Alexander Roßnagel
Peter Wedde
Volker Hammer
Ulrich Pordesch

DIE VERLETZLICHLKEIT DER 'INFORMATIONSGESELSCHAFT'

Elektronische Ausgabe

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

Alexander Roßnagel · Peter Wedde
Volker Hammer · Ulrich Pordesch

Die Verletzlichkeit der 'Informationsgesellschaft'

Sozialverträgliche Technikgestaltung Band 5

Herausgeber: Minister für Arbeit, Gesundheit und Soziales
des Landes Nordrhein-Westfalen

Die Schriftenreihe "Sozialverträgliche Technikgestaltung" veröffentlicht Ergebnisse, Erfahrungen und Perspektiven des vom Minister für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen initiierten Programms "Mensch und Technik - Sozialverträgliche Technikgestaltung". Diese Programm ist ein Bestandteil der "Initiative Zukunftstechnologien" des Landes, das seit 1984 der Förderung, Erforschung und sozialen 'Gestaltung von Zukunftstechnologien dient.

Der technische Wandel im Feld der Mikroelektronik und der modernen Informations- und Kommunikationstechnologien hat sich weiter beschleunigt. Die ökonomischen, sozialen, und politischen Folgen durchdringen alle Teilbereiche der Gesellschaft. Neben positiven Entwicklungen zeichnen sich Gefahren ab, etwa eine wachsende technologische Arbeitslosigkeit und eine sozialunverträgliche Durchdringung der Gesellschaft mit elektronischen Medien und elektronischer Informationsverarbeitung. Aber es bestehen Chancen, die Entwicklung zu steuern. Dazu bedarf es einer breiten öffentlichen Diskussion auf der Grundlage besserer Kenntnisse über die Problemzusammenhänge und Gestaltungsalternativen. Die Interessen aller vom technischen Wandel Betroffenen müssen angemessen berücksichtigt werden, die technische Entwicklung muß dem Sozialstaatspostulat verpflichtet bleiben. Es geht um sozialverträgliche Technikgestaltung.

Die Schriftenreihe "Sozialverträgliche Technikgestaltung" ist ein Angebot des Ministers für Arbeit, Gesundheit und Soziales, Erkenntnisse und Einsichten zur Diskussion zu stellen. Es entspricht der Natur eines Diskussionsforums, daß die Beiträge die Meinung der Autoren wiedergeben. Sie stimmen nicht unbedingt mit der Auffassung des Herausgebers überein.

Alexander Roßnagel · Peter Wedde
Volker Hammer · Ulrich Pordesch

Die Verletzlichkeit der 'Informationsgesellschaft'

3. Auflage (elektronische Fassung)

3. Auflage 2002/2009 durch die Autoren
(Im Text unveränderte elektronische Fassung, Veränderungen betreffen nur das Layout und den Seitenumbruch. Version: provet_PB1_3-Aufl_10_b.doc, Stand: 31. Oktober 2009)

Download über den Resolving-Dienst der Deutschen Nationalbibliothek
unter http://nbn-resolving.de/urn:nbn:de:hebis:34-2009103030803
oder von: http://www.provet.org/bib/f-pb-01.htm

1. Auflage 1989 und 2. Auflage 1990 Westdeutscher Verlag
Der Westdeutsche Verlag ist ein Unternehmen der Verlagsgruppe Bertelsmann

ISBN der gedruckten Fassung: 3-531-121137-5
URN der elektronischen Ausgabe: urn:nbn:de:hebis:34-2009103030803

INHALT

Vorwort

Computer sind bereits heute allgegenwärtig. Datennetze werden ausgebaut und immer dichter. Informations- und Kommunikationstechnik bestimmt zunehmend unser Leben. In Fabrikhallen steuern Computer Werkzeugmaschinen, Fertigungsstraßen und ganze Produktionsbereiche. Händler, Lieferanten, Banken und Kunden sind durch verzweigte Informationssysteme vernetzt. Staatliche Behörden verwalten die Bürger in riesigen Datenbanken. Sogar in das Privatleben dringt die Technik ein: Telespiele für Kinder, Bildschirmtext und Teleshopping für Erwachsene. - Und alles dies ist erst der Anfang. Wir sind auf dem Weg in die Informationsgesellschaft.

Viele drängen auf diesen Weg, weil sie hoffen, weil die Technik uns schwere gefährliche und stupide Arbeit abnimmt, uns von langweiligen und zeitraubenden Tätigkeiten befreit, die Fülle menschlichen Wissens jedem zugänglich macht, uns hilft, unser Denken und unsere Phantasie erst richtig zu entfalten, und bei alledem auch noch die wirtschaftliche Produktivität gewaltig steigert. Nüchterne Verfechter verweisen schlicht auf die Zwänge des Weltmarkts.

Wer aber fragt danach, was geschieht, wenn hochsensible Daten durch 'Trojanische Pferde' für Unberechtigte zugänglich werden, wenn sich in einem gesellschaftsweiten Computernetz Viren ausbreiten oder wenn lebenswichtige Informations- und Steuerungssysteme durch 'logische Bomben' zerstört werden? Welche sozialen Kosten in Form von Freiheits- und Demokratieverlusten wird die sichere 'Informationsgesellschaft' verursachen? Wird sie trotz großer Anstrengungen überhaupt das Maß an Sicherheit erreichen können, das bei einer hohen gesellschaftlichen Abhängigkeit von dieser Technik erforderlich wäre?

Nahezu täglich werden wir mit neuen Produkten und Verfahren konfrontiert. Die Informations- und Kommunikationstechnik wird in einem atemberaubenden Tempo fortentwickelt. Können in diesem 'Strudel' die genannten Risiken ausreichend berücksichtigt werden? Gesteuert wird die Entwicklung vor allem durch die Sichtweise von Technikern, durch das Machtstreben von Bürokraten und durch Gewinnerwartungen von Unternehmen. Diese Interessen sind jedoch blind gegenüber den meisten Folgen. In einer demokratischen Gesellschaft müssen in die Entwicklung solch gesellschaftsverändernder Technik auch die bisher ausgeblendeten Interessen eingehen. Vor allem aber müssen wir die Technik und das soziale Feld, in dem sie genutzt wird, so gestalten, daß die befürchteten gesellschaftlichen Risiken nicht Wirklichkeit werden.

Notwendig ist also eine sozialverträgliche Technikgestaltung. Was aber ist "sozialverträglich"? Um dieses Gestaltungsziel und die Gestaltungsaufgaben und -möglichkeiten zu konkretisieren, haben die Autoren als "Projektgruppe verfassungsverträgliche Technikgestaltung (provet)" von 1986 bis 1998 das Forschungsprojekt "Informatisierung der Gesellschaft: Verfassungsverträglichkeit und Verletzlichkeit des sozialen und politischen Systems" durchgeführt. Die Untersuchung war Teil des Forschungsprogramms 'Mensch

und Technik: Sozialverträgliche Technikgestaltung' des Landes Nordrhein-Westfalen. Ziel des Forschungsprojekts war, zwei Kriterien der Sozialverträglichkeit, nämlich die Verfassungsverträglichkeit der Informations- und Kommunikationstechnik und die Verletzlichkeit der Gesellschaft, zu konkretisieren, mit ihrer Hilfe Zukunftspläne zur 'Informationsgesellschaft' zu bewerten und Gestaltungsvorschläge für eine Technikentwicklung zu unterbreiten, die möglichst Freiheit und Demokratie verstärkt und die Verletzlichkeit der Gesellschaft verringert. Dieses Buch enthält den ersten Teil unserer Projektergebnisse: die Untersuchung der Verletzlichkeit der 'Informationsgesellschaft'.

Obwohl in dieser Studie kein Raum ist, Grundlagen der Informations- und Kommunikationstechnik zu vermitteln, haben wir uns bemüht, selbst schwierige technische Sachverhalte so darzustellen, daß sie auch für interessierte Laien verständlich sind. Dennoch sind technische Fachausdrücke bisweilen nicht zu vermeiden. Für solche Fälle enthält das Glossar im Anhang die notwendigen Erklärungen.

Für die Darstellung künftiger Gesellschaftsentwicklungen sowie die Abschätzung und Bewertung von Technikfolgen waren viele Gespräche mit Experten zu führen. Ohne von der Praxiserfahrung unserer Gesprächspartner zu profitieren - allein auf der Grundlage veröffentlichter Literatur - wäre diese Untersuchung nicht möglich gewesen. Für Ihre Gesprächsbereitschaft schulden wir ihnen Dank. Für die gute Zusammenarbeit seitens des Auftraggebers und des Projektträgers danken wir den Herren Ulrich von Alemann, Willi Riepert, Klaus Theo Schröder und Dieter Viefhues. Unser Dank gilt besonders auch Urs Andelfinger, Evelyne Billo, Uta Conze, Anne Flocken, Birgit Gumprecht-Riad Michael Schneider, Jochen Scholz, Robert Stramm, Matthias Teinert und Rainer Steen, die unsere Arbeit auf vielfältige Weise unterstützt haben.

Darmstadt, Bremen, Heidelberg und Miltenberg
im Januar 1989 Die Verfasser.

I. EINLEITUNG

1. Verletzlichkeit der Gesellschaft

Düsselberg, Montag 2. November 2019

6 Uhr 30
Ungläubig blickt Obersekretär Wilfried Schulz auf die Anzeige des Fernüberwachungssystems. Danach wären alle Telekommunikationsvermittlungsstellen im Zentrum von Düsselberg ausgefallen. Seit sechs Jahren arbeitet er im regionalen Netzkontrollzentrum von TELEKOM und hat noch nie erlebt, daß die softwaregesteuerte Vermittlung in drei Anlagen gleichzeitig ausgefallen war. Erfahrungen zur Genüge hat er dagegen mit unrichtigen Fehlermeldungen. Er vermutet also auch diesmal eine Fehlanzeige. Auf keinen Fall will er - wie beim letzten Mal - einen Fehlalarm auslösen.

6 Uhr 50
Der Bildschirm zeigt immer noch "Ausfall" an. Langsam wird Schulz unruhig. Er bespricht sich mit einem Kollegen. Der empfiehlt ihm, noch abzuwarten.

7 Uhr 00
Obersekretär Schulz entschließt sich, der Anzeige nun doch nachzugehen. Alle Versuche, telefonisch bei den Vermittlungsstellen nachzufragen, schlagen fehl. Auch über die separate Notverbindung meldet sich niemand. Über Funk alarmiert er schließlich die Polizeizentrale von Düsselberg. Auch dort bemüht man sich vergeblich, die örtlichen Polizeistationen über die üblichen Telekommunikationsverbindungen zu erreichen. Die Zentrale verständigt jedoch per Funk einige Streifenwagen, die in den Vermittlungsstellen nachsehen sollen.

