen informationstechnischen Industrie hinaus hat die Anwendung der modernen Informationstechnik einen noch nachhaltigeren Einfluß auf die Entwicklung von Wirtschaft und Gesellschaft, wie dies im Bericht richtig dargestellt wird.

Durch die rasche Verfügbarkeit neuer informationstechnischer Produkte und Leistungen ergeben sich ständig erweiterte oder neue Anwendungsmöglichkeiten in vielen Bereichen, von der Fertigungsautomation bis hin zum Gesundheitswesen. Leider

werden diese Möglichkeiten wegen der mangelnden Vorbereitung durch die Anwender oft nur zögerlich angenommen. Dies zeigt sich in der von dem Bericht richtig konstatierten geringeren Dichte von Produkten und Systemen der Informationsverarbeitung in der Bundesrepublik verglichen mit Ländern wie USA, Japan und selbst UK.

Notwendig sind daher

- verstärkte Aus- und Weiterbildung,
- Förderung von anwendungsorientierten Unternehmen,
- verstärkte innovative öffentliche Anwendungsbeschaffung,
- weitere Entwicklung der Systemtechnik.

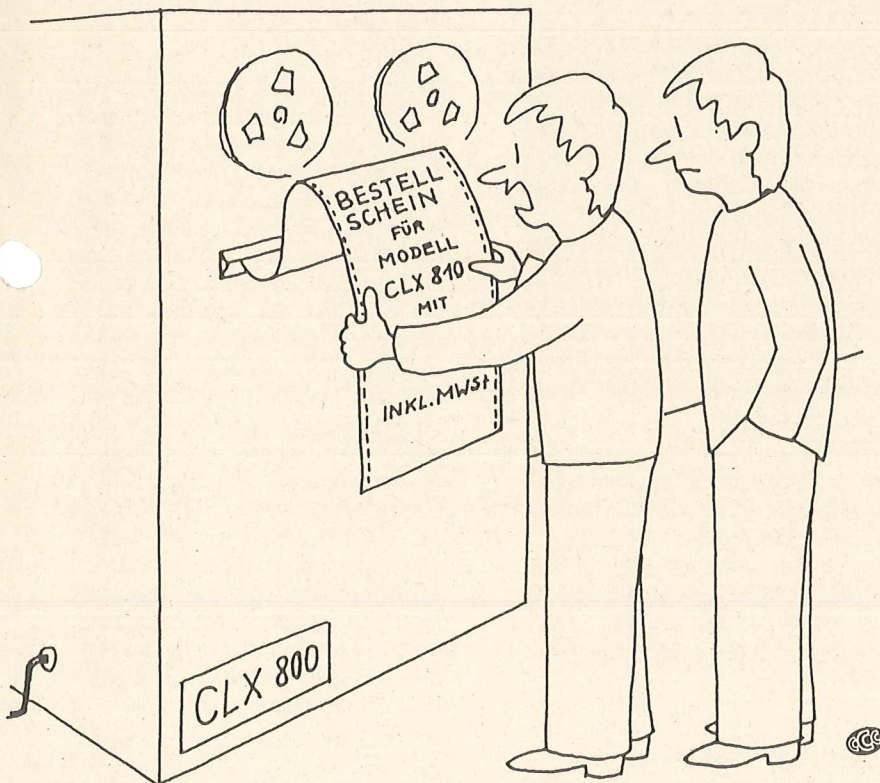
Die industrielle Automatisierungstechnik ist von herausragender Bedeutung für alle Industriezweige und ein wichtiger Faktor für den Export von Ausrüstungen und Anlagen. Diesem Anspruch wird das Zukunftskonzept nur unzureichend gerecht.

Zur Entwicklung und Durchsetzung von Normen

Wittkowsky: Im ZKI wird der Stellenwert der Normung betont, um "die Wettbewerbsbedingungen und die Angebotsstruktur auf dem Markt der Informationstechnik" im Sinne der deutschen Wirtschaft zu fördern. Maßgebend für die "Durchsetzungsfähigkeit nationaler Interessen" sei "die Wirtschaftskraft der im Normungsverfahren beteiligten Partner".

Die Argumentation des ZKI richtet sich vollkommen auf die Interessen der Großkonzerne aus, die Vorteile größerer Märkte zu nutzen. Andere Interessengruppen wie Verbraucher, Arbeitnehmer, Wissenschaftler oder auch kleine Betriebe werden kaum berücksichtigt. Diese haben aber, bedingt durch den europäischen Binnenmarkt '92 und die Internationalisierung der Normung, allein schon durch den immens hohen Abstimmungsaufwand, immer weniger Chancen, an der Entwicklung von Normen mitzuwirken. Dies wird zunehmend das Geschäft von Großkonzernen. Erschwerend kommt hinzu, daß die Innovationsraten im Bereich der IT noch sehr hoch sind und häufig von kleinen oder Kleinstbetrieben ausgehen. Eine vorzeitige Festschreibung von Normen im hier angenommenen Verfahren kann sehr leicht zum "Abwürgen" innovativer Ansätze führen.

Generell ist zu fragen, welche Normungsvorhaben uns als Konsumenten oder Arbeitnehmern nützen. Nutzt es den Konsumenten wirklich, wenn durch Normen "eine Zersplitterung der Märkte im Bereich der Unterhaltungselektronik-Industrie" vermieden wird? Zwar hätte dann weltweit (?) jeder Konsument jedes Programm verfügbar, die Eingebundenheit von Kultur in eine Region, in einen sozialen Zusammenhang ginge aber verloren, da regionale Programme kaum noch konkurrenzfähig wären, die überregionalen Programme sich zwangsläufig auf den kleinsten gemeinsamen Nenner des vermeintlich von den Konsumenten Gewünschten anpassen.



"stell Dir vor, er hat von sich aus bereits den Bestellschein für seinen Nachfolger ausgedruckt"

(Helmut Schreiner, Quelle: Cartoon-Caricatur-Contor)

Auch im Bereich CIM wird durch die ausschließliche Betonung von Schnittstellen-Normen der Kern der Frage, wie die Fabrik von morgen aussehen sollte, auf rein technologische Aspekte reduziert. Die bloße Integration von Daten nutzt nur in einer vollständig automatisierten Fabrik; sollen aber weiterhin Menschen in der Fabrik arbeiten - und dies ist meine Forderung -, so müssen vorrangig Arbeitsabläufe "integriert", also im Hinblick auf erfolgreiche zwischenmenschliche Kommunikation aufeinander abgestimmt werden und nicht Daten. Erst mit dieser Zielsetzung kann dann daran gegangen werden, die dieser "Integration" entgegenstehenden Schnittstellen durch Normung zu beseitigen.

Handlungsbedarf bei der Entwicklung von Kommunikationstechniken

Gissel: Es ist zu begrüßen, daß die Entwicklung eines europäischen HDTV-Standards unterstützt wird. Neben der Bedeutung für die Massenkommunikation ist darauf hinzuweisen, daß eine hochauflösende Darstellungstechnik auch in Terminals Platz greift. Dies darf nicht zu einer Zweigleisigkeit in den Standards führen.

Dominanz großtechnischer Vorstellungen

Wittkowsky: Das ZKI zeigt eine ausgeprägte Orientierung an großtechnischen und sehr kapitalintensiven Investitionen, wie an JESSI mit erwarteten öffentlichen Aufwendungen von mindestens 1 Mrd. DM oder am Ausbau des Kabelfernsehnetzes mit jährlichen Aufwendungen der Bundespost von 1,5 Mrd. DM, ohne daß hinreichend der öffentliche Nutzen im Verhältnis zu den Wirkungen auf die Arbeitswelt oder die Lebensbedingungen der Bevölkerung abgewogen wurde.

Der Hinweis auf einzelne Begleitforschungsprojekte kann die Bedenken gegen die weitreichenden ökonomischen und gesellschaftlichen Folgen nicht annähernd ausräumen. Auch hat das jähe Ende eines anderen, aus "Expertensicht" "wohlbegründeten" Großprojektes

(WAA Wackersdorf) gezeigt, wie unzureichend die Folgen analysiert und vorausbedacht waren. Es kann nicht hingenommen werden, wenn ein solches Vakuum durch sehr spezielle und stark interessengebundene Argumente gefüllt und gegenüber der (in Wackersdorf nachträglich in ihrem Widerstand gerechtfertigten) Bevölkerung einfach durchgesetzt wird.

Gissel: Die Informationstechnik ist auch als ein wesentlicher Faktor für die Bewältigung der Verkehrsproblematik nicht nur im nationalen Rahmen, sondern europaweit zu sehen (*PRO-METHEUS, Anmerkung der Redaktion*).

Ein weiterer wesentlicher Faktor im Anwendungsbereich ist die Verwendung offener Informationssysteme (OSI). Es ist zu begrüßen, daß sich die Bundesregierung hierfür einsetzen will. Offen ist allerdings, ob dies in der Praxis auch gerade vom öffentlichen Auftraggeber so gehandhabt wird. Hier scheint oft die Abstützung auf sog. Industriestandards als der einfachere Weg gesehen zu werden.

Es ist zu bedauern, daß die hochentwickelte Glasfaser- und Breitbandübertragungstechnik heute nicht in einem kostendeckenden Rahmen eingesetzt wird, da es an einer ausreichenden Anzahl passender Anwendungen fehlt. Daher sind Projekte wie BERKOM in Berlin zu begrüßen.