7 Uhr 10
Ingenieur Ingo Scharf traut seinen verschlafenen Augen nicht. Der elektronische Weckdienst hat versagt. Als er sein Heiminformationssystem anschaltet, erhält er lediglich die Meldung, daß die Telekommunikationsverbindung unterbrochen ist. Das heißt: kein Fernsehen, keine elektronische Zeitung, keine elektronische Post. Er ist spät dran und verläßt hastig das Haus. Auf den Straßen herrscht Verkehrschaos. Die Ampelanlagen sind nicht mehr verkehrsgerecht geschaltet und die elektronischen Hinweistafeln zeigen keine Umwegempfehlungen mehr an. Auch der Bordcomputer empfängt keine Verkehrsflußdaten und kann ihm nicht helfen.

7 Uhr 13
Verärgert sitzt Familie Frei am leeren Frühstückstisch. Der Lebensmittelfrischdienst ist nicht gekommen. Entweder ist der Lieferwagen im Verkehrschaos steckengeblieben oder die aktuelle elektronische Bestellung von heute früh ist gar nicht mehr angekommen.

7 Uhr 25
Wegen des Verkehrsstaus erreichen die Polizeistreifen trotz Martinshorn erst jetzt die Ortsvermittlungsstellen in Atal, Bedorf und Ceheim und stellen über ihr Funknetz eine Verbindung zum Netzkontrollzentrum her. So erfahren nun Schulz und seine Kollegen, daß gegen 6 Uhr 20 in allen drei Anlagen die Vermittlungssysteme abgestürzt sind. Trotz großer Bemühungen ist es den Systemoperatoren vor Ort nicht gelungen, den Fehler zu finden. Entnervt können sie nur mitteilen, daß praktisch alle Kommunikationsverbindungen wie auch das Mobilfunknetz zusammengebrochen sind. An eine Benachrichtigung des Netzkontrollzentrums über die bisher unbenutzte Notrufverbindung hat in der Aufregung keiner gedacht.

7 Uhr 30
Auf der Mainzer Landstraße ist es zu einem schweren Verkehrsunfall gekommen. Weil der Notruf nicht funktioniert und der Verkehr so dicht ist, vergeht über eine Stunde, bis Krankenwagen und Notarzt am Unfallort sind. Im Krankenhaus ist der erforderliche Spezialist telefonisch nicht zu erreichen. Auch eine Videokonferenz mit anderen Spezialisten ist nicht möglich. Die improvisierte Notoperation kann das Leben der zwei Schwerverletzten nicht mehr retten.

7 Uhr 50
Ein Bote des großen Automobilherstellers erscheint in der Zentrale von TELEKOM und fordert unter Androhung von Schadensersatzforderungen, sofort mehrere Notverbindungen zu schalten. Ohne direkten Kontakt zu ihren Zulieferern würde in drei Stunden ihre gesamte Produktion zum Erliegen kommen.

8 Uhr 15
Ähnliche Forderungen nach bevorzugter Behandlung erreichen TELEKOM nun auch von einigen Banken. Der Ausfall von Telegeschäften mit Privat- und Geschäftskunden könnte kurzfristig noch verkraftet werden. Schwerer wiegt jedoch, daß sie keinerlei Bank- und Börsengeschäfte mit anderen Institutionen abwickeln können. Kurz darauf gehen die ersten Beschwerden von Versicherungsgesellschaften ein, denen jeder Kontakt zu ihren Zentralen, ihren Geschäftspartnern und ihren Vertretern fehlt. Später am Tag werden zahlreiche Kaufleute hohe Schäden geltend machen, weil sie wichtige Vertragsverhandlungen nicht führen und Angebote weder erhalten noch abschicken konnten.

8 Uhr 40
Ingenieur Scharf hat sein Büro erreicht. Die bisher eingetroffenen Kollegen stehen in den Fluren zusammen und versuchen, sich durch Bewegen warm zu halten. Die über das Fernwirksystem gesteuerte Zentralheizung wurde heute nicht hochgefahren, so daß in allen Räumen eine gleichmäßige Temperatur von 12 Grad herrscht. Aus dem Fenster sieht er, daß die Mitarbeiter der gegenüberliegenden Behörde auf der Straße stehen, weil die zentral verriegelten Türen nicht zu öffnen sind. Nach einiger Zeit beruhigt er sich mit dem Gedanken, daß er auch in warmen Räumen nicht arbeiten könnte, weil er für seine Arbeit, elektronisch einen Außenspiegel für das neue Automodell zu konstruieren, noch Daten aus der Zentrale benötigt, die er heute nicht erreichen kann.

8 Uhr 50
Die Spezialisten aus dem Netzkontrollzentrum sind inzwischen eingetroffen und beginnen mit der Schadensaufnahme. Alle drei Ortsvermittlungsstellen sind vollständig ausgefallen. Aus unerfindlichen Gründen ist ein Hochfahren der Anlage nicht möglich. Im Innenstadtbereich und den südlich angrenzenden Wohn- und Industriegebieten sind sämtliche Hauptanschlüsse außer Betrieb. Es ist kein Telefon, Text-, Bild- und Datenverkehr möglich. Störungen gibt es auch in anderen Anschlußbereichen, weil deren Verbindungen inzwischen überlastet sind.

9 Uhr 00
Auch Informatikstudent Frido ist aufgestanden und geht für die Wohngemeinschaft das Frühstück einkaufen. Aber im Handelszentrum des Stadtteils gibt es keine frischen Lebensmittel, keine Milch, keine Eier, keine Butter, keine Wurst, weil das Warenwirtschaftssystem ausgefallen ist. Die haltbaren Lebensmittel und der Rest von gestern sind schon beinahe ausverkauft, obwohl sie heute nur gegen das selten gewordene Bargeld abgegeben werden. Elektronisches Zahlen ist nicht mehr möglich, weil die Verbindungen von den Kassenterminals zu den Bankrechnern unterbrochen sind. Da Frido wie die meisten kein Bargeld dabei hat, bleiben er und seine Wohngemeinschaft heute morgen hungrig.

9 Uhr 15
Vor den wenigen Bankschaltern für Bargeld bilden sich Schlangen. Die Geldausgabeautomaten in der Stadt funktionieren nicht und die in den Bankfilialen sind schon lange leer. Später an diesem Tag werden auch die Bankschalter geschlossen. Zur gleichen Zeit drängen immer mehr Menschen in die Ortszentrale von TELEKOM, schildern aufgeregt ihre Notlage und fordern Telekommunikationsverbindungen.

9 Uhr 40

Im Rathaus wird ein Krisenstab aus Beamten von TELEKOM, der Polizei und der Stadtverwaltung gebildet, der den Schaden aufnehmen und Sofortmaßnahmen beschließen und einleiten soll. Sie stellen fest: Durch den Ausfall der Telekommunikation in den drei Stadtteilen ist das Verkehrsleitsystem, das Hinweise zum Verkehrsfluß und zu freien Parkplätzen gibt sowie die Ampeln nach der jeweiligen Verkehrsdichte steuert, außer Betrieb und der Verkehr im ganzen Stadtgebiet zusammengebrochen. Das Notrufsystem für Kranke und Alte funktioniert nicht und auch sonst kann keine medizinische Versorgung angefordert werden. Apotheken können keine Arzneimittel, Gewerbetreibende keine Waren von ihren Grossisten und Lieferanten bestellen. Und die Bürger können weder zu Behörden noch zu Banken, Versicherungen, Kaufhäusern und Dienstleistungsanbietern Telekontakte herstellen. Sie haben keine Möglichkeit, Taxen zu bestellen, Rechtsauskünfte einzuholen oder die Polizei zu rufen. Oft hilft es nicht einmal weiter, wenn die notwendigen Kontakte persönlich hergestellt werden können. Denn auch die direkt Angesprochenen sind fast ausnahmslos von der Telekommunikation abhängig oder können wegen des Verkehrschaos nichts liefern oder beziehen.

10 Uhr 30
Informatikstudent Frido wird - wie viele andere auch - nicht an der Televorlesung eines bedeutenden Professors aus Hamburg teilnehmen. Auch die Übungsaufgaben zur Vorbereitung aufs Diplom kann er sich nicht ausdrucken lassen. Der Bildschirm zeigt immer nur an: "Verbindung unterbrochen".

10 Uhr 45
Hausfrau Elke Frei ist an diesem Morgen in heller Aufregung. Nicht nur, weil keine Aufträge für ihre Telearbeit hereingekommen sind. Auch die Nachbesprechungskonferenz mit Dr. Hamberg wegen ihres Magenleidens findet nicht statt. Und der besonders abgestimmte Speiseplan kann nicht in ihr Heiminformationssystem übermittelt werden.

11 Uhr 30
Der Krisenstab tagt weiter. Der Bürgermeister wurde von der Polizei herbeigebracht. Mit ihm wird die Lage besprochen. Bisher konnte noch nicht geklärt werden, wodurch dieser Ausfall verursacht wurde. Ebensowenig läßt sich angeben, wann er behoben sein wird. Wenn der Fehler jedoch nicht bald gefunden und beseitigt wird, befürchtet der Krisenstab weitere Schäden. In den Industriebetrieben könnte die Produktion erschwert werden oder zusammenbrechen, weil Verbindungen zu Zulieferern und Kunden unterbrochen sind und zentrale Wissensbanken etwa für Werkstoffe oder Konstruktionen nicht mehr konsultiert werden können. Fernmeß- und Fernwirkdienste versagen. Sofern mit ihrer Hilfe kritische Produktionsprozesse gesteuert, Tankfüllungen gemessen oder Brände gemeldet werden, kann deren Ausfall zu großen finanziellen Schäden oder Gefahren für Gesundheit und Umwelt führen. Durch den Ausfall des elektronischen Zahlungsverkehrs und der Waren-

wirtschaftssysteme dürfte es zu größeren Versorgungsengpässen kommen. Wenn in dieser Situation bekannt wird, daß auch Fernüberwachungssysteme und Einbruchsmeldeanlagen nicht mehr funktionieren, ist mit Überfällen auf Banken und Plünderungen von Geschäften zu rechnen. Notfallsysteme im sozialen und medizinischen Bereich sind gefährdet. Behörden, die auf den Informationsaustausch mit anderen Behörden oder Bürgern angewiesen sind, können nicht arbeiten. Viele Dienstleistungsunternehmen die auf Telekommunikation angewiesen sind, dürften einen längeren Einnahmeausfall nicht verkraften können. Ein volkswirtschaftlicher Schaden in großer Höhe ist zu befürchten. Nach eingehender Diskussion entschließt sich der Krisenstab zu einer Pressemitteilung: "Aus noch ungeklärter Ursache sind heute drei Ortsvermittlungsstellen in Düsselberg ausgefallen. Sofortmaßnahmen zur Behebung des Schadens wurden eingeleitet. Es besteht kein Grund zur Beunruhigung. Der Krisenstab hat die Lage im Griff."

Das Kriterium der Verletzlichkeit

So oder so ähnlich könnte sich ein relativ begrenzter Schadensfall in einer informationstechnisch vernetzten Gesellschaft abspielen. Solche und ähnliche Möglichkeiten prägen jedoch nicht das gegenwärtige Bild einer 'Informationsgesellschaft'. Denn die Befürworter einer solchen, durch technisch vermittelte Informationsverarbeitung und Kommunikation bestimmten Gesellschaft stellen uns unter dieser Sammelbezeichnung nur deren positive Aspekte vor. Sie versprechen uns die Befreiung von schweren und stupiden Arbeiten, die Beseitigung menschlicher Fehlerquellen, die Unterstützung menschlichen Denkens, Wissens und sogar menschlicher Phantasie und - damit einhergehend - eine gewaltige Steigerung wirtschaftlicher Produktivität. Werden diese Versprechen aber je eingelöst werden können, wenn die neue Technik mißbraucht werden oder versagen kann und dadurch große Schäden zu befürchten sind?

Die "Informationsgesellschaft" wird uns als eine offene Gesellschaft freier Informationsflüsse beschrieben, in der das Individuum sich intellektuell frei entfalten und die Gesellschaft demokratischer werden kann.[1] Welche gesellschaftlichen Folgen für Freiheit und Demokratie werden jedoch all jene Anstrengungen haben, die notwendig sind, um große Schäden zu verhindern?

Die Kritiker dieser Technik-'Euphorie' machen geltend, der Weg in die 'Informationsgesellschaft' werde Kommunikationsbeziehungen aushöhlen, lebendige Arbeit verdrängen und vor allem die private und staatliche Kontrolle individuellen Verhaltens und gesellschaftlicher Beziehungen steigern. Sie wollen den "Überwachungsstaat" verhindern. Ist dies aber überhaupt möglich, wenn die Gesellschaft von der neuen Technik so abhängig ist, daß sie deren Sicherungszwang nachgeben muß?

1 S. z.B. BDI 1988, 63; Haefner 1989; ders. 1984, 179 ff.

Die Informatisierung der Gesellschaft ist nicht zu verhindern. Negativen Auswirkungen einer künftigen 'Informationsgesellschaft' vorzubeugen, erfordert daher, die Technik und ihre Anwendungen nach Kriterien der Sozialverträglichkeit zu gestalten. Wie keine anderen bisher sind die Informations- und Kommunikations(IuK)-Techniken zum Zeitpunkt ihrer Einführung ebenso gestaltungsfähig wie -bedürftig. Wie aber kann und soll der breite Spielraum technischer Alternativen genutzt werden, um zu verhindern, daß die Verletzlichkeit der Gesellschaft weiter erhöht wird oder nur unter nicht akzeptablen Bedingungen gering gehalten werden kann?

Alle diese Fragen zeigen, welch großer Wissensbedarf über die Zusammenhänge zwischen Informatisierung und gesellschaftlicher Verletzlichkeit besteht. Obwohl die Verletzlichkeit einer künftigen 'Informationsgesellschaft' ein wichtiges Kriterium jeder sozialverträglichen Technikgestaltung ist, fehlt es bisher jedoch an einschlägigen Untersuchungen. Zwar wurden viele Studien in Auftrag gegeben, um festzustellen, wie die Verfügbarkeit technischer Systeme gewährleistet werden kann, doch betrachten diese nie die gesellschaftlichen Folgen eines Systemausfalls. Zwar gibt es einige Studien zur Sicherung der Datenverarbeitung, doch sind diese auf die heutigen Probleme und auf konkrete Handlungsempfehlungen für Sicherungsmaßnahmen beschränkt. Zwar finden sich auch Darstellungen von Fällen zur 'Computerkriminalität', doch kommen diese selten über spektakuläre Fälle der Vergangenheit hinaus. Wissenschaftliche Untersuchungen zu diesem Thema sind auf kriminologische Fragestellungen begrenzt. Die einzige uns vorliegende Untersuchung, die die Verletzlichkeit der Gesellschaft durch die IuK-Technik zum Gegenstand hatte, ist die Studie des schwedischen 'Verwundbarkeits-Komitees' (SARK) "Datenverarbeitung und die Verwundbarkeit der Gesellschaft". Sie ist allerdings inzwischen zehn Jahre alt, wurde für Schweden erstellt, hatte ein ausdrücklich militärisches Erkenntnisinteresse und war überwiegend gegenwartsbezogen. Wenn wir hier eine zukunftsorientierte Studie vorlegen, die unter dem Blickwinkel von Gestaltungsalternativen untersucht, welchen Einfluß die IuK-Technik auf die Verletzlichkeit der Gesellschaft haben kann, betreten wir wissenschaftliches Neuland.

Das zu untersuchende Problem entsteht vor allem dadurch, daß *gesellschaftliche Funktionen* von Menschen *auf Informations- und Kommunikationssysteme übertragen* werden, also auf technische Systeme, die auf der Basis der Mikroelektronik Verfahren der Datenverarbeitung und der Nachrichtentechnik zur Automatisierung von Informationsverarbeitung und -übertragung nutzen. Die Übertragung sozialer Funktionen ist möglich, weil die IuK-Systeme es erlauben, die Verarbeitung von Informationen aus den Gehirnen der Menschen herauszunehmen, sie zu verselbständigen und ihren Austausch technisch zu verwirklichen. Informationsverarbeitung und Kommunikation werden dadurch vom Funktionieren einer Technik abhängig, auf die sich die Menschen verlassen. Im Vertrauen auf die Technik erhöhen sie deren Leistungsfähigkeit - und damit zugleich das Schadenspotential. Durch diese Übertragung werden zudem Informationsverarbeitungs- und Kommunikationsprozesse für Dritte zugänglich. Sie können diese leichtfertig oder mißbräuchlich

ausforschen, manipulieren, unterbinden, beschädigen oder zerstören. Fehler und Manipulationen können so die Erfüllung der dem technischen System übertragenen gesellschaftlichen Funktionen beeinträchtigen.

Allgemein bezeichnet *Verletzlichkeit* die Möglichkeit, die Funktionsfähigkeit eines Systems so zu stören, daß es von einem erwünschten in einen unerwünschten Zustand überführt wird, daß also Schäden verursacht werden.[2] Diese Definition ist für unsere Fragestellung allerdings noch zu unpräzise. Wir müssen die Begriffe des Systems, des Schadens und des Störens näher bestimmen.

Welches *System* soll der Bezugspunkt der zu untersuchenden Verletzlichkeit sein? Unser Erkenntnisinteresse gilt nicht dem technischen System als solchem, sondern der *Funktionsfähigkeit des sozialen und politischen Systems*. Entscheidend ist also nicht, ob eine Datenbank oder ein Netzwerk beschädigt wird oder ausfällt. Relevant für uns sind die gesellschaftlichen Folgewirkungen. Können diese vermieden werden, so ist der technische Ausfall als solcher für die Verletzlichkeit der Gesellschaft ohne Bedeutung. Um diese Unterscheidung sprachlich zu verdeutlichen, wollen wir im folgenden von der *Verwundbarkeit* des technischen Systems und der dadurch möglichen *Verletzlichkeit* des sozialen und politischen Systems sprechen. Zu fragen ist also, welchen *sozialen* oder *politischen* Schaden der Funktionsverlust eines technischen Systems anrichtet.

Die Festlegung des Bezugssystems liefert auch gleich ein Kriterium, um zu bestimmen, welcher Zustand erwünscht oder unerwünscht ist bzw. welche *Schäden* vorrangig zu untersuchen sind. Um das Kriterium der Verletzlichkeit für die politische Diskussion über Technikalternativen zu konkretisieren, ist die Betrachtungsperspektive von Allgemeininteressen, wie sie etwa im Grundgesetz von allen anerkannt formuliert sind, zu wählen.[3] Als Schäden gelten danach nicht nur finanzielle Verluste, sondern vor allem die Beeinträchtigung der physischen und psychischen Integrität einzelner und der Bevölkerung insgesamt, der informationellen Selbstbestimmung und anderer Grundrechte sowie der sozialen und politischen Zielsetzungen des demokratischen und sozialen Rechtsstaats. Schäden, die bei einzelnen auftreten, stehen danach vor allem dann im Mittelpunkt der Untersuchung, wenn sie indirekt auch das Allgemeininteresse berühren.

Die wirtschaftlichen Verflechtungen zwischen Allgemeininteressen und Partikularinteressen dürfte allerdings in vielen Fällen dazu führen, daß Schäden bei einzelnen auch zu Nachteilen für die Allgemeinheit führen. Große finanzielle Verluste einer Bank etwa können zu wirtschaftlichen Einbußen für weite Teile der Bevölkerung, zu einer Störung des Zahlungsverkehrs und zu volkswirtschaftlichen Verlusten führen. Der Produktionsausfall in einem großen Betrieb kann Versorgungsstörungen, Komforteinbußen, Wettbewerbsnachteile und den Verlust von Arbeitsplätzen nach sich ziehen. Die Zerstörung der Da-

2 S. z.B. Otto/Sonntag 1985, 135.

3 Hier zeigt sich eine inhaltliche Nähe zur Prüfung der Verfassungsverträglichkeit, dem zweiten Kriterium der Sozialverträglichkeit, das in unserem Projekt untersucht wurde - s. hierzu Roßnagel, SoTech-Rundbrief Nr. 5 (1987), 22 ff.; s. hierzu auch ders. RuP 1987, 4 ff. und 1989.

tenverarbeitungsanlage eines Adressenhändlers dürfte nach diesem Kriterium allerdings aus dem Untersuchungsfeld herausfallen.

Die *Größe des möglichen Schadens* hängt ab von der gesellschaftlichen Funktion, die auf die Technik übertragen wird. Mit der Technik kann dann im schlimmsten Fall auch diese Funktion ausfallen. Wird der Bordingenieur eines Flugzeugs durch einen Computer ersetzt, kann eine Störung dieses Computers zu 'Fehlhandlungen' des elektronischen 'Bordingenieurs' und sogar zu einem Absturz des Flugzeuges führen. IuK-Technik ermöglicht aber auch, die übertragene Funktion zu verändern und damit die Größe des Schadenspotentials zu beeinflussen. Sie vermag die Leistungsfähigkeit von Computern oder Datennetzen ebenso zu erhöhen wie die der 'alten' Technik, in die sie integriert wird. Mit Hilfe elektronischer Steuerung können Eisenbahnen erheblich schneller fahren, können die Sicherheitsmargen in chemischen Prozessen reduziert, die Lager von Produktionsbetrieben verkleinert oder die Bearbeitung und Durchführung von Geldgeschäften gesteigert werden. Sie könnte aber auch das Schadenspotential verringern, wenn mit ihrer Hilfe gesellschaftliche Funktionen verteilt werden. Werden zum Beispiel die bisher bei einem Ministerium zentralisierten Informationen und Aufgaben auf nachgeordnete Verwaltungsbehörden übertragen, hat der Ausfall einer Funktionseinheit nur noch regional begrenzte Wirkungen.