Für den Erfolg des ISDN ist es notwendig, daß die vielfältigen Möglichkeiten, die dieses System bietet, auch genutzt werden. Neue Anwendungen wie z.B. das Bildtelefon, sollten daher verstärkt weiterentwickelt und auch beschafft werden.

Die Öffnung der Mobilkommunikation für einen zweiten privaten Betreiber eines flächendeckenden digitalen zellularen Mobilfunknetzes ist zu begrüßen. Es erscheint wichtig, daß auf diesem Weg fortgeschritten wird und weitere Dienstleistungen im Mobilbereich privaten Anbietern zugänglich werden.

Handlungsbedarf bei der Entwicklung von Software

Gissel: Die deutsche Software-Branche ist, wie richtig im Zukunftskonzept festgestellt wird, heute gekennzeichnet durch eine weitgehende Zersplitterung

in kleine und kleinste Unternehmen und durch eine starke Anwendungsorientierung. Dies steht ganz im Gegensatz zu der Struktur und den Schwerpunkten dieser Branche in den USA und auch Ländern wie UK, wo die den Weltmarkt prägenden Softwareprodukte entwickelt werden.

Als Ursachen dafür sind neben den schwachen finanziellen Ressourcen die fehlende Kopplung mit bedeutenden Herstellern von Informationssystemen zu sehen. Hier Abhilfe zu schaffen ist eine Grundvoraussetzung für eine Stärkung der deutschen Software-Branche.

Die Unterstützung von Projekten zur Entwicklung leistungsfähiger Software-Entwicklungsumgebungen, wie z.B. dem EUREKA Projekt ESF, wird begrüßt. Das Vorhandensein derartiger Entwicklungssysteme ist Voraussetzung für eine wettbewerbsfähige Entwicklung von Software insbesondere im Anwendungsbereich und damit Existenzgrundlage für eine Vielzahl kleiner und mittlerer Firmen.

Bewertung des EUREKA Projektes JESSI

Gissel: Das JESSI-Programm ist ein konsequenter Schritt für die Entwicklung einer wettbewerbsfähigen Mikroelektronik in Europa. Der Vergleich mit anderen Ländern, z.B. USA mit dem Programm SEMATECH, zeigt, daß es nur mittels solcher Programme möglich ist, ausreichend Ressourcen zu bilden. Wegen der zunehmenden Bedeutung von ASICs für die Entwicklung neuer, wettbewerbsfähiger informationstechnischer Geräte und Systeme kommt dem dieser Technik gewidmeten Teil des JESSI-Programmes besondere Bedeutung zu. Die zur Entwicklung, Fertigung und Prüfung von ASICs notwendigen Methoden und Techniken sollten besonderes Gewicht erhalten. Auf die Bedeutung der Einrichtungen für Fertigung und Prüfung von Halbleitern, die im Rahmen JESSI entwickelt werden, wurde schon hingewiesen.

Die in der Studie Mikroelektronik 2000 zum Ausdruck gebrachte Strategie, parallel zueinander sowohl die Herstellungstechniken für hochintegrierte Mikroschaltkreise als auch die Anwendungstechnologien zu entwickeln, kommt in dem derzeit vorgese-

henen Ablauf von JESSI nicht genügend zur Geltung.

Das Technikverständnis ist traditionell

Wittkowsky: Das ZKI geht von einem überholten Verständnis technischer Entwicklung aus, das bereits von der Industrie selbst zunehmend in Frage gestellt wird. Danach wird Technik vor allem als Mittel für beliebige, gewinnversprechende Zwecke verstanden; Technik ersetzt zunehmend produktive, planende und dispositive Funktionen des Menschen und bestimmt die verbleibenden menschlichen Eingriffe und die dazu notwendigen Qualifikationen. Aber das damit verbundene Ideal der vollautomatisierten, möglichst menschenleeren Fabrik kontrastiert inzwischen mit der Einsicht, daß z.B. Produktionstechniken, die auf die Bedürfnisse der arbeitenden Menschen keine Rücksicht nehmen und deren Fertigkeiten und Fähigkeiten, aber auch deren Wertvorstellungen vernachlässigen, mittelfristig keine Zukunft haben.

Ein hiervon ausgehender, konsequent verfolgter alternativer Pfad von Technikentwicklung erfordert integrierte arbeits- und technikbezogene Entwicklungsansätze, die auch zur Konstruktion und Entwicklung veränderter Produktionsmittel und Produkte führen müssen. Solche Zukunftsalternativen sind im ZKI nicht einmal angedacht worden. Die Thematisierung des Verhältnisses von Arbeit und Technik wird der Wirkungsforschung und dem Programm "Arbeit und Technik" überlassen, obwohl sie in das Zentrum einer jeden Technikentwicklung gehört.

Das eingeschränkte Verständnis von Technikentwicklung im ZKI führt auch zu einer ausgeprägten Trennung von technischer Entwicklungsforschung und sozialwissenschaftlicher Technikforschung. Wenn aber die Wirkungen von IT sich vor allem im Zusammenspiel mit anderen technischen Innovationen (von der CNC-gesteuerten Hochgeschwindigkeitsschleifmaschine, über Hochgeschwindigkeitszüge bis hin zu neuen Kommunikationsmedien) entfalten, muß die Struktur

der Forschung dem entsprechen und ein neuer Typ von Entwicklungsforschung gefördert werden, der Interdisziplinarität schon im Entwicklungsprozeß selbst verankert.

Das Konzept ist mit demokratischer Beteiligung kaum vereinbar

Wittkowsky: Das ZKI läßt schließlich jeden Ansatz einer Bürgerbeteiligung an der Entwicklung von IT und ihren Zwecksetzungen vermissen und überläßt die Steuerung den Experten in Hochschulen und Industrie. Dies steht im Gegensatz zu der angenommenen "Universalität" der IT und ihrer Auswirkungen. Es verfestigt das Auseinanderlaufen von Technikentwicklung und demokratischer Partizipation.

Einsatz der Informationstechnik im Produktionsbereich

Wittkowsky: Das ZKI übernimmt pauschal die Modellvorstellung, wonach die rechnerintegrierte Produktion (CIM) den Trend zur "Fabrik der Zukunft" bestimmt, ohne nach deren produktionstechnischer Zweckmäßigkeit und deren sozialen und arbeitspolitischen Bedingungen und Konsequenzen zu fragen. Es verkürzt die Probleme der Produktionsautomatisierung auf den Fertigungssektor.

Die benannten Fakten werden übergangen, wonach noch 1987 z.B. nur 2% der Betriebe in der Investitionsgüterindustrie als voll integrationsfähig galten und über die Hälfte der Firmen mit Erfahrung im Gebrauch rechnergestützter Produktionsplanungs- und Steuerungssysteme (PPS) und rechnergestützter Fertigung (CAM) auch in Zukunft auf deren informationstechnische Verknüpfung verzichten wollen. Ebenso wird der alarmierende Befund ignoriert, daß nur 8% der Betriebe der Investitionsgüterindustrie mit dem Einsatz der Informationstechnik Humanisierungsziele anstreben (...).

Stattdessen scheint das ZKI die keineswegs mehr unumstrittene Strategie zu fördern, die jene von veränderten Wettbewerbsbedingun-

gen hervorgerufene "Krisis der Fabrik" (SPUR) als ein im wesentlichen informationstechnisch zu lösendes Problem der Gesamtsteuerung des Auftragsvolumens und der Arbeitsabläufe auf allen Ebenen interpretiert. Diese Krisis soll durch die Modellierung der Fabrik als Struktur von Funktionsbereichen, die durch Informationsflüsse miteinander verbunden sind, und durch Steuerung dieses Systems mit integrierten Rechnersystemen gelöst werden. Folgerichtig schrumpft dann die CIM-Problematik auf Datenintegration, d.h. die Entwicklung von Datenbanken, die Schaffung geeigneter Kommunikationsnetze sowie die Definition und technische Normung der dazu erforderlichen Schnittstellen zusammen.

Diese Position verkürzt die Probleme des Einsatzes von IT im Produktionsbereich in unzulässiger Weise:

- Sie vernachlässigt, daß auch in Zukunft nur ein kleiner Industriebereich für CIM-Konzeptionen geeignet ist und die verbleibenden mechanisch-manuell fertigenden Betriebe (z.B. Schiffsbau) ganz andere Einführungs- und Anwendungsstrategien der IT erfordern;
- sie vernachlässigt die zwar gewandelte, aber wachsende Bedeutung von menschlicher Arbeit und Arbeitsorganisation bei Einführung computergestützter Systeme (...);
- sie postuliert eine "grundlegende Bedeutung" von CIM für die Wettbewerbsfähigkeit der Industrie, obwohl die CIM-Einführung bei betriebswirtschaftlicher Bewertung bislang lediglich zu vorläufigen Nutzenerwartungen bei viel zu hohem Investitionsaufwand geführt hat und die absolute Wirtschaftlichkeit nicht bestimmt werden kann (...);
- sie gefährdet durch aufwendige (für viele Betriebe unerschwingliche) flexible Automatisierung die Eigenständigkeit von KMU, obgleich das Konzept gerade deren Stärkung anstrebt. Schon heute sind viele KMU kundenabhängig oder eng an Großkunden gekoppelt. Flexible Automatisierung ermöglicht es, auch Klein- und Mittelserien zu Bedin-

gungen von Großserien wirtschaftlich zu produzieren und damit in das Produktionsspektrum von KMU einzubrechen. Da flexible Produktionsmittel im Vergleich zu spezialisierten in der Regel teurer sind, können sie wirtschaftlich nur bei erhöhter Kapazität und deren Auslastung sein und eben dies führt zur Verdrängung von KMU.