Die Definition des *Störens* ist ebenfalls auf das zu untersuchende System zu beziehen: Die IuK-Technik wirkt als Mittel, das den Schaden für das soziale und politische System anrichtet. Der Begriff des Störens ist bezogen auf die gesellschaftliche Funktion, die die Technik übernehmen soll. Diese wird in der Regel bestimmt durch den jeweiligen Eigentümer oder Verfügungsberechtigten oder für die Allgemeinheit durch die zuständigen staatlichen Organe.

Die Ursachen, die zu Schäden führen, können unterschieden werden in die Auslösung von Schadensereignissen, die von Menschen zu verantworten sind, und solche, die Menschen nicht verantworten müssen, weil sie vor allem auf Naturkatastrophen oder höhere Gewalt zurückgehen. Zufällige Störungen und fahrlässige Fehler verursachen zwar die Mehrzahl der Schäden. Von großen Naturkatastrophen abgesehen, können aber alle so entstandenen Schäden auch vorsätzlich herbeigeführt werden. Da vorsätzliches Handeln darüberhinaus weitere Schäden anrichten kann, führt es zu einem breiteren Schadensspektrum. Vorsätzliche Aktionen sind somit die 'Umhüllenden', die das Schadenspotential anderer Ursachen abdecken. Dies erklärt, warum im folgenden der Scheinwerfer systematischer Untersuchung vor allem auf jene gerichtet ist.

Vorsätzliche Aktionen, die die gesellschaftliche Funktion stören, die auf die IuK-Technik übertragen wurde, wollen wir Mißbrauch nennen. *Mißbrauch* ist danach jeder Umgang mit der IuK-Technik, der nicht ihrer gesellschaftlich akzeptierten Funktionsbestimmung entspricht. Nicht jeder Mißbrauch muß allerdings rechtswidrig oder strafbar sein. Der Begriff des Mißbrauchs wird hier enger verstanden als im allgemeinen Sprachgebrauch. Als Mißbrauch wird gewöhnlich jede Techniknutzung bezeichnet, die zu nega-

tiv bewerteten Folgen führt. Ein Gewerkschafter dürfte Personalinformationssysteme, betriebliche Rationalisierungsmaßnahmen oder die polizeiliche Erfassung von Demonstrationsteilnehmern als Mißbrauch bezeichnen. Der Arbeitgeber oder der Polizeichef würden dem aber widersprechen. Für ein allgemein akzeptiertes Kriterium der Technikbewertung taugt dieser interessenabhängige Mißbrauchsbegriff nicht. Außerdem kann durch ihn nicht der Unterschied zwischen der Funktionslogik eines IuK-Systems und dem Verstoß gegen dieselbe erfaßt werden. Auch der bestimmungsgemäße Gebrauch der IuK-Technik kann negative Folgen für das soziale und politische System nach sich ziehen. Diese können zum Beispiel am Maßstab der Verfassungsverträglichkeit gemessen und bewertet werden. Dies soll allerdings nicht hier, sondern in einer weiteren Untersuchung erfolgen.

Wir wollen daher den *Mißbrauch* von dem *Gebrauch* der IuK-Technik unterscheiden und uns hier auf die funktionswidrige Nutzung der IuK-Technik konzentrieren. Das Abhören fremder Kommunikation durch einen Privatmann fällt danach in das Untersuchungsfeld der Verletzlichkeit, während die gleiche Tätigkeit, entsprechend ihrem gesetzlichen Auftrag ausgeübt von Behörden der inneren Sicherheit, nach dem Kriterium der Verfassungsverträglichkeit zu beurteilen wäre. Um allerdings die Verwendung des Computers zu Betrugszwecken oder die gegen eine Betriebsvereinbarung verstoßende Rasterfahndung in einem Personalinformationssystem auch als Mißbrauch erfassen zu können, messen wir die Funktionsbestimmung des IuK-Systems an gesellschaftlichen Normen. Elektronische Fahndungsmaßnahmen der Polizei wären daher als Mißbrauch zu werten, solange sie ohne Rechtsgrundlage durchgeführt werden. Sobald der Gesetzgeber diesen Gebrauch von IuK-Systemen billigt, sind die Folgen dieser Normabweichung nicht mehr im Rahmen einer Verletzlichkeitsanalyse zu bewerten. Vielmehr ist die Funktionslogik dieses Technikgebrauchs dann auf ihre Verfassungsverträglichkeit hin zu überprüfen.

Unter *Verletzlichkeit* verstehen wir also die *Möglichkeit großer Schäden für die Gesellschaft*. Sie kann durch die IuK-Technik beeinflußt werden, indem sie das *Schadenspotential oder die Fehler- und Mißbrauchsmöglichkeiten technischer Systeme verändert*.

2. Methode und Gang der Untersuchung

Wer mit gesundem Optimismus den technischen Wandel forciert und darauf vertraut, daß die gesellschaftlichen Probleme später schon in den Griff zu bekommen sind, verkennt, daß bereits heute die Grundlagen für die künftigen Entwicklungen gelegt werden. Heutige Entscheidungen begründen Sachzwänge und bereiten Anschlußzwänge vor, eröffnen oder verschütten Entwicklungsmöglichkeiten, die sich vielleicht erst in später Zukunft bemerkbar machen oder voll auswirken. Zur Bewertung heutiger Entscheidungen müssen auch deren künftige Auswirkungen berücksichtigt werden.

Ziel der Untersuchung ist daher, eine Vorstellung zu erarbeiten, wie eine künftige 'Informationsgesellschaft' aussehen könnte (Teil II), deren Verletzlichkeit qualitativ zu analysieren (Teil III), um daraus Schlußfolgerungen für die Gestaltung bestehender sozio-technischer Entwicklungsalternativen zu ermöglichen (Teil IV).

Wir beschränken uns in unserer Untersuchung auf den 'zivilen' Aspekt der Verletzlichkeit. Wir berücksichtigen zwar Einflüsse des Rüstungswettlaufs auf die zivile IuK-Nutzung und verwenden einige illustrierende Beispiele aus dem militärischen Bereich, untersuchen aber systematisch weder die Anwendung von IuK-Technik zu kriegerischen Zwecken noch den Krieg als Schadensursache. Der militärische Aspekt der Verletzlichkeit hat weitgehend andere Gründe und erfordert andere technische, organisatorische und politische Strategien zu ihrer Beseitigung. Diese detailliert zu analysieren, erfordert eine eigene Untersuchung. Wir haben uns außerdem auf den zivilen Aspekt beschränkt, weil es im Gegensatz zu diesem zu Fragen wie einem 'Atomkrieg aus Versehen' oder dem elektromagnetischen Puls bereits ausführliche Untersuchungen gibt.[1] Die Verletzlichkeit der Gesellschaft läßt sich erst vollständig beurteilen, wenn ihr ziviler und militärischer Aspekt zusammen gesehen werden. Insofern untersuchen wir die Verletzlichkeit der Gesellschaft durch die IuK-Nutzung nicht abschließend. Und es ist uns sehr wichtig, darauf ausdrücklich hinzuweisen: das Problem der Verletzlichkeit ist noch erheblich größer, als unser Bericht andeutet.

Das Zukunftsbild einer 'Informationsgesellschaft'

Kriterien der Technikbewertung und Vorschläge zur Technikgestaltung können politische Relevanz nur in geschichtlichen Verzweigungssituationen gewinnen. Die Freiheit, nach diesen zu entscheiden, setzt Handlungsalternativen voraus. Fehlen diese, können nur Sachzwänge vollzogen und deren negative Folgen beklagt werden. Daher wäre es auch im Fall der IuK-Techniken ideal, wenn unterschiedliche Entwicklungsmöglichkeiten auf ihre Verletzlichkeit hin bewertet werden könnten. Die intensive Diskussion in der Öffent-

1 S. z.B. Frei oder die Jahrbücher des Stockholm International Peace Research Instituts.

lichkeit hatte es zum Beispiel der Enquete-Kommission "Zukünftige Kernenergie-Politik" möglich gemacht, vier politisch repräsentative Entwicklungs'pfade' des Energiesystems zu beschreiben. Diese konnten dann auf ihre Verletzlichkeit hin untersucht werden.[2] Im Gegensatz zur Energiediskussion wurden im politischen Diskurs um die Nutzung der IuK-Technik bisher immer nur einzelne Folgen kritisiert. Konsistente Alternativen zu den Konzern- und Bürokratiestrategien wurden in dieser 'Arena' bisher noch nicht erörtert.

Zwar gab es einige wissenschaftliche Versuche, durch das Aufzeigen von Entwicklungsalternativen diese Diskussion anzustoßen.[3] Im Rahmen des nordrhein-westfälischen Programms "Sozialverträgliche Technikgestaltung" etwa wurden jüngst vier Optionen der Telekommunikation vorgestellt[4] und weitere spezifische Szenarien geschrieben. Sie wurden entwickelt, um am Verhältnis von Mikroelektronik und Arbeitsmarkt beispielhaft zu zeigen, daß auch Betroffene an der Erstellung von Zukunftsbildern beteiligt werden können[5], um Kriterien der Sozialverträglichkeit an ihnen zu testen[6] oder verschiedene wirtschaftliche Entwicklungsmöglichkeiten einer Region zu demonstrieren.[7] Diese Szenarien sind jedoch für eine Analyse der Verletzlichkeit nur beschränkt geeignet. Sie sind zu sehr durch ein spezifisches Erkenntnisinteresse geprägt, und meist fehlen gerade die unter Verletzlichkeitsaspekten relevanten Merkmale. Sie können daher nicht Ausgangspunkt, sondern nur Hilfsmittel unserer Analyse sein.

Die Untersuchung kann also nicht an politisch relevanten Alternativen anknüpfen, sondern muß vielmehr dazu beitragen, solche zu entwickeln. Wir haben uns daher entschieden, *ein Zukunftsbild - als Fortschreibung heute absehbarer Trends* - zu zeichnen, und wollen Ansätze für Alternativen aus der Kritik dieser Trendentwicklung gewinnen. Wir zielen auf eine Beschreibung des Trends, weil es aufgrund der atemberaubenden Geschwindigkeit IuK-technischer Entwicklungen vor allem darauf ankommt, die Folgen anstehender Entscheidungen zu bestimmen und möglichst schnell im Sinne sozialverträglicher Technikgestaltung zu beeinflussen.

Zwar gibt es, ebensowenig wie es *das* Kapital oder *den* Staat gibt, auch nicht *den* Trend. Auch künftig wird es unterschiedliche Kapital- und Bürokratiestrategien und daher ebenso unterschiedliche Entwicklungstrends geben. Dennoch wird es nur eine Wirklichkeit geben, in der widersprüchliche Entwicklungstendenzen nebeneinander bestehen, sich gegenseitig bremsen oder zu einer neuen Entwicklung vereinen. Diese unterschiedlichen Interessen und Strategien gilt es zu berücksichtigen. Folglich kann selbst ein aus

2 S. z.B. Roßnagel 1983a; ders. 1984a; Meyer-Abich/Schefold 1986, 61 ff.

3 S. z.B. Reese/Lange 1984 für politische Strategien in der Bundesrepublik; Manto 1986 für die Auswirkungen auf Siedlung und Verkehr in der Schweiz.

4 S. Berger/Kühn/Kubicek/Mettler-Meibom/Voogt 1988.

5 S. Baumgartner u.a.

6 S. Müller-Reißmann/Bohmann/Schaffner.

7 S. Gleich/Lucas/Schleicher.

den Visionen der Mächtigen entwickeltes Zukunftsbild ebensowenig wie die Zukunft selbst völlig widerspruchsfrei sein.

Das im zweiten Teil dargestellte Zukunftsbild einer 'Informationsgesellschaft' ist keine Prophezeiung. Es kann vom Anspruch her schon deswegen keine sein, weil es zu Gestaltungsmaßnahmen führen soll, die negative Entwicklungen, soweit sie hier beschrieben werden, künftig verhindern. Es geht also nicht darum, die Zukunft vorherzusagen, sondern um eine *kritische Überprüfung heutiger Zukunftswünsche*. Das Zukunftsbild ist keine Antwort auf die Frage: Wie wird die Zukunft sein? Es will vielmehr durch die Information über eventuell unbedachte Folgen zu einer rationalen Klärung der Frage beitragen: Welche Zukunft sollen wir wollen?

Das folgende Zukunftsbild ist eine bedingte Prognose. Da wir die Zukunft nicht kennen können, orientieren wir uns an den Interessen, Plänen und Hoffnungen, die die künftige Entwicklung wohl am stärksten bestimmen werden. Das Zukunftsbild ist also ein *Gedankenexperiment*, das eine mögliche Zukunft der gesellschaftlichen Bereiche, die für die Beurteilung der IuK-Technik relevant sind, unter der Voraussetzung beschreibt, daß sich die gegenwärtigen Trends fortsetzen und die (im doppelten Sinn) mächtigen Visionen realisieren. Es ist insoweit bedingt, als es bestimmte Randbedingungen der Entwicklung unterstellt und große Krisen oder gar Trendbrüche ausschließt. Seine Aussagekraft ist durch diese Bedingungen begrenzt. Da diese aber explizit dargestellt werden, kann das Zukunftsbild nachvollzogen, kritisiert und verbessert werden.

In einem ersten Schritt sind die wichtigsten Randbedingungen der künftigen Technikanwendung zu identifizieren. Sie können hier nicht im Detail hergeleitet werden, sondern werden mit einem gewissen Anspruch auf Plausibilität als Annahmen gesetzt (Kap. 3). Danach sind die für den Ausbau des IuK-Systems relevanten Techniken zu bestimmen (Kap. 4). In einem dritten Schritt sind dann die wichtigsten Anwendungsbereiche und -formen der IuK-Technik abzuschätzen. Dabei gilt es zu versuchen, gegliedert nach sozialen Subsystemen Interessen und Bedürfnisse gesellschaftlicher Gruppen in Beziehung zu möglichen Anwendungen der Technik zu bringen (Kap. 5). In einem vierten Schritt ist dann die künftige gesellschaftliche Wirklichkeit so darzustellen, wie sie sich ergibt, wenn man versucht, die zuvor getrennt betrachteten Entwicklungen in einzelnen gesellschaftlichen Bereichen als Ganzes zu sehen. Dies soll exemplarisch für das Arbeitsleben und den Alltag unternommen werden (Kap. 6). Das Zukunftsbild versucht, auf engem Raum ohne Bewertung eine möglichst umfassende Darstellung künftiger Technikentwicklung und -nutzung zu geben, die jedem Leser eine eigene Bewertung der Vor- und Nachteile ermöglicht.

Zur zeitlichen Strukturierung des Zukunftsbildes haben wir zwei Orientierungspunkte gewählt:

- *bald* - in etwa 10 Jahren - also um das Jahr 2000
- *später* - in etwa 20 bis 30 Jahren - also um das Jahr 2020.

Wir sind uns des Wagnisses bewußt, in einem wissenschaftlichen und politischen Diskurs Aussagen zu gesellschaftlichen Verhältnissen über einen so langen Zeitraum zu treffen. Viele technische Systeme werden erst noch konzipiert und entwickelt. Wie kann da heute bereits angegeben werden, wie sie in 20 oder 30 Jahren angewendet und welche sozialen Folgen sie haben werden? Wäre es unter diesen Umständen nicht sinnvoller, sich auf einen Zeitrahmen von drei bis fünf Jahren zu beschränken? Gleichzeitig müssen wir aber annehmen, daß Entscheidungen von heute Auswirkungen haben können, die selbst den von uns gewählten Zeitrahmen weit übersteigen. Die Grenzen unserer Prognosefähigkeit, die Beschränktheit des Wissens um künftige Technikrisiken und um nützliche Anwendungen, führen uns in ein Dilemma. Die sozialen Auswirkungen eines Technik-Systems können nur für einen sehr kurzen Zeitraum relativ sicher vorhergesagt werden. Sind die künftigen Auswirkungen klar erkennbar, ist es für gestalterische Maßnahmen meist zu spät.

Genausowenig wie wir können die 'Entscheidungsträger' in Staat und Wirtschaft die Zukunft kennen. Sie aber treffen heute Entscheidungen, die noch in 20 oder 30 Jahren die Lebensverhältnisse bestimmen werden. Auf welcher Grundlage schätzen *sie* den gesellschaftlichen Bedarf, die volkswirtschaftlichen Kosten, die Umwelteinwirkungen und die Sozialverträglichkeit ihrer Entscheidungsfolgen ein - wenn sie dies überhaupt versuchen? Auch sie können dem beschriebenen Dilemma nur entgehen, indem sie unter Berücksichtigung des gesamten Wissens, das wir von unserer Zukunft haben können, versuchen, auch die zeitlich weiter entfernten Folgen zu beschreiben. Auf der gleichen Grundlage und mit dem gleichen Anspruch auf Seriosität ist es möglich (und notwendig), diese Zukunftsvisionen in einem Gedankenexperiment daraufhin zu überprüfen, wie sozialverträglich die Verhältnisse wären, in die sie uns führen wollen. Nur durch ein solches gedankliches Probehandeln können wir verlustarm lernen, Zukunftsrisiken bewußt zu reduzieren und Zukunftschancen zu nutzen. Ein solches Vorgehen ist also die Voraussetzung jedes demokratischen Diskurses über künftige Techniknutzung.

Aus diesem Grund haben wir auch versucht, eine Zukunftsmöglichkeit mit einer großen Verwirklichungschance darzustellen. Das Zukunftsbild wurde daher orientiert an den vermutlich geschichtsmächtigsten Visionen und von den Interessen her konstruiert, die sich entsprechend den politischen Kräfteverhältnissen wohl am ehesten durchzusetzen vermögen. Deren Zukunftsvorstellungen werden konzeptualisiert, um sie dann später von ihren bedachten und unbedachten positiven und negativen Folgen her bewerten zu können. Auch wenn wir zum Beispiel skeptisch sind, ob sich die Träume einer computerintegrierten Fabrik oder eines Glasfaseruniversalnetzes verwirklichen lassen, haben wir diese Konzeptionen zum Ausgangspunkt unserer Untersuchung genommen und nur im Hinblick auf übertriebene Erwartungen kupiert. Dieser Ansatz erfordert folgende Konstruktionsmerkmale für das Zukunftsbild:

- Hinsichtlich der verfolgten Ziele müssen sich die 'Zurechnungssubjekte', die Verantwortlichen in Wirtschaft und Politik, in dem Bild wiederfinden können, (Zieltreue).

- Das Zukunftsbild muß hinsichtlich der technischen, wirtschaftlichen und gesellschaftlichen Elemente in sich schlüssig sein (Konsistenz).
- Es muß - die Ziele als gegeben unterstellt - von möglichst realistischen Annahmen ausgehen (Realismus).

Um dieses Ziel zu erreichen, wurden in einer modifizierten Delphi-Methode die im Anhang aufgeführten Experteninterviews durchgeführt und die dort benannte Literatur ausgewertet. In besonderem Maß wurden die bis zum Jahr 2020 reichenden Planungen der Deutschen Bundespost[8], die bis zum Jahr 2000 und weiter reichenden Empfehlungen der deutschen Industrie[9], die Empfehlungen der EG[10], die Untersuchungen des Bundestags[11], der Bundesregierung[12], der Regierungen der Länder[13] und viele weitere offizielle Dokumente und Stellungnahmen von "Entscheidungsträgern" in Wirtschaft und Staat berücksichtigt.[14]

Ein Vorentwurf des Zukunftsbildes wurde von weiteren Experten kritisch überprüft und entsprechend korrigiert. Dadurch hoffen wir, die Beschreibung einer wahrscheinlichen Zukunft vorlegen zu können, die als Grundlage der politischen Diskussion über die Verletzlichkeit der IuK-Technik breit akzeptiert werden kann. Trotz der Orientierung an den durchsetzungsfähigsten Interessen und den herrschenden Trends müssen unterschiedliche Einschätzungen und widersprüchliche Informationen subjektiv bewertet und mit viel Phantasie zu einem 'Gesamtkunstwerk' verbunden werden. Letztlich ist und bleibt es daher ein Zukunftsbild der Autoren.[15]

Die Verletzlichkeitsananlyse

Die so dargestellte 'Informationsgesellschaft' wird im dritten Teil auf ihre Verletzlichkeit hin überprüft. Zu diesem Zweck werden ihre hierfür relevanten Teile - wiederum nach der Methode der Trendprognose - weiter präzisiert. Während jedoch das zuvor beschriebene Zukunftsbild von den Visionen der Entscheidungsträger und den technischen und gesellschaftlichen Vorbedingungen her erst konstruiert werden mußte, wird dieses nun vorausgesetzt und auf seine Konsequenzen hin untersucht. Während das Zukunftsbild bean-

8 BMPF 1984.

9 S. Bericht der vier Arbeitsgruppen an die Bundesregierung "Informationstechnik 2000", 10. Juni 1987; BDI 1988.

10 EG-Kommission 1987.

11 S. Enquete-Kommissionen "Neue Informations- und Kommunikationstechniken" - BT-DrS 9/2442 und "Technikfolgenabschätzung" - BT-DrS 10/6801 und die dazugehörenden Materialien.