Viele verbleibende KMU werden von der Großindustrie gezwungen, sich deren informationstechnologischen Konzepten zu unterwerfen. Eine solche Entwicklung im Produktionssektor fördert die Konzentration und zerstört die Vielfaltigkeit der Industrielandschaft.

Es wäre eine Konzeption erforderlich gewesen, die im öffentlichen Interesse mit dem Schwerpunkt auf arbeitsbezogenen Kriterien im Sinne einer menschengerechten Gestaltung nach einer sinnvollen Förderung und Begrenzung von CIM-Anwendungen gefragt und die zur Behebung ungelöster Probleme notwendige Forschungs- und Entwicklungsarbeit thematisiert hätte. Aus industriepolitischer Sicht hätte aufgezeigt werden müssen, wie die Eigenständigkeit von KMU in Zukunft gesichert werden soll und wie eine sie unterstützende Förderpolitik gestaltet werden soll.

Erwartete Auswirkungen auf die deutsche Wirtschaft

Gissel: Eine konsequente und zielgerichtete Umsetzung des Zukunftskonzept Informationstechnik wird sich unter Einbeziehung der gegebenen Anregungen und bei einem angemessenen Einsatz von Mitteln, zu denen im Zukunftskonzept nur wenige konkrete Hinweise zu finden sind, auf die Wettbewerbsfähigkeit der informationstechnischen Industrie und der ihre Produkte und Dienstleistungen nutzenden Industriezweige (vor allem auch mittelständige Unternehmen) positiv auswirken und damit dazu beitragen, den Industriestandort Bundesrepublik attraktiv zu halten. Wichtig ist dabei, daß ausreichend langfristige Perspektiven gesetzt werden.

Zur Bildung als Zukunftsaufgabe

Wittkowsky: Das ZKI huldigt einem Bildungsverständnis, an dessen Ende eigentlich nur noch "jedem Schüler einen Roboter" stehen kann. Ausgehend von der magischen Vorstellung einer naturgesetzlichen "Durchdringung aller Lebensbereiche" vertritt es einen unverantwortlichen informationstechnischen Bildungsimperialismus, wenn es fordert, informationstechnische Bildung sei als "durchgängiges und integratives Prinzip" für die Ausbildungsinhalte zu realisieren. Das ZKI ignoriert, daß Bildung primär die Entwicklung einer zum sozialen Zusammenleben in der Demokratie bereiten, kulturell vielseitig befähigten und verantwortungsbewußten Persönlichkeit zum Ziele hat, und fällt damit auf den Stand der bildungspolitischen Situation vor 10 Jahren zurück. Insbesondere werden weder die Notwendigkeiten gesehen, die sich aus der europäischen Einigung für die Schule ergeben, noch auch nur andeutungsweise entwickelt zu Lasten welcher Ausbildungsinhalte (Geschichte? Religion? Sprachen?) denn informationstechnische Grundbildung eingeführt werden soll.

So unbestritten informationstechnische Ausbildungsinhalte heute zur beruflichen oder Hochschulbildung gehören, gilt doch für das allgemeinbildende Schulwesen: es kann zur Bewältigung der Herausforderungen der Zukunft nicht beitragen, wenn es nur "die Fähigkeit zur Nutzung der Informationstechnik als Hilfsmittel bei der sinnvollen Erschließung der durch sie erst verfügbaren Datenmengen" (Seite 105/106) vermittelt. Menschliches Zusammenleben in Europa kann Bildung nur dann fördern, wenn sie Kenntnisse und Respekt von den Besonderheiten anderer europäischer Völker und dafür umfassende sprach- und religionswissenschaftliche, geographische und historische Qualifikationen vermittelt.

Gissel: In den öffentlichen Diskussionen in der Bundesrepublik ist immer wieder ein erschreckender Mangel an fundiertem Wissen und Objektivität über die Informationstechnik und ins-

besondere ihre wachsende Bedeutung für Wirtschaft und Gesellschaft zu sehen. Die z.T. sehr polemische Ablehnung moderner Informationstechnik steht einer geradezu euphorischen Einstellung zur Informationstechnik in Japan, aber auch USA, gegenüber. Hier ist daher ein wesentlicher Handlungsbedarf an öffentlicher Aufklärung und im Rahmen der Aus- und Weiterbildung gegeben.

Förderpolitische Anmerkungen zum ZKI

Wittkowsky: Im Gegensatz zu den Wirtschaftsdaten zur IT läßt das ZKI keine vernünftige Zuordnung und Saldierung der staatlichen Aufwendungen zu. Es fügt sich damit ein in die Undurchschaubarkeit der Förderlandschaft im Bereich F+E auf nationaler und EG-Ebene, die die Durchsetzung von Einzelinteressen begünstigt - insbesondere der gut organisierten Großindustrie oder auch bestimmter Wissenschaftlergruppen. So wird auch nicht deutlich, daß ungefähr jede zweite DM von den auf ca. 1,7 Mrd. DM geschätzten Ausgaben der Bundesregierung für F+E im Gebiet der IT für unmittelbar militärische Zwecke eingesetzt wird - ein im Zuge der Entspannung nicht mehr nachvollziehbarer Vorgang. Zu warnen ist auch vor den im ZKI nicht problematisierten Folgen des "Dual Use"-Entwicklungskonzeptes, wonach ja nicht etwa militärische Entwicklungen zivile Anwendungen berücksichtigen sollen, sondern umgekehrt eine Militarisierung ziviler IT-Entwicklung angestrebt wird. Da die vom BMVg festgelegten Teilgebiete für IT-Anwendungen praktisch identisch sind, führt die Logik dieser Verzahnung zu einer Dominanz militärpolitischer Interessen an der Technikentwicklung und zu einem Verlust von Steuerungsmöglichkeiten durch zivile Ressorts, wie z.B. das BMFT. Dieser "Pentagoneffekt" steht in völligem Gegensatz zu den unter 2. genannten Notwendigkeiten der F+E-Förderung und ist daher abzulehnen.

Zu fragen ist auch nach dem Umfang der staatlichen IT-Förderung überhaupt. Die auch im ZKI dokumentierte gute Wirtschaftslage der IT-Produkte erzeugenden Industrie müßte eine erhöhte Eigen-

finanzierung von F + E erlauben und Mittel für die viel drängenderen Probleme rationeller Energienutzung, Emissionsvermeidung und das Programm "Arbeit und Technik" freisetzen.

Hemmnisse und Handlungsbedarf bei den wirtschaftlichen Rahmenbedingungen

Gissel: Hemmnisse bzw. Handlungsbedarf werden in folgenden Punkten gesehen:

- Die staatlichen Rahmenbedingungen bestimmen sehr wesentlich die Qualität eines Industriestandortes, vor allem vor dem Hintergrund des Einheitlichen Marktes ab 1992. Die in dem Zukunftskonzept enthaltenen Aussagen zur Verbesserung der Unternehmensbesteuerung und zum Kartellrecht sind zwar zu begrüßen; sie sind aber zu wenig konkret, um sie wirklich bewerten zu können. Es ist notwendig, den Unternehmen den notwendigen Spielraum zu schaffen, um die für die Zukunftssicherungen notwendigen F&E-Aufwendungen erwirtschaften zu können. Gerade im Kartellrecht erscheint eine Anpassung dringend notwendig. Auch jüngste Entscheidungen zeigen immer wieder, daß der Bedeutung des europäischen Marktes oder gar des Weltmarktes nicht Rechnung getragen wird. Auch sollte die Bundesregierung ihren Einfluß geltend machen, damit ein europäisches Kartellrecht bis zum Beginn des Einheitlichen Marktes Realität ist.
- Die im Zukunftskonzept zitierte Gruppenfreistellungsverordnung für F&E-Vereinbarungen ist nach übereinstimmender Ansicht der führenden europäischen Unternehmen der Informations- und Telekommunikationstechnik nicht mehr ausreichend für eine wirksame Zusammenarbeit auf dem F&E-Gebiet z.B. in den Technologieprogrammen der EC.
- Innovative Beschaffungen der öffentlichen Hand werden zurecht als ein wichtiges Instrument zur Stärkung der Informationstechnik in der Bundesrepublik genannt. Es kommt nun darauf an, daß dieses Instrument auch entsprechend genutzt wird. Ob dafür alleine die Novellierung der VOL ausreicht

muß bezweifelt werden. Das Ausland, voran die USA und Japan, zeigt immer wieder, wie die öffentliche Beschaffung, zumal wenn sie mit entsprechenden Entwicklungsaufträgen einhergeht, als ein wirksames Instrument zur Verbesserung der Wettbewerbsfähigkeit der eigenen informationstechnischen Industrie mit nachhaltigem Erfolg genutzt wird.

- Ein weiterer Handlungsbedarf wird in einer verstärkten Abstimmung der langfristigen Forschungs- und Entwicklungsprogramme des BMVg auf dem Gebiet der Informationstechnik in der Verteidigung mit diesem Zukunftskonzept gesehen. Wie in dem Zukunftskonzept richtig dargestellt, gewinnt die Informationstechnik auch in der Verteidigungstechnik einen immer breiteren Raum auch in einem Umfeld der Abrüstungsmaßnahmen. Gebiete für eine solche Abstimmung reichen von der Mikroelektronik über Bildverarbeitung, Software Engineering oder Künstliche Intelligenz bis zur Sicherheit von Informationssystemen.

Hemmnisse und Defizite im Bereich der europäischen Zusammenarbeit, der Zusammenarbeit mit USA und Japan etc.

Gissel: Die sich stetig verkürzenden Innovationszeiten und die steigende Komplexität der Systeme auf dem Gebiet der Informationstechnik erfordert immer höhere F&E-Aufwendungen für jedes neue Produkt oder System in immer kürzerer Zeit. Die dafür notwendigen Ressourcen, Kapazitäten und Mittel lassen sich zunehmend nur noch in einem europäischen, wenn nicht sogar Weltmaßstab, sehen, d.h. sie müssen auf den europäischen bzw. den Weltmarkt ausgerichtet werden. Handlungsbedarf besteht daher zu folgenden Themen:

- Die europäischen Technologieprogramme der EC haben sich als notwendig und erfolgreich erwiesen. Neue Programme stehen an, die umfangreicher und anspruchsvoller sind (neues Frame Work Programm und ENS). Die Bundesregierung sollte diese Programme, die ja zum größeren Teil unter der Mitwirkung der deutschen IT-Indu-

strie entstanden sind, nachdrücklich unterstützen, vor allem gegen die Bestrebungen anderer Mitgliedsstaaten, die Mittel entscheidend zu kürzen oder die Programminhalte zu verwässern. Dabei sollten Bundesregierung und Industrie zusammenarbeiten. In diesem Zusammenhang wird insbesondere auf das ENS-Programm hingewiesen, das erstmals im europäischen Rahmen ein Beschaffungsprogramm werden kann.

- Die deutsche IT-Industrie muß sich in zunehmendem Maße auf dem europäischen und dem Weltmarkt orientieren, der jedoch z.T. sehr von nationalen Interessen geprägt ist. Das gilt einmal für die USA, in denen es vielschichtige legale Möglichkeiten gibt, den ausländischen Wettbewerb, selbst wenn er in den Staaten produziert, von öffentlichen Beschaffungen auszuschließen. Auch in Japan gibt es ähnlich wirkende Mechanismen. Dies führt zu einer erheblichen Wettbewerbsverzerrung. Der notwendige Handlungsbedarf besteht darin, in Verhandlungen mit diesen Ländern solche Wettbewerbsverzerrungen zuungunsten der deutschen bzw. europäischen IT-Industrie zu beseitigen oder aber für die Firmen solcher Länder in Europa ähnliche Bedingungen bei der öffentlichen Beschaffung zur Wirkung zu bringen.
- Die mit dem einheitlichen europäischen Binnenmarkt erreichte Öffnung des europäischen Marktes für die deutschen IT-Unternehmen (und die der anderen Mitgliedsländer) wird alleine noch nicht ausreichen, diesen die notwendige Leistungsfähigkeit im Weltmaßstab zu geben. Es wird unumgänglich sein, europäische Firmengruppierungen zu schaffen. Hierfür sollte die Bundesregierung helfen, die notwendigen Rahmenbedingungen zu schaffen einschließlich einer EUROPA-AG.

Auswirkungen auf die deutsche Wirtschaft - insbesondere Beschäftigungswirkungen

Wittkowsky: Das ZKI behauptet, wissenschaftliche Untersuchungen hätten "keine Anhaltspunkte" dafür

ergeben, daß mit der Einführung von IuK-Techniken auf gesamtwirtschaftlicher Ebene zwangsläufig die Freisetzung von Arbeitskräften - also Entlassungen und Arbeitslosigkeit - verbunden sei (Seite 14), räumt aber andererseits "in Einzelfällen Beschäftigungsrisiken" ein (Seite 137) unter Bezugnahme auf die META-Studie, d.h. je nach Innovationsstärke einer Branche.

Diese Behauptung verharmlost die immer noch unerträglich hohe Arbeitslosigkeit in der Bundesrepublik und z.B. rationalisierungsbedingte "Freisetzen" von Frauen auf Arbeitsplätzen mit geringeren Qualifikationsanforderungen. Sie ist politisch unannehmbar und auch sachlich falsch. So ergibt die META-Studie z.B. für die Beschäftigungswirkungen der (für die Entwicklung der Fabrik der Zukunft vergleichsweise marginalen) Industrieroboter einen Rückgang der Beschäftigung von rund 50.000 Personen bis 1990 und rund 100.000 Personen bis 1995. Selbst bei günstigen Annahmen über kompensatorische Wirkungen der wachsenden Gesamtproduktion bleibt ein Drittel dieser "Freisetzungseffekte" wirksam.

Die Analyse von drei Innovationsszenarien mit unterschiedlichen Annahmen über zusätzliche Investitionen und die dadurch erzielten Produktionsgewinne ergibt kein besseres Bild. Nur unter unrealistisch optimistischen Annahmen über eine Ausweitung des Exportes ist kein Netto-Arbeitsplatzverlust zu erwarten.

Wenn der IT die dominierende Rolle bei technischer Innovation und den damit verbundenen Arbeitsmarkteffekten zuerkannt wird, müßte die zukünftige Förderung dieser Technologie in eine volkswirtschaftliche Strategie der Beschäftigungssicherung eingebunden sein. Dazu genügt nicht eine vorausschauende Analyse der Technikfolgen für den Arbeitsmarkt, sondern es müssen kompensierende politische Maßnahmen im Rahmen des ZKI entwickelt werden.

Zusammenfassung

Wittkowsky: Das ZKI beruht auf einer kaum noch verständlichen

Unsensibilität gegenüber Entwicklungen, von denen Carl Friedrich von Weizsäcker schon 1986 sagte, die "Menschheit befindet sich heute in einer Krise, deren katastrophaler Höhepunkt wahrscheinlich noch vor uns liegt". Es verkennt die Notwendigkeit, Technikentwicklung als eine Aufgabe sozialer Gestaltung einzelner Technologien zu verstehen und diesen Ansatz zur Grundlage der Förder- und Wirtschaftspolitik zu machen.

Mit dem ZKI wird

- lediglich ein Anpassungskonzept an das vorgelegt, was industrielle Interessengruppen insbesondere der Großindustrie ohnehin schon machen;
- eine Eigendynamik technischer Entwicklung, losgelöst von gesellschaftlichen Entwicklungen, unterstellt, die zwar noch sozialwissenschaftlich untersucht, aber keinesfalls beschränkt oder im Sinne menschengemäßer Technikgestaltung nachhaltig beeinflusst werden darf und
- umstandslos ein absoluter Anspruch der informationstechnischen Industrie hingenommen, wenn IT-Systeme Arbeits- und Privatleben "prägen" und "durchdringen", so als ob dies jeder demokratischen Gestaltung und dem Handeln von Menschen entzogen sei.

Das ZKI kann daher als Beratungsgrundlage für Förderpolitik, Gesetzgebung und Forschungspolitik zur Entwicklung der Informationstechnik nicht empfohlen werden.

Zur Weltmarktposition

Gissel: Die deutsche Position im internationalen Wettbewerb ist in dem Zukunftskonzept recht zutreffend dargestellt. Die zu den unter "Erwartete Auswirkungen auf die deutsche Wirtschaft" und "Zur Bildung als Zukunftsaufgabe" gemachten Aussagen gelten daher sinngemäß auch für die Weltmarktposition.



ÜBERALL

Berlin

Hubert hat versucht, die alten FIFFler in Berlin anzusprechen, bisher ohne Erfolg. Ein **Neuanfang** wird notwendig sein, er möchte versuchen, Kontakte mit InformatikerInnen in der DDR aufzunehmen.

(Hubert Biskup)

Bonn

Manfred Domke betreut die Bonner Regionalgruppe, derzeitiges Schwerpunktthema ist **Computer und die Macht des Geldes**. Die Gruppe ist relativ stabil, setzt sich überwiegend aus MitarbeiterInnen der GMD zusammen.

(Helga Genrich)

Bremen

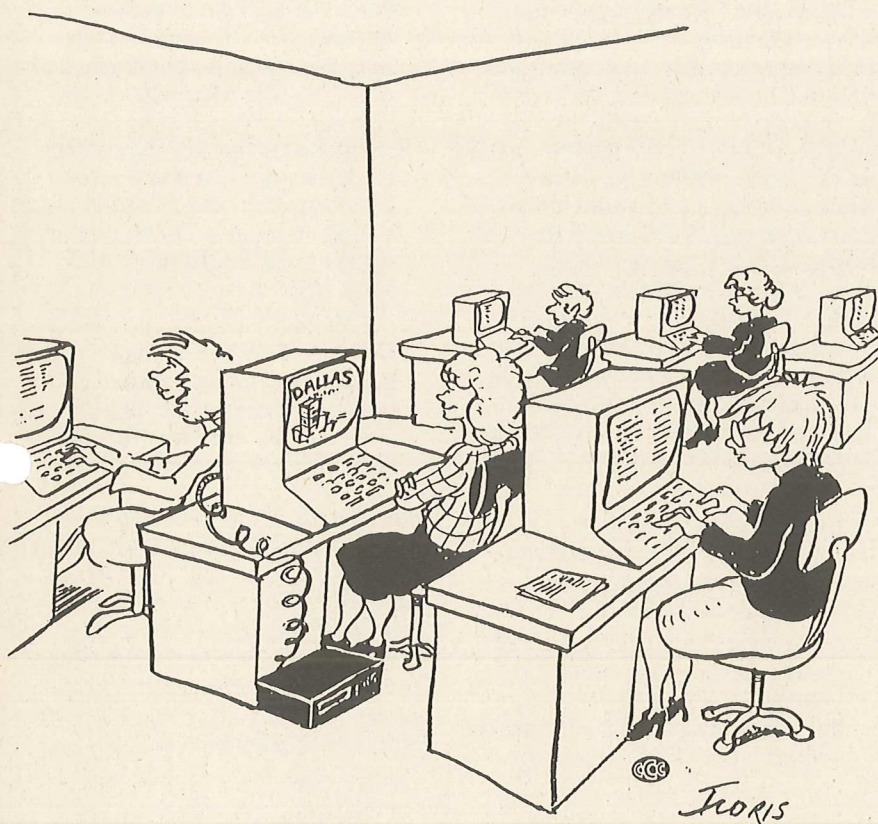
Im Herbst fand in Bremen eine eintägige Veranstaltung statt zum Thema **Rüstungskonversion**, in der Uni läuft eine Ringvorlesung zum selben Thema.