12 S. BMFT 1984.

13 S. z.B. Innenminister NRW; Landesregierung NRW; Diebold/Dornier/Ikoss; Landesregierung Baden-Württemberg.

14 S. hierzu das Literaturverzeichnis.

15 Aus diesem Grund wurde auch auf Anmerkungen zu dem Zukunftsbild verzichtet.

sprucht, von den unterschiedlichsten Interessen als realistische Beschreibung der Trendentwicklung und damit als gemeinsame Diskussionsgrundlage akzeptiert zu werden, will die ihm folgende Analyse die Diskussion um die Verletzlichkeit der Gesellschaft überhaupt erst eröffnen.

Die Umsetzung dieses Vorhabens stößt auf eine Reihe methodischer Schwierigkeiten:

(a) Die künftige Entwicklung eines IuK-Systems kann aufgrund ihrer Komplexität weder vollständig abgeschätzt noch beschrieben werden. Weder die Möglichkeiten der technischen Entwicklung noch die Menge der künftigen Anwendungen von IuK-Technik lassen sich mit einem Anspruch auf Vollständigkeit beschreiben.
(b) Selbst für die beschriebenen Techniken und Anwendungen ist es ebensowenig möglich, sämtliche Fehler und Sicherheitstechniken, Angriffs- und Verteidigungsmöglichkeiten in allen möglichen Kombinationen zu untersuchen, wie die Schadensfolgen bis in ihre letzten Verzweigungen zu verfolgen.
(c) Das Gewicht eines Schadens und damit seine Bedeutung für die Verletzlichkeit der Gesellschaft läßt sich auch unter Berücksichtigung verfassungsrechtlicher Vorgaben letztlich nur politisch bestimmen. Eindeutige Kriterien für die Bestimmung des Allgemeininteresses gibt es nicht.

Die Lösung dieser methodischen Probleme kann nur pragmatisch erfolgen. Für die Probleme (a) und (b) empfiehlt sich eine exemplarische Auswahl, die sich an der Bedeutung orientiert, die das technische System oder der durch einen Angriff anzurichtende Schaden für die Interessen der Allgemeinheit hat. Dieser Lösungsversuch leitet damit über zum Bewertungsproblem (c). Die Bedeutung, die einer Mißbrauchsmöglichkeit, einer Sicherungsmaßnahme, einer Schadensfolge oder einem Verletzlichkeitsaspekt zukommt, ist als eine Frage politischer Bewertung im demokratischen Willensbildungsprozeß zu bestimmen. Wir können letztlich nur versuchen, die untersuchte Technik, die Anwendungsfälle und die Mißbrauchs- und Schadensmöglichkeiten so auszuwählen, daß sie im Hinblick auf das Ziel der Untersuchung von der Mehrzahl der an der politischen Diskussion Beteiligten akzeptiert werden können: Ihre Darstellung soll eine Grundlage dafür sein, die Verletzlichkeit eines bestimmten IuK-Systems zu bewerten und Schlußfolgerungen für die Technikgestaltung zu ziehen.

Zur *Beurteilung der Verletzlichkeit* ist sowohl das Ausmaß möglicher Schäden als auch die Wahrscheinlichkeit der schadensauslösenden Ereignisse abzuschätzen. Das *Ausmaß möglicher Schäden* hängt ab von der konkreten Anwendung des Technik-Systems (d.h. der ihm übertragenen gesellschaftlichen Funktionen) und der Möglichkeit, Schäden abzupuffern, zu kompensieren und zu beheben. Die *Wahrscheinlichkeit der Schadensereignisse* ist bedingt durch die Möglichkeiten von Material-, Konstruktions-, Bedienungs- und Systemfehlern sowie durch die Motive und Aktionsmöglichkeiten zum Mißbrauch und die Sicherungsmöglichkeiten, um diese zu verhindern bzw. in ihrem Erfolg zu begrenzen.

Zur Beurteilung der Verletzlichkeit einer künftigen 'Informationsgesellschaft' sind danach folgende Untersuchungsschritte notwendig:

Als Ausgangspunkt der Untersuchung sind die in der Zukunft wahrscheinlichsten *Anwendungen* der IuK-Technik abzuschätzen. Sie bestimmen den Rahmen für mögliche Aktionen und Sicherungsmaßnahmen. Aus ihnen ist vor allem der *virtuelle*[16] *Schaden* eines Fehlers oder Mißbrauchs der IuK-Technik abzuleiten. Dieser ergibt sich aus den negativen gesellschaftlichen Auswirkungen, wenn eine gesellschaftliche Funktion, die dem Technik-System übertragen wurde, ausfällt oder gestört wird. Das inhärente Schadenspotential eines Technik-Systems ist die Kehrseite der Abhängigkeit einer Gesellschaft von dieser Technik (Kap. 7 und 8).

Die künftigen Anwendungen und ihre gesellschaftlichen Randbedingungen erlauben auch Aussagen zur *virtuellen Wahrscheinlichkeit* dieser Schäden. Sie setzt sich zusammen aus der Wahrscheinlichkeit unbeabsichtigten menschlichen und technischen 'Versagens' (Kap. 9) und der Wahrscheinlichkeit künftiger Motive (Kap. 10) sowie zukünftiger Aktionsmöglichkeiten (Kap. 11) bei heute üblichen Sicherungen. Virtuelles Schadensausmaß und virtuelle Wahrscheinlichkeit des Mißbrauchs beschreiben die Notwendigkeit und den Intensitätsgrad der künftigen Sicherungsmaßnahmen.

Diese werden bestimmt durch die künftigen technischen und organisatorischen *Sicherungsmöglichkeiten* (Kap. 12) und deren *Grenzen* (Kap. 13). Das *tatsächliche Sicherungsniveau* hängt allerdings weniger von den Sicherungsmöglichkeiten als vielmehr von deren Realisierung und ihrer Verläßlichkeit ab. Es ist unter Berücksichtigung kontraproduktiver Effekte, Zielkonflikte, knapper Ressourcen und Widerstände sowie der organisatorischen, menschlichen, sozialen und politischen Voraussetzungen jedes Sicherungssystems abzuschätzen (Kap. 14). Schließlich wirken auch die sozialen Kosten der Sicherheitsproduktion auf das Schadenspotential und das Sicherungsniveau zurück (Kap. 15).

Als *Ergebnis* der Untersuchung sind qualitative Aussagen zur Verletzlichkeit der Informationsgesellschaft möglich, die mit der gegenwärtigen Verletzlichkeit der Gesellschaft verglichen werden (Kap. 16).

Gestaltungsalternativen und Handlungsempfehlungen

Die Veränderungen der Verletzlichkeit unserer Gesellschaft sind allerdings nicht zwangsläufig. Sie sind nur zu erwarten, wenn die derzeit mächtigen Interessen sich entsprechend dem absehbaren Trend durchsetzen und keine kräftige Gegensteuerung erfolgt. Die Trendbeschreibung (Kap. 3 bis 16) soll zeigen, wo die Risiken und Folgen der Verletzlichkeit der Gesellschaft zu hoch sind, wo also Bedürfnisse und Ansatzpunkte für

16 Wir bezeichnen einen Schaden oder eine Wahrscheinlichkeit als virtuell, die als Ergebnis eines analytischen Zwischenschritts zu erwarten wären, wenn keine besonderen Gegenmaßnahmen ergriffen werden.

eine sozialverträgliche Gestaltung der Technik bestehen. Um nun nach Risikominderungen zu suchen, ist ein methodischer Bruch notwendig und nicht mehr nach der Trendentwicklung zu fragen, sondern nach sozio-technischen Alternativen und Gestaltungsmöglichkeiten - die notwendige politische Handlungsbereitschaft immer unterstellt. Die Suche gilt themenspezifischen Bestandteilen eines erstrebenswerten Zukunftsbildes.

Nach der Erörterung des politischen Handlungsbedarfs und der Handlungsmöglichkeiten (Kap. 17) untersuchen wir an den Beispielen 'Optionen der Telekommunikation' und 'Zukunft der Industriearbeit' sozio-technische Alternativen, die sich in der politischen Diskussion befinden, nach dem Kriterium der Verletzlichkeit (Kap. 18). Danach werden für die Verbesserung in der konkreten Anwendung technische und organisatorische Gestaltungsvorschläge zur Reduzierung der informatisierten Gesellschaft diskutiert (Kap. 19). Und schließlich untersuchen wir, wie die sinnvollen Gestaltungsvorschläge politisch umgesetzt werden könnten (Kap. 20).

II. EINE KÜNFTIGE 'INFORMATIONSGESELLSCHAFT'

3. Randbedingungen

Ähnlich wie in den vergangenen Jahren wird auch in Zukunft das Potential der IuK-Technik kräftig weiterentwickelt werden. Welche Bereiche der IuK- Technik in welchem Ausmaß gefördert werden und zur Anwendung gelangen, ist abhängig von den folgenden Randbedingungen.

Weltrüsten

Einen konstanten und starken Druck auf die Entwicklung und Anwendung von IuK-Technik wird der Rüstungswettlauf der Supermächte ausüben. In späteren Jahren wird auch der Konflikt zwischen den nördlichen bevölkerungsarmen Wohlstandsgesellschaften und den südlichen bevölkerungsreichen Armutsgesellschaften Rüstungsrechtfertigungen schaffen. Die IuK-Technik verspricht eine Verbesserung der Schlagkraft durch 'intelligente' Waffen und eine Optimierung der Informationsgewinnung und -verarbeitung durch C_3I-Systeme (command, control, communication and intelligence), sowie auf längere Sicht das fast vollständig automatisierte Gefechtsfeld. Ein Vorsprung in der IuK-Technik kann kriegsentscheidend sein. Ihn innerhalb des militärtechnologischen Wettlaufs nicht anzustreben, führt zu militärischer Unterlegenheit. Das militärische und das IuK-Wettrüsten sind untrennbar miteinander verbunden. Sie haben die gleichen Tatbestände, Ideologien und Interessen zur Grundlage.

Militärtechnologische Programme werden künftig vor allem die Entwicklung

- ultraschneller Schaltkreise für den Einsatz in Raketen, Flughilfe- und ähnlichen Militärsystemen,
- 'künstlicher Intelligenz' zum Beispiel für den Einsatz in autonomen Militärfahrzeugen, in 'natürlichsprachlichen' Partnersystemen für Kampfflugzeuge und in 'intelligenten' Schlachtmanagementsystemen für die Marine sowie
- der Softwaretechnik und verteilter Systeme vorantreiben, die u.a. später in einem "Krieg der Sterne" Anwendung finden sollen.