(Reinhold Franck)

Hamburg

Die Abrechnung der Hamburger Jahrestagung ist immer noch nicht abgeschlossen; es wird jedoch ein Überschuß bleiben.

Geplant ist eine Werbeaktion außerhalb der Universität. Bisher gibt es an der Universität eine **Initiative gegen den Einsatz der Programmiersprache Ada**; zu dieser



(Andreas Floris, Quelle: Cartoon-Caricature-Contor)

Aktion wurde Informationsmaterial zusammengestellt und als Sonderheft einer Fachschaftszeitschrift veröffentlicht.

(Ralf Klischewski)

München

Im Plenum der Münchner Regionalgruppe hielt Dr. Rolf Günther einen Vortrag zum Thema "Menschenbild in der Informatik".

Anhand des Positionspapiers von Ditz Schroer und Heidelotte Craubner (siehe im **FORUM** dieser **FIF KOMMUNIKATION**) wurde das Selbstverständnis des **FIF** diskutiert.

Die Regionalgruppe hat sich im Gasteig mit einer Ausstellung am "Tag der Initiativen" beteiligt und wird sich am Kirchentag 1990 beteiligen.

Für das September-Plenum ist ein Vortrag von Prof. Dr. Margret Falck

von der Humboldt-Universität in Ost-Berlin vorgesehen.

Schon längere Zeit veranstaltet die **Münchner Volkshochschule** in Zusammenarbeit mit dem **FIF Arbeitstreffen**, in denen die gesellschaftlichen Auswirkungen der Informationstechnologien erarbeitet und zur Diskussion gestellt werden. (PO 353, Volkshochschule Rosenkavalierplatz 16, jeden 2. Donnerstag im Monat 20.00 Uhr, Einschreibung nicht erforderlich)

Außerdem sind **FIF**-Mitglieder an den folgenden beiden Veranstaltungen der Münchner Volkshochschule beteiligt:

Das **Wochenendseminar "Datenschutz in der Praxis"** soll das Bewußtsein über die Notwendigkeit des Datenschutzes im Bereich der personenbezogenen Daten wecken. Kursinhalte sind: Das informationelle Selbstbestimmungsrecht, gesetzliche Datenschutzbestimmungen auf Länder-, Bundes- und Europäebene, Verknüpfung von Daten und die dazugehörigen gesellschaft-

lichen Zusammenhänge, Gefahren durch den uneingeschränkten Computereinsatz und damit verbunden, die informationelle Gewaltenteilung, Datenschutzpraxis im öffentlichen und privaten Bereich, Funktion und Aufgaben des Datenschutzbeauftragten. (PS 352, Volkshochschule Albert-Roßhaupter-Straße 8, Genauer Termin und weitere Auskünfte unter Tel. (089) 48006-106)

Der Kurs "Computer-Netze" wird über Einsatzbereiche und Möglichkeiten der Computervernetzung im privaten, gewerblichen und öffentlichen Bereich informieren. Kursinhalte sind: Grundlagen von Kommunikationsverhalten; Sprach-, Text-, Bild- und Datenübertragung in lokalen und weltweiten Netzen; technische und anwenderbezogene Realisierung und die entsprechenden Normen und gesetzlichen Bestimmungen. Zu den erarbeiteten Beispielen werden soziale und gesellschaftspolitische Auswirkungen auf das menschliche Kommunikationsverhalten dargestellt und diskutiert. (PG 345, VHS Zentrum Gasteig, 5 x Montag 17.30 bis 19.30 und 1 x Samstag 10.00 bis 16.00 Uhr, 23. April bis 26. Mai 1990)

(Ditz Schroer)

Stuttgart Tübingen

Die Regionalgruppen haben mit den Vorbereitungen für die **Jahrestagung 1990** begonnen.

(Gerhard Wohland)

Erinnerung




**DAS BÜRO
HAT EINE NEUE
TELEFONNUMMER:
(0228) 21 95 48**

LESEN?

DFKI - Gegensätzliche Interessen an der KI

(Die in der FIFF KOMMUNIKATION 2/90 erwähnte Studie über das Deutsche Forschungsinstitut für KI von Rupert Röder hat sich als lohnende Lektüre erwiesen. Hier also die angekündigte ausführliche Besprechung.)

Studie zur Technologiebewertung der "Künstlichen Intelligenz", Hans-Böckler-Stiftung, Mitbestimmungs-, Forschungs- und Studienförderwerk des Deutschen Gewerkschaftsbundes, Bertha-von-Suttner-Platz 3, 4000 Düsseldorf 1

Die Situation

Am 4. Juli 1988 wurde das 'Deutsche Forschungszentrum für Künstliche Intelligenz' (DFKI) als privatrechtliche gemeinnützige GmbH offiziell gegründet. Gleichberechtigte Gesellschafter sind zum einen die Fraunhofer-Gesellschaft und die Gesellschaft für Mathematik und Datenverarbeitung (GMD), zwei Großforschungseinrichtungen des Bundes. Ihnen stehen neun Privatfirmen gegenüber: Siemens, Nixdorf, Philips, IBM, Krupp Atlas Elektronik, Mannesmann Kienzle, AEG, ADV/Orga und die Mainzer KI-Firma Insiders. Bund und Länder halten sich als Sponsoren diskret im Hintergrund.

Da in diesem Bereich die Devise gilt: 'Klotzen, nicht kleckern', sollen nach

der Aufbauphase etwa hundert WissenschaftlerInnen an diesem Institut arbeiten. Die Finanzierung wird im wesentlichen von der öffentlichen Hand getragen: Das Bundesministerium für Forschung und Technologie schießt anfangs 5 Millionen jährlich, später 10 bis 15 Millionen zu, die Länder stellen die Infrastruktur bereit. Das ist neben den Baukosten von 25 Millionen für den Institutsbau (zu tragen vom Bundesland Rheinland-Pfalz) und 40 Millionen Raumausstattung die Bereitstellung von Lehrstühlen und Projektleiterstellen, die natürlich in Absprache mit der Industrie zu besetzen sein werden. Die Industrie ist mit einem Beitrag von je 100.000 DM pro Partner dabei.

Ebenso unterschiedlich wie die Höhe der finanziellen Beteiligung der beiden Seiten sind auch ihre Erwartungen an das Institut:

- Als wissenschaftliche Vision für das DFKI wurde formuliert, KI-Systeme dazu zu bringen, sich kontext-gemäß zu verhalten, also endlich 'gesunden Menschenver-

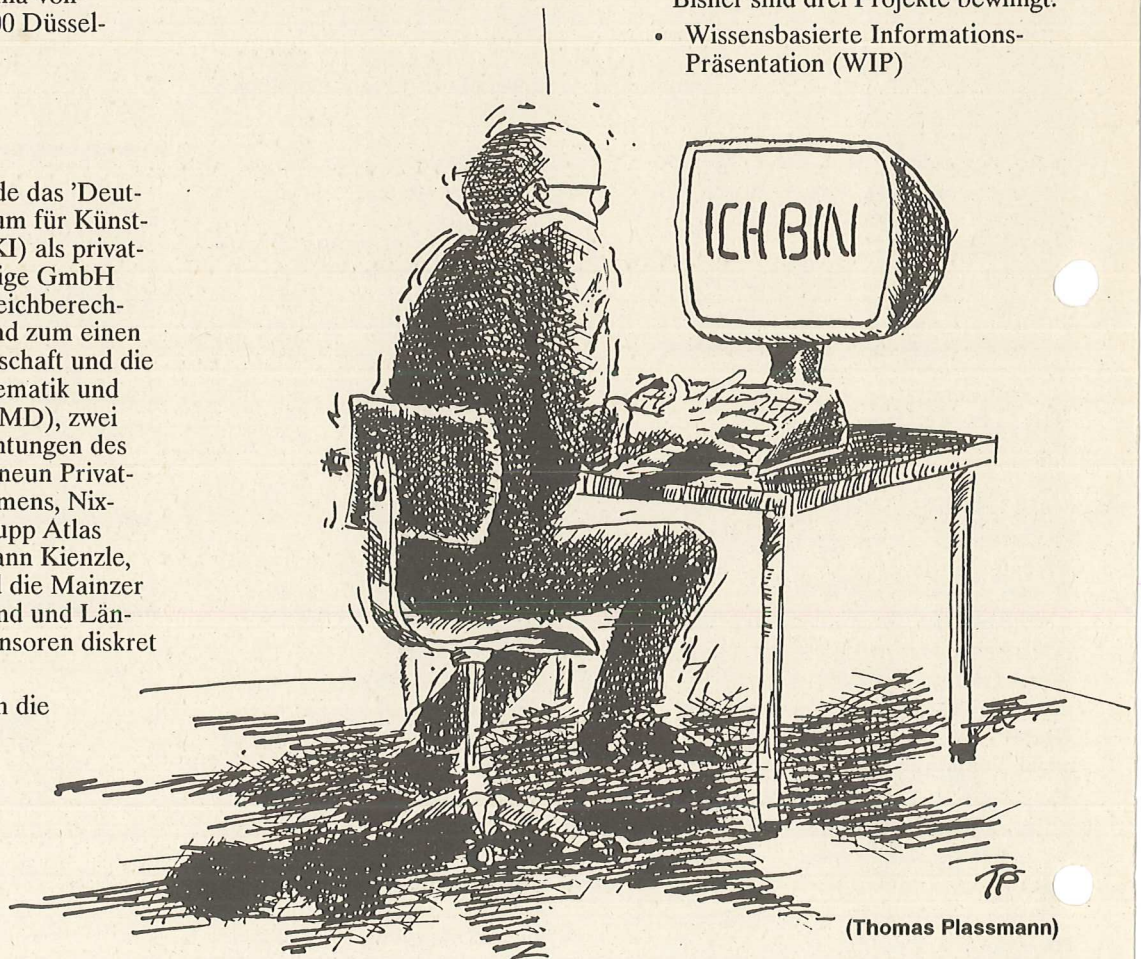
stand' zu entwickeln. Diese Zielsetzung zieht sich von Anbeginn durch die KI-Forschung und zeichnet sich wie jede Grundlagenforschung dadurch aus, daß zumindest die Möglichkeit der Sokratischen Einsicht in die Nicht-Erreichbarkeit des gesetzten Zieles gedacht werden muß. Der Fortschritt der Wissenschaft besteht in diesem Fall in einer verbesserten Begründung für diese Nicht-Erreichbarkeit.

- Die Industrie dagegen verspricht sich vor allem den Transfer von Ergebnissen akademischer Forschung in betriebliche Erprobung und Nutzung in Form von vermarktbareren Produkten.

Kosten für die notwendige Forschung und das damit verbundene Risiko sollen also vom Staat finanziert werden, die Industrie hat mit ihrer Beteiligung das Recht zur Vermarktung der Ergebnisse erworben. Der aktuelle Stand in diesem Zielkonflikt ist nicht einmal für den Gutachter abzuschätzen.

Bisher sind drei Projekte bewilligt:

- Wissensbasierte Informations-Präsentation (WIP)



(Thomas Plassmann)

- Autonome, kooperierende Agenten (AKA)
- Akquisition, Repräsentation und Compilation von technischem Wissen (ARC-TEC)

Die Tendenz dieser Projekte deutet in die Richtung einer Verlagerung von Entscheidungen in KI-Systeme. Die maschinellen 'Agenten' sollen zu Entscheidungen befähigt werden, etwa auch darüber, wie sie mit menschlichen 'Agenten' zusammenarbeiten. Da nach den bisherigen Erfahrungen in diesem Bereich ein Erreichen dieser Ziele kaum zu erwarten ist, die Industrie andererseits vermarktbare Produkte benötigt, ist nicht auszuschließen, daß zunächst auf betrieblicher Ebene und auf lange Sicht auf gesellschaftlicher Ebene eine formalisierte Wirklichkeit geschaffen wird, der diese Systeme besser angemessen sind als der 'Störfaktor Mensch'.

Diesen Konflikt und die damit verbundenen Gefahren so deutlich herausgearbeitet zu haben, ist einer der Vorzüge der Studie.

Das Umfeld

Dabei läßt es der Autor jedoch nicht bewenden. Seiner kritischen Darstellung des Forschungsprogramms des DFKI schickt er einen Überblick über die Anfänge der KI sowie ihrer Risiken und Chancen voraus.

Die Versprechungen der Gründerväter der KI wie Herbert A. Simon und Marvin Minsky aus den 60er Jahren dürften heute nur mehr Unterhaltungswert haben angesichts der immer wieder verschobenen Termine, zu denen es endlich gelingen soll, die Leistungen der 'meat machine' menschlicher Geist von Computern erbringen zu lassen. Das Lachen bleibt einem jedoch im Halse stecken, wenn man sich angesichts eines Unternehmens wie des DFKI vor Augen führt, welche Auswirkungen auf die gesellschaftliche Realität diese nicht eingelösten (und wahrscheinlich auch nicht einlösbaren) Versprechungen haben (können) und haben werden.

Wolfgang Coy und Lena Bonsiepen berichten in ihrem Buch ("Erfahrung und Berechnung",

Kritik der Expertensystemtechnik, Informatik Fachberichte 229, Springer Verlag, 1989) über das Konfigurationssystem XCON der Firma DEC, eines der wenigen wirklich genutzten Expertensysteme, das angeblich enorm kostensparend sei, de facto jedoch nicht mehr wartbar ist. Da nur mehr dieses System alles Expertenwissen kennt, also die Experten ersetzt wurden, ist die Firma DEC von diesem inzwischen als strategisch wichtig eingestuften System abhängig.

Jörg Siekmann, einer der führenden Exponenten der KI in der Bundesrepublik sagt in gewissen Bereichen, etwa der Verwaltung, eine drastische Reduzierung der Arbeitsplätze durch den Einsatz von Expertensystemen voraus: "Durch diesen Prozeß werden Millionen von Arbeitern und Verwaltungsangestellten zunächst das verlieren, was ihren 'Marktwert' und nicht zuletzt ihr Selbstwertgefühl ausmacht, nämlich ihre Qualifikation, die nun nicht mehr gebraucht wird, und sie werden schließlich im großen Heer der 'nicht mehr vermittelbaren' Arbeitslosen landen."

Und vollends kalt kann es der Leserin und dem Leser werden, wenn sie erfahren, daß die Forschungsförderung des Bundes und der Länder die bisherigen Ergebnisse der Technikfolgen-Diskussion in diesem Bereich großzügig ignoriert. Auch die Tatsache, daß das mit soviel Elan begonnene japanische Projekt der 5. Generation inzwischen stillschweigend zu Grabe getragen wurde, hat auf die hiesigen Forschungsförderer keinen Einfluß.

Eine Alternative

Dem un-menschlichen Forschungsprogramm des DFKI stellt der Autor eine konstruktive Alternative gegenüber:

Ausgehend von der Erfahrung, daß Humanität sich rechnet, d.h. daß es für Betriebe auf die Dauer unrentabel ist, menschliche Arbeitskraft zu ersetzen, liefert der Autor einen Ansatz für eine betroffenenorientierte KI-Forschung. Erste Forderung an eine solche ist, "eine System-Philosophie zu entwickeln, wie KI-Anwendungen diskursfähig (nachvollziehbar, bewertbar, erör-

terbar und entwicklungsfähig) gestaltet werden können.... Als zweite Forderung müssen für den betrieblichen Bereich arbeitsorganisatorische Konzepte für den qualifikations-orientierten Einsatz von KI-Systemen entwickelt werden. Drittens ist eine Methodik der partizipativen Systementwicklung für KI-Systeme auszuarbeiten."

Als Anhang regt der Autor der Studie ein Forschungsprojekt nach diesen Leitlinien an.

Nach Meinung des Referenten ist diese Studie ein wichtiger Beitrag zur Auseinandersetzung über die Risiken und Chancen der KI.

(Hellmut Weber)

Hurra, Konkurrenz ist da!

Zu unserer FIFF KOMMUNIKATION gibt es jetzt erfreulicherweise ein "Konkurrenzblatt", den Informationsdienst COMPUTER & MEDIEN. Als Herausgeber erscheint eine gleichnamige Bundesarbeitsgemeinschaft DER GRÜNEN, was insofern etwas überrascht, als DIE GRÜNEN bisher im Ruf standen, Computertechnik so vollständig abzulehnen, daß schon die bloße Beschäftigung damit "pfui" zu sein schien. Wir freuen uns also sehr über das neue Heft 1/90, besonders natürlich auch deshalb, weil es einen Artikel "FIFF: ISDN-AK doch nicht aufgelöst" enthält.

Aus dem breiten Spektrum des Heftes einige weitere Beispiele: "Infodienst-Adressverwaltung ohne PC", "Mailboxdiskussion: Kritische Stellungnahme", "Grobe Checkliste bei alternativem Computereinsatz", "Wählscheibentelefone stärken ISDN" (siehe dazu unter AKTUELL in dieser FIFF KOMMUNIKATION). Vielleicht können wir auch etwas Werbung für unser Blatt im Informationsdienst COMPUTER & MEDIEN unterbringen, jedenfalls wünschen wir den GRÜNEN viel Erfolg.