Die drastische Förderung der IuK-Technik durch das Militär wird sich auch auf die IuK-Nutzung in anderen gesellschaftlichen Bereichen auswirken. Wie in der Vergangenheit werden auch künftig viele militärische IuK-Produkte in veränderter Form auf dem zivilen Markt erscheinen. Insgesamt wird von der Militärforschung und -anwendung eine Beschleunigung der IuK-Entwicklung ausgehen. Zwar widersprechen sich zum Teil militäri-

sche und zivile Anforderungen an die Technik. Die militärische Technik wird jedoch in Zukunft mehr und mehr auf kostspielige Sonderentwicklungen verzichten und die zivile Technik mitberücksichtigen. Zwar wird Geld und personelle Kapazität in der Militärforschung gebunden. Doch werden beide nicht der zivilen Forschung entzogen, sondern konkurrieren unter den gegebenen Verhältnissen mit anderen Rüstungstechnologien. Unternehmen könnten sich die industriell unergiebige Grundlagenforschung des Militärs kaum leisten. Unmittelbare Auswirkungen der Militärforschung dürften künftig bei optischen Speichern, der Glasfasertechnik, Satelliten und der 'Künstlichen Intelligenz' zu erwarten sein. Unabhängig von jeder fördernden und begrenzenden Wirtschaftspolitik wird der Rüstungswettlauf die IuK-Entwicklung forcieren.

Weltmarkt

Die künftige Entwicklung des Weltmarkts wird für den wirtschaftlichen und politischen Handlungsspielraum der Bundesrepublik Deutschland von größter Bedeutung sein. Sie ist gegenwärtig stark vom Weltmarkt abhängig. Sie importiert Waren im Wert von etwa 21% ihres Bruttoinlandprodukts. Insbesondere ist sie auf die Einfuhr von Energieträgern und Rohstoffen angewiesen. Deren Preise werden aufgrund ihrer Verknappung künftig ansteigen. Umgekehrt produziert die Bundesrepublik rund 27% aller Güter für den Export. Dort wird die deutsche Volkswirtschaft in den nächsten Jahrzehnten einer zunehmend starken Konkurrenz ausgesetzt sein. Nach der vorherrschenden Überzeugung muß sie in dem Wettbewerb um die Märkte der Welt bestehen, wenn der Wohlstand in der Bundesrepublik erhalten und soziale Konflikte vermieden werden sollen. Sie wird auf dem Weltmarkt folgende Bedingungen vorfinden:

Künftig werden große Teile der Massenproduktion in die Schwellenländer, die lohnintensive Produktion in die Billiglohnländer und die Rohstoffveredelung in die Rohstoffländer verlagert werden. Die Konkurrenz auf diesen Märkten wird für die Bundesrepublik härter.'Intelligente Produkte' und Systemtechnik werden für sie daher immer wichtiger. In diesem Bereich wird der Weltmarkt überproportional wachsen. Insbesondere ist für Bauelemente, Computer sowie Computersoftware und -services eine sehr große Nachfrage mit jährlichen Wachstumsraten von über 10% zu erwarten. Etwas geringere Wachstumsraten werden für den Markt für Telekommunikationsausstattung prognostiziert.

Die beiden mächtigsten Konkurrenten, die USA und Japan, werden ihren relativen Vorsprung im Bereich der Bauelemente und der Datenverarbeitung ausbauen oder zumindest zu halten versuchen. Japan wird außerdem auf seinen Vorsprung im Roboterbau bedacht sein. Hierzu sind beide schon deshalb genötigt, um ihre Energieimporte auszugleichen. Alle von Informationstechnik bestimmten Industriezweige sind in hohem Maß auf Überseeimporte von Mikroelektronik-Bauelementen und Datenverarbeitungsanlagen angewiesen. Die Möglichkeit, aufgrund amerikanischer Sicherheitsinteressen oder japanischer Industriepolitik von diesen abgeschnitten zu werden, wird als nicht zu verantwor-

tende Gefahr eingeschätzt. Auf reinen Hardware-Märkten (z.B. Personalcomputer, Drucker, Video, TV) ist die Konkurrenz der Billiglohnländer sehr groß und wird weiter ansteigen.

Das ökonomische 'Wettrüsten' ergreift zwar alle Nationalökonomien gleichermaßen. Auch ist der Markt der IuK-Techniken sehr differenziert. Keine Volkswirtschaft führt auf allen Teilmärkten. Eine eindeutige ökonomische Vormachtstellung einzelner Konkurrenten ist daher wenig wahrscheinlich. Doch kann es sich keine Nation leisten, sich abzukoppeln. Insbesondere ist die Bundesrepublik gezwungen, die Vorsprünge, die sie auf dem Weltmarkt hat, wie etwa in der Telekommunikation, zu halten. In rückständigen Bereichen muß sie versuchen aufzuholen, um nicht in ökonomische Abhängigkeiten zu geraten. In der Mikroelektronik wird daher mit starker staatlicher Unterstützung versucht, ein inländisches Produktionsvolumen zu erreichen, das dem Eigenbedarf der Bundesrepublik entspricht, der im Jahr 2000 etwa auf das zehnfache des heutigen gestiegen sein wird. Wer auf den internationalen Märkten nicht selbst durch im Inland produzierende Unternehmen mithalten kann, wird von ausländischen Produkten zunehmend bedrängt.

Europäischer Binnenmarkt

Seit dem Ausbau des europäischen Binnenmarkts mit etwa 320 Millionen Einwohnern nach 1992 verfügen europäische Unternehmen über einen ausreichenden 'Heimatmarkt'. Sie haben den freien Verkehr von Personen, Waren, Dienstleistungen und Kapital forciert, weil die alten Binnenmärkte zur Amortisierung der hohen, ständig steigenden Ausgaben für Forschung und Entwicklung zu klein waren. Die Harmonisierung der Steuern und Marktbedingungen und der Abbau von Handelshemmnissen hat zwar in einzelnen (eher schwachen) Wirtschaftszweigen erhebliche Strukturanpassungen notwendig gemacht. Dafür verbesserte sich aber die Wettbewerbsposition Europas vor allem im IuK-Bereich gegenüber den anderen großen Wirtschaftszentren USA und Japan nachhaltig.

Um ihre internationale Wettbewerbsfähigkeit zu verbessern, suchen die großen Unternehmen europaweite Zusammenschlüsse. Die Fusionskontrolle wird nicht mehr an der möglichen Beherrschung eines nationalen Marktes, sondern am europäischen Markt und der Konkurrenzfähigkeit am Weltmarkt orientiert. Sie werden durch nationale und europäische Förderprogramme für Forschung und Entwicklung unterstützt.

Die wirtschaftliche Integration Europas hat zwar im Durchschnitt der Wirtschaft der Bundesrepublik, die über die Hälfte ihrer Exporte in den europäischen Binnenmarkt liefert, Vorteile gebracht. In besonderem Maß profitierten Unternehmen aus dem Bereich der IuK-Technik. Eine europaweite Normung und Standardisierung der IuK-Technik und verbindliche Vorgaben zur Digitalisierung und Liberalisierung der Telekommunikation schaffen bis zum Jahr 2000 die Voraussetzungen für einen einheitlichen und offenen Markt für IuK-Produkte und -Dienstleistungen in ganz Europa. Er bietet eine ausreichend große Produktionsbasis und dient als Testmarkt für weltmarktfähige Produkte. Als Ge-

genleistung für diese Vorteile mußten aber viele staatliche Entscheidungskompetenzen auf die Gemeinschaft übertragen werden. Und Zugeständnisse waren erforderlich zur Harmonisierung von Umweltnormen, Sicherheitsstandards und sozialen Schutznormen.

Bevölkerungsentwicklung

Zu den seltsamsten Paradoxien vieler moderner Gesellschaften gehört, daß sie in dem Maß in Kinderarmut verfallen, in dem sie die medizinischen, sozialen und rechtlichen Voraussetzungen für Kinderreichtum schaffen. Stärker noch als in anderen vergleichbaren Industrienationen ist in der Bundesrepublik mit einem Bevölkerungsrückgang zu rechnen. Die deutsche Bevölkerung wird von 57 Mio. (1983) auf etwa 52 Mio. im Jahr 2000, 48 Mio. 2010 und 38 Mio. im Jahr 2030 zurückgehen. Demgegenüber dürfte der Anteil der ausländischen Mitbürger von derzeit 4,5 Mio. auf etwa 7 Mio. im Jahr 2000 ansteigen, danach jedoch wegen der sozialen Integrationsprobleme nicht mehr bedeutend anwachsen.

Die Gewichtsverlagerung in der Bevölkerungsstruktur von den Jungen zu den Alten wird zwar den Arbeitsmarkt entlasten, zugleich jedoch eine Reihe besonderer Probleme mit sich bringen. So wird im Jahr 2030 der Anteil der unter 18jährigen von derzeit 22% auf 15% gesunken und der der über 65jährigen von derzeit 15% auf 24% gestiegen sein. Dieser ungleiche Altersaufbau führt zu einer Abfolge demographischer Wellen oder 'Problemberge': vom 'Schülerberg' über den 'Studentenberg' bis zum späteren 'Rentnerberg'. Bei einer Beibehaltung des heutigen Rentenrechts müßten dann die Rentenbeiträge beinahe verdoppelt, bei einer Beibehaltung des heutigen Beitragssatzes das Bruttorentenniveau halbiert werden. Ähnliche Probleme werden im Gesundheitswesen entstehen. Immer mehr alte Menschen werden eine wachsende medizinische Versorgung beanspruchen, gleichzeitig werden aber die Transferleistungen in diesen Bereich immer schwerer zu erbringen sein. Dies wird beide Bereiche einem Druck zur Rationalisierung und Privatisierung aussetzen. Die Alten werden ihren hohen Stimmenanteil nutzen, um ihre Interessen durchzusetzen. Sie werden zur Sicherung ihrer Versorgung Druck ausüben, die wirtschaftliche Produktivität mit Hilfe der IuK-Technik zu steigern.

Volkswirtschaft

Der Binnenmarkt der Bundesrepublik ist relativ klein und wird in Zukunft noch weiter an Bedeutung einbüßen. Abnehmende Bevölkerungszahlen und tendenziell sinkende Einkommen als Folge steigender Sozialabgaben machen eine starke Nachfrage und stabile Kaufkraft nicht sehr wahrscheinlich. Trotz der Wachstumsimpulse durch den europäischen Binnenmarkt ist die Wirtschaftsentwicklung von hoher struktureller Arbeitslosigkeit und nur geringen Wachstumsraten des Sozialprodukts gekennzeichnet. Wirtschaftlicher

Aufschwung und eine Verringerung der Arbeitslosigkeit werden nur durch höhere Exportanstrengungen und dies insbesondere in den expandierenden Märkten der IuK-Technik möglich sein. Zwar ist diese hinsichtlich der Wertschöpfung kein besonders relevanter Faktor der Volkswirtschaft. Als 'Schlüsselindustrie' wird ihr aber eine besondere strategische Bedeutung zugemessen. Denn der internationale Wettbewerb übt einen permanenten Rationalisierungsdruck und damit einen Zwang zur Verwendung von IuK-Techniken auf nahezu alle Bereiche der Volkswirtschaft aus.