Kontakt: Redaktion COMPUTER
& MEDIEN Günter J. Schäfer
Ostlandweg 33
34 Göttingen
Tel. (0551) 371791

FIFF jetzt auch Verlag

Tagungsband '89 ist da

Nachdem es in und nach Frankfurt noch zu Diskussionen gekommen war, in welcher Form ein Reader der Tagung erscheinen sollte, hat der FIFF-Vorstand nach gründlichen Preis- und Aufwandsabschätzungen beschlossen, ein Buch im Eigenverlag herauszugeben. Daraus wäre aber ohne den großen Einsatz der Herausgeberin nichts geworden. Deshalb an sie nochmals vielen Dank. Eine solche unentgeltliche Eigenarbeit für den Eigenverlag macht das Buch nicht nur schneller in der Erstellung (verglichen man es mit dem Buch der '88er Tagung), sondern auch erheblich billiger: über 300 Seiten kosten statt 19,80 DM wie früher sage und schreibe nur 12,80 DM (zzgl. Porto). Deshalb bekommen alle zahlenden Tagungsteilnehmer den Tagungsband '89 kostenlos zugeschickt. Alle anderen können ihn ab sofort im Büro oder über den Buchhandel bestellen.

Allen, die nicht dabei waren, sei hier aus der Themenpalette des Buches vorgestellt:

- Netzknoten Frankfurt
- Die Psyche des Menschen ist (un)berechenbar
- POS-Banking - Entwicklungen und Gefahren
- Rüstungshaushalt und Informationstechnik
- Verfassungsverträglichkeit als Kriterium der Technikbewertung am Beispiel der Informationstechnik
- Anarchie und Informatik

All dies und noch viel mehr in:

Jutta Schaaf (Hrsg.): Die Würde des Menschen ist unverNETZbar,
Bonn, 1990, 12,80 DM

TERMINE

In dieser Rubrik ist jede Menge Platz für Termine von Veranstaltungen, die für LeserInnen der FIFF KOMMUNIKATION interessant sein könnten. Hinweise auf Veranstaltungen bitte an die Redaktion senden (*Anschrift siehe IMPRESSUM*).

Termin ?, ARD, Fernsehfilm "Die elektronischen Eierköpfe - Macht und Macher der künstlichen Intelligenz" von Charlott Acklin und Manuel Esser

Wegen der aktuellen politischen Situation wurde der vorgesehene Sendetermin verschoben. Er wird voraussichtlich noch vor der Sommerpause gesendet. Wer den Film sehen will, muß die Tagespresse beobachten.

9. bis 13. Mai 1990, München, Tagung "Ökologie und Frieden durch Entmilitarisierung" des IPF (Institut für Psychologie und Friedensforschung)

Kontakt: Birgit Ertl, Frundsbergstr. 26, 8000 München 19, Tel (089) 166601, Fax. (089) 1684198

11. bis 13. Mai 1990, Bad Boll, Seminar "Das Menschenbild der künstlichen Intelligenz" (Tagungsnummer U2 07 90)

Kontakt: Timm Klotz, Evangelische Akademie, Sterngrasse 14, 7900 Ulm, Tel. (0731) 67064/65

14. bis 17. Juni 1990, Ulm, Zukunftskonzept Informationstechnik -- unsere Zukunft? Fachtagung des Fachbereichs "Informatik und Gesellschaft"

Kontakt: FH Ulm, Prof. Pieper, FB TI, Prittwitzstr. 10, Postfach 3860, D-7900 Ulm, Tel. (0731) 2053-0, Fax: -270

22. bis 24. Juni 1990, Hamburg, Kongress "Verwundbarkeit der Industrielandschaft Europa - Perspektiven kooperativer Sicherheit für die nachmilitärische Ära" in der Hochschule für Wirtschaft und Politik, Von Melle Park 9. Veranstalter: Verantwortung für den Frieden - Naturwissenschaftler-Initiative e.V., BRD und Einrichtungen an der Akademie der Wissenschaften der DDR.

Kontakt: Prof. Dr. Hubert Kneser, Institut für Genetik, Weyertal 121, 5000 Köln 41.

Zum Thema und zu den Zielen des Kongresses schreiben die Veranstalter: "Immer häufiger zeigen uns dramatische Unfälle mit technischen Großsystemen, daß in unserer industriellen Zivilisation schon kleine Störungen ausreichen können, um die Welt, in der wir leben, zu zerstören. Welche Folgen kann dann der Gebrauch von militärischer Gewalt in der Industrielandschaft Europa auslösen? Wir streben mit dem Kongreß zwei konkrete Ziele an:

1. Sammlung und Einschätzung von Belegen zum Ausmaß der zivilen Selbstzerstörungspotentiale und zur existentiellen Abhängigkeit moderner Industriegesellschaften von der Betriebsbedingung Frieden.

2. Erarbeitung von Kriterien, denen eine Sicherheitspolitik und ihre Mittel genügen müssen, damit sie der Zukunftsfähigkeit unserer Zivilisation nicht entgegenwirken, sondern sie umfassend fördern.

Wir wollen damit in einer Zeit, da die verkrusteten Blöcke und Denkblockaden aufbrechen, die Zukunftssicherung unserer Zivilisation und der globalen Lebensmöglichkeiten als Mittelpunkt und Maßstab einer neuen Sicherheitspolitik für Europa einfordern."

28. Juli 1990, Boston/USA, Symposium "Directions and Implications of Advanced Computing" des CPSR

Kontakt: Douglas Schuler, CPSR/Seattle, P.O.Box 85481, Seattle, WA 98105.

VIELZWECK-SCHNIPSEL

Die/Der bin ich:

Name: _____ Straße: _____
 Wohnort: _____ Mitgliedsnummer (falls bekannt): _____
 Telefon (Angabe nur wenn erwünscht, privat): _____ (Arbeit): _____

Das möchte ich:

- ☐ Ich möchte ☐ aktives bzw. ☐ förderndes Mitglied des F!FF werden
 (Mindestbetrag ist für Verdienende 60.-- DM, für Studierende 15.-- DM pro Jahr)
☐ Ich möchte, ohne F!FF-Mitglied zu sein, die F!FF KOMMUNIKATION für 15.-- DM/Jahr abonnieren
☐ Ich überweise _____ DM auf Konto 48000798 der Sparkasse Bonn (BLZ 38050000)
☐ Einzugsermächtigung (siehe unten) ist ausgefüllt

☐ Ich möchte meine neue/korrigierte Anschrift mitteilen (siehe oben). Meine alte/falsche Anschrift:
 Straße: _____ Wohnort: _____

- ☐ Ich möchte F!FF etwas spenden
☐ Verrechnungsscheck über _____ DM liegt bei
☐ Spendenquittung am Ende des Kalenderjahres erbeten

☐ Ich möchte mehr über F!FF wissen, bitte schickt mir _____

☐ Ich möchte gegen Rechnung zuzüglich Portokosten bestellen:

- ☐ Ich möchte F!FF informieren über einen Artikel/ein Buch
☐ Zitat (siehe unten)
☐ Kopie liegt bei

- ☐ Ich möchte zur F!FF KOMMUNIKATION beitragen mit
☐ einem Manuskript zur Veröffentlichung (liegt bei)
☐ einer Anregung (siehe unten)
- _____
- _____
- _____

☐ Ich möchte einen richtigen Brief schreiben. Der VIELZWECK-SCHNIPSEL ist nichts für mich!

Einzugsermächtigung

Hiermit ermächtige ich das F!FF e.V. widerruflich, meinen Mitgliedsbeitrag durch Lastschrift einzuziehen.

Jahresbeitrag: _____ DM, erstmals: _____ Konto-Nr.: _____ BLZ: _____
 Geldinstitut: _____ Wenn das Konto keine

Deckung aufweist, besteht keine Verpflichtung des Geldinstitutes, die Lastschrift auszuführen

Name: _____ Straße: _____
 Wohnort: _____ Datum: _____ Unterschrift: _____

(Wir werden Ihre Daten nur für Zwecke des F!FF verarbeiten und keinem Dritten zugänglich machen.)

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 Beiträge geben die jeweilige AutorInnen-Meinung wieder.

Nachdruckgenehmigung wird nach Rücksprache mit der Redaktion in der Regel gerne erteilt. Voraussetzung hierfür ist die Quellenangabe und die Zusendung von zwei Belegexemplaren.

Heftpreis: 3.-- DM. Der Bezugspreis für die **FIFF** KOMMUNIKATION ist für FIFF-Mitglieder im Mitgliedsbeitrag enthalten. Nichtmitglieder können die **FIFF** KOMMUNIKATION für 15.-- DM/Jahr (inkl. Versand) abonnieren.

Erscheinungsweise: einmal vierteljährlich

Erscheinungsort: Bonn

Auflage: 1800

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

Verlagsadresse: FIFF-Geschäftsstelle, Reuterstraße 44, 5300 Bonn 1, Tel. (0228) 219548

Druck: PR-Druck und Verlag, Dorotheenstraße 117, 5300 Bonn 1

Redaktionsadresse: Christine Fischer, Solalindenstraße 108, 8000 München 82

Redaktions-Team für FIFF KOMMUNIKATION 2/90: Ute Bernhardt, Christine Fischer (verantwortlich), Friedemann Gerster-Streit, Peter Kaiser, Fritz Obermaier, Ingo Ruhmann, Winfried Seidel, Hellmut Weber (verantwortlich)

Eine Bitte: Postvertriebsstücke werden von der Post auch auf Antrag nicht nachgesendet, daher bitten wir alle Mitglieder und Abonnenten, jede Adressänderung rechtzeitig bekannt zu geben.

Redaktionsschluß für FIFF KOMMUNIKATION 3/90: 4. Mai 1990 (Leserbriefe und Kurznachrichten der Regionalgruppen und AKs: 18. Mai 1990).

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 Fachgebietes verantwortlich fühlen und entsprechende Arbeit leisten wollen:

Erarbeiten einer Geschichte der Informatik, in welcher der entscheidende Einfluß militärischer Ziele für die bisherige Entwicklung der Informatik nicht verschwiegen wird.

Zusammentragen von Wissen über die Wirkung der Informationstechnik auf Gesellschaft und Umwelt, Diskutieren dieses Materials in der Öffentlichkeit.

Suchen nach Möglichkeiten für einen sozialverträglichen Einsatz von Datenverarbeitungs-Anlagen und -Anwendungen; Entwickeln und Erproben einer auf Menschen hin orientierten Informationstechnik.

Schärfen des Verantwortungsbewußtseins von FachkollegInnen; Beitragen zur Verbreitung einer Berufsethik, die den Menschen auch in der Arbeit im Mittelpunkt sieht und es daher nicht zuläßt, die eigenen Kenntnisse für menschenfeindliche Zwecke einzusetzen.

Eintreten in der Öffentlichkeit für einen friedlichen, gesellschaftlich nützlichen Einsatz der Informationstechnik.

Zusammenarbeiten mit vergleichbaren Organisationen in anderen Ländern (Computer Professionals for Social Responsibility (CPSR) in USA).

Im FIFF sind gleichberechtigt und gleichgewichtig Studierende, WissenschaftlerInnen und im Berufsleben stehende InformatikerInnen organisiert. Sie fordern alle in der Informationstechnik Arbeitenden auf, sich ebenfalls mit dem gesellschaftlichen Umfeld, insbesondere den betrieblichen Voraussetzungen und den sozialen Auswirkungen ihrer Arbeit zu beschäftigen.

Der FIFF-Vorstand

Prof. Dr. Reinhold Franck[†]
(Vorsitzender)
Saarbrücker Straße 43
2800 Bremen 1

Hubert Biskup
Hindenburgdamm 65e
1000 Berlin 45

Helga Genrich
(Stellvertr. Vorsitzende)
Im Spicher Garten 3
5330 Königswinter 21

Pia Grund
Jakobsgasse 18
7400 Tübingen

Ralf Klischewski
Goldbachstraße 2
2000 Hamburg 50

Gilla Reckert
Fuldastraße 22
4600 Dortmund 41

Jürgen D. Schroer
Am Bergl 2
8031 Seefeld-Meiling

Hellmut Weber
Degenfeldstraße 2
8000 München 40

Gerhard Wohland
Hohenlehenstraße 18
7408 Wankheim

Bitte um Beiträge

Die **FIFF** KOMMUNIKATION lebt von der aktiven Mitarbeit ihrer LeserInnen. Die Redaktion wünscht sich viele lebendige Beiträge, die zur Diskussion über FIFF-Themen anregen. Die Redaktion behält sich Kürzungen vor. Erbeten sind auch Zeichnungen, Comics usw. zu Informatik-Themen oder zu eingereichten Beiträgen. Die Bearbeitung wird erleichtert, wenn die Beiträge auf Disketten (5¹/₄-Zoll, MS-DOS ASCII-Format, keine Silbentrennung) oder sauber und groß gedruckt (zur Verarbeitung mit einem Scanner) der Redaktion zugehen. Eine Adresse für Electronic Mail kann bei der Redaktion erfragt werden.

ADRESSEN

Das FIFF bemüht sich, den Mitgliedern die Möglichkeit zu regionalen Kontakten und zur Gründung von Initiativen zu geben. Folgende Kontaktadressen wurden uns bisher gemeldet, weitere werden hoffentlich folgen (vorzugsweise mit Telefonnummer).

Regionale Kontaktadressen

- 1000** Hubert Biskup
Hindenburgdamm 65e
Berlin 45
Tel. (030) 314-25471
- 2000** Simone Pribbenow
Fachbereich Informatik
Bodenstedtstraße 16
Hamburg 50
Tel. (040) 4123-6115
- 2370** Hans-Otto Kühl
c/o Schlesweg AG
Kieler Straße 19
Rendsburg
Tel. (04331) 201-2187
- 2800** Karin Vosseberg
Universität Bremen
Fachbereich Informatik
Postfach 330440
Bremen 33
Tel. (0421) 218-2280
- 2900** Fachschaft Informatik
Carl-von-Ossietzky-Universität
Ammerländer Heerstraße
Oldenburg
- 4400** Werner Ahrens
Hohe Geest 120
Münster
Tel. (02051) 3054 (p) und
(0251) 491-429 (d)
- 5000** Manfred Keul
Landsbergstraße 16
Köln
Tel. (0221) 317911
- 5330** Manfred Domke
Ölbergstraße 94a
Königswinter

- 5400** Michael Möhring
EWH Koblenz
Rheinau 3-4
Koblenz
Tel. (0261) 12156 (App. 292)
- 6000** Ingo Fischer
Dahlmannstraße 31
Frankfurt/Main 60
- 6101** Hans Rupp
Friedrich-Merz-Straße 32
Groß-Bieberau
(bei Darmstadt)
Tel. (06166) 8039
- 6750** Paul-Thomas Kandzia
Lothringer Dell 72
Kaiserslautern
Tel. (0631) 70645
- 7000** Karsten Hofmann
Gorch-Fock-Straße 1
Stuttgart 75
Tel. (0711) 472626
- 7500** Gerhard Jordan
Rüपुरer Straße 35
Karlsruhe 1
- 7750** Thomas Freytag
Am Briel 48
Konstanz
Tel. (07531) 50367
- 7900** Timm H. Klotz
Franz-Wiedemeier-Str. 108
Ulm
Tel. (0731) 385657
- 8000** Bernd Rendenbach
Grünwalderstraße 145a
München 90
Tel. (089) 6422119
- 8520** Prof. Dr. Horst Müller
Inst. f. math. Maschinen und
DV der Universität
Erlangen-Nürnberg
Martensstraße 3
Erlangen
- 8900** Eberhard Zehendner
Schubertstraße 4
Augsburg
Tel. (0821) 414554

Kontaktadressen der überregionalen Arbeitskreise

ISDN-AK

Hans Rupp
Friedrich-Merz-Straße 32
6101 Groß-Bieberau
(bei Darmstadt)
Tel. (06166) 8039

AK RUIN

"Rüstung und Informatik"

Helga Genrich (vorläufig)
Im Spicher Garten 3
5330 Königswinter 21
Tel. (02244) 3264

AK "Neue Wege in der Informatik"

Michael Möhring
EWH Koblenz
Rheinau 3-4
5400 Koblenz
Tel. (0261) 12156 (App. 292)

AK "FIFF europaweit"

Dagmar Boedicker
Daiserstraße 45
8000 München 70
Tel. (089) 7256547



FIFF-Geschäftsstelle

FIFF-Geschäftsstelle
Reuterstraße 44
5300 Bonn 1
Tel. (0228) 219548.

Das Büro ist dienstags von 14 bis 19 Uhr und donnerstags von 16 bis 19 Uhr besetzt. Der Geldverkehr läuft über das Konto 48000798 der Sparkasse Bonn (BLZ 38050000).

SCHLUSS- P



FIFF e.V., Reuterstr.44, 5300 Bonn 1

Kurt Fussangel
Heddernheimer Kirchstr. 30
6000 Frankfurt 50

Vom Fischernetz zum neuronalen Netz!

Was der Ichthyologe einem Informatiker zu sagen hat!

Eine Parabel von Sir Arthur Eddington

In dieser Parabel werden InformatikerInnen (*Im Original Naturwissenschaftler*) mit Ichthyologen, Fischkundigen, die das Leben im Meer erforschen, verglichen. Er, der Ichthyologe, wirft dazu sein Netz aus, zieht es an Land und prüft seinen Fang nach der gewohnten Art eines Wissenschaftlers. Nach vielen Fischzügen und gewissenhaften Überprüfungen gelangt er zur Entdeckung von zwei Grundgesetzen der Ichthyologie:

1. Alle Fische sind größer als fünf Zentimeter.
2. Alle Fische haben Kiemen.

Er nennt diese Aussagen Grundgesetze, da beide Aussagen sich ohne Ausnahme bei jedem Fang bestätigen lassen. Versuchsweise nimmt er deshalb an, daß diese Aussagen auch bei jedem künftigen Fang sich bestätigen, also wahr bleiben werden.

Ein kritischer Betrachter (*oder eine kritische Betrachterin, wir wollen ihn/sie hier einmal als FIFF-Mitglied benennen*) ist jedoch mit dieser Schlußfolgerung des Ichthyologen höchst unzufrieden und wendet energisch ein: "Dein zweites Grundgesetz, daß alle Fische Kiemen haben, lasse ich als Gesetz gelten, aber dein erstes Grundgesetz, über die Mindestgröße der Fische, ist gar kein Gesetz. Es gibt im Meer sehr wohl Fische, die kleiner als fünf Zentimeter sind, aber diese kannst du mit deinem Netz einfach nicht fangen, da dein Netz eine Maschenweite von fünf Zentimeter hat!"

Unser Ichthyologe ist aber von diesem Einwand keineswegs beeindruckt und entgegnet: "Was ich mit meinem Netz nicht fangen kann, liegt prinzipiell außerhalb fischkundlichen Wissens, es bezieht sich auf kein Objekt der Art, wie es in der Ichthyologie als Objekt definiert ist. Für mich als Ichthyologen gilt: Was ich nicht fangen kann, ist kein Fisch."

(gefunden in: Hans-Peter-Dürr, *Das Netz des Physikers, Naturwissenschaftliche Erkenntnis in der Verantwortung*, Hanser Verlag, München, 1988)