Die internationale Konkurrenz wird eine Fortsetzung des wirtschaftlichen Strukturwandels erfordern. Die Wirtschaftsbedingungen der Grundstoffindustrie und der handwerklichen Industrie werden sich verschlechtern und sie zu Verlagerungen ins Ausland zwingen. In allen Wirtschaftsbereichen wird eine Bereitschaft zu ständigen Innovationen erforderlich sein. Von den einzelnen Unternehmen wird ein hohes Maß an Anpassungsfähigkeit gefordert. Die Zeit für die notwendigen Anpassungen wird relativ kurz sein. Der Spielraum für Kompensationen ist gering, wird aber voll ausgenutzt, um den sozialen Frieden möglichst zu erhalten.

Auch auf nationaler Ebene wird sich der Trend zur Unternehmenskonzentration weiter fortsetzen, schon um die großen Kapitalsummen aufzubringen, die notwendig sind, um die Innovationsfähigkeit der Unternehmen zu gewährleisten. Klein- und Mittelbetriebe werden es schwerer haben, Marktnischen zu finden, da die Konzerne ihren Tätigkeitsbereich ausweiten, um ihren Umsatz und ihre Kapitalkraft zu steigern. Großunternehmen übernehmen die Vermarktung selbst, Handelskonzerne produzieren selbst viele Güter, Banken und Versicherungen weiten ihr Dienstleistungsangebot aus. Allerdings dürfte es im Bereich der spezialisierten Dienstleistungen, insbesondere im IuK-Bereich, auch weiterhin einen lukrativen Markt für kleinere Unternehmen geben.

Allgemein wird sich der Arbeitsmarkt entsprechend diesen Vorgaben weiterentwickeln. Der Bevölkerungsrückgang wird zwar zu einer gewissen Entspannung führen, der Rationalisierungsdruck durch die Weltmarktkonkurrenz und die ansteigende Zahl arbeitsuchender Frauen werden jedoch weiterhin eine stagnierend hohe Arbeitslosenquote verursachen. Danach könnte mit einer deutlichen Abnahme der Arbeitslosigkeit erst gegen 2010 gerechnet werden. Recht günstige Arbeitsmarktbedingungen werden bis dahin für eine intellektuelle Oberschicht, für eine breitere Schicht von wissenschaftlich-technisch versierten Fachleuten und für die Mehrzahl der Dienstleistungsberufe zu erwarten sein.

Erwerbslosigkeit, Segmentierung des Arbeitsmarktes und Flexibilisierung der Lohnarbeit schwächen die Durchsetzungskraft der Gewerkschaften. Obwohl eine leichte Reduzierung der regelmäßigen Wochenarbeitszeit errungen werden kann, ist es nicht möglich, eine gleichmäßige Verteilung der gesellschaftlichen Arbeit durchzusetzen. Neben den Stammbelegschaften auf gesicherten Arbeitsplätzen wird es viele Erwerbstätige mit zeitlich befristeten oder auf eine Teilzeit beschränkten Arbeitsverträgen, gelegentlich tätige Selbständige sowie ein großes Heer Arbeitsloser geben. Das gesicherte Auskommen

einer 'Zweidrittelmehrheit' überdeckt die relative Armut des Rests. Ein deutliches Anwachsen der Schattenwirtschaft geht mit dem Abbau sozialer Auffangmechanismen einher.

Politische Steuerung

Der bisher eingeschlagene Weg der politischen und wirtschaftlichen Förderung der IuK-Industrie wird künftig fortgesetzt. Technische Innovationen werden als wesentliche Voraussetzung für die Konkurrenzfähigkeit auf dem Weltmarkt und als entscheidender Motor für das Wirtschaftswachstum angesehen. In der Hoffnung, neue Weltmarktanteile zu gewinnen, werden hohe gesellschaftliche Ressourcen in die Entwicklung der IuK-Techniken als 'Schlüsselindustrie' investiert. Es werden große Anstrengungen unternommen, um die Bundesrepublik zum 'Modell- und Testmarkt' für IuK-Techniken zu machen. Hierfür stellt der Staat angebotsorientierte Vorleistungen bereit (z.B. Forschung, Technologietransfer und Infrastruktur).

Vorherrschend ist die Überzeugung, daß einzelne nationale Unternehmen ohne staatliche Unterstützung auf dem Weltmarkt nicht bestehen können. Daher fördert der Staat insbesondere im IuK-Bereich Zusammenschlüsse von Unternehmen, um so über bisherige Branchengrenzen hinweg Kapital und Know How zu konzentrieren. Technische Innovationen werden außerdem gefördert, weil die Hoffnung besteht, über eine wachsende Wirtschaft gesellschaftliche Probleme wie zum Beispiel das der Massenarbeitslosigkeit lösen und Ressourcen-Überschüsse im Verteilungskampf zur Friedensstiftung verwenden zu können.

Eckpunkte dieser Politik sind eine massive Förderung der IuK-Industrie, vor allem durch Übernahme von Forschungs- und Entwicklungsaufgaben, Verbesserungen der Aus- und Weiterbildung, gezielte Beschaffungsprogramme der öffentlichen Hand als Starthilfe für neue Produkte, ein zügiger Ausbau der Telekommunikationsnetze, Zulassung privater Rundfunkveranstalter, Rückbau sozialstaatlicher Regelungen, ohne dabei gravierende Konflikte zu riskieren, und die gesetzliche Beschränkung gewerkschaftlicher Gegenmachtpotentiale, soweit sie den Ausbau der informationstechnischen Infrastruktur verzögern und die Anwendung neuer Technologien hinausschieben könnten.

Die Bundesregierung betreibt für die Telekommunikation eine angebotsorientierte Infrastruktur- und Ordnungspolitik. Sie will 'Hebammendienste' für die Durchsetzung neuer IuK-Angebote leisten. Um die Konkurrenz zwischen den IuK-Herstellern im Endgeräte-Markt zu fördern und eine Durchsetzung der Industriestandards des Marktführers zu verhindern, treibt sie eine aktive europäische Standardisierungspolitik. Die Deutsche Bundespost wird in drei weitgehend selbständig wirtschaftende Unternehmen aufgeteilt, in den 'Postdienst', die 'Postbank' und TELEKOM. Wie in ganz Europa behält das staatliche Unternehmen das Monopol für die Netze. Telekommunikationsdienste und der Endgerätemarkt werden liberalisiert, um die Konkurrenz auf diesen Gebieten und damit auch

die Verbraucherakzeptanz zu erhöhen. Ende der 80er Jahre war zwar noch der Fernsprechdienst im Monopol von TELEKOM. Nach seiner Integration in das ISDN werden auch für diesen Dienst um das Jahr 2000 private Anbieter zugelassen. Der 'gelbe' Postdienst erleidet durch Reduzierung der Quersubventionen, die daraus folgenden Gebührenerhöhungen und die dadurch bedingten Einschränkungen des materiellen Schriftverkehrs zugunsten der Telekommunikation große Umsatzeinbußen.

Umwelt

Das Ansteigen der Weltbevölkerung und die weitere Industrialisierung werden die Naturkreisläufe in noch stärkerem Maß als bisher stören und in immer kürzeren Abständen zu Umweltkatastrophen führen.

Zum einen fehlt es noch immer an wirksamen Lösungen für die kontinuierlichen globalen Probleme - Zerstörung der Ozonschicht und CO_2-Aufheizung der Atmosphäre. Die Folgen - Verschiebung der Klimazonen, Ansteigen des Meerwasserspiegels und Zunahme von Krebserkrankungen - werden gegen 2020 schon zu spüren sein. Trotz einschneidender Maßnahmen zur Luftreinhaltung verliert die Bundesrepublik einen großen Teil ihrer Wälder. Die schleichende Vergiftung der Böden und des Grundwassers lassen die Nahrungsmittelproduktion zu einem ernsten Problem werden.

Zum anderen werden Unfälle in Chemieanlagen, Atomkraftwerken oder gentechnischen Produktionsstätten immer wieder zu Umweltzerstörungen führen und die Lebensbedingungen auch in der Bundesrepublik beeinträchtigen. Dennoch bleiben die Katastrophen weit unterhalb des Schadenspotentials, das durch solche Anlagen gegeben ist. Der Weg der Industrialisierung wird daher zwar immer schärfer kritisiert, aber nicht mehrheitlich in Frage gestellt. Die mit ihm verbundenen ökologischen Risiken werden mehrheitlich weiter verdrängt.

Wertwandel

Der Bedeutungsverlust traditioneller Wertorientierungen, verursacht durch die gesellschaftlichen Strukturveränderungen, wird sich in Zukunft fortsetzen. Der abnehmende Anteil der Berufstätigen an der Gesamtbevölkerung, die Verkürzung der Lebens- und Wochenarbeitszeit, die Wechsel- und Anpassungsleistungen innerhalb eines Berufslebens werden die prägende Kraft der Erwerbsarbeit für kollektive und individuelle soziale Identitäten vermindern. Sozialstaatliche Leistungen, Risikoübernahmen und steigende Einkommen erlauben für viele, Lebenserfahrungen und -bestätigungen vermehrt im Freizeit- und Konsumbereich zu suchen. Die fortschreitende soziale Differenzierung der Gesellschaft und der Rückgang gemeinsamer sozialer Erfahrungen wird ein Nebeneinander vielfältiger Wertmuster verursachen, instabile, an jeweiligen Zwecken orientierte Haltun-

gen vermehren und eine hohe Wertschätzung von Individualität und Unabhängigkeit bewirken. Dementsprechend wird die Integrationskraft von großen ideologischen Organisationen wie Kirchen, Parteien oder Gewerkschaften ebenso sinken wie die des Staates. Für ihr Werben um Bevölkerungsgruppen müssen sie ebenfalls ihre Organisationsphilosophie an vielen gesellschaftlichen Werten orientieren.

Alle diese Teilentwicklungen machen eine Prognose der Gesamtentwicklung sehr schwierig. Relativ sicher dürften nur folgende drei Trends angenommen werden: Die Eindeutigkeit und Übersichtlichkeit der Zuordnungen von Werthaltungen und sozialer Situation wird verloren gehen. Die fortschreitende gesellschaftliche Arbeitsteilung erhöht die Abhängigkeit des einzelnen vom Funktionieren der wichtigen gesellschaftlichen Subsysteme und den Leistungen der staatlichen Daseinsvorsorge. Das Bewußtsein dieser Abhängigkeit und die von ihm in immer schnellerer Abfolge geforderten Anpassungsleistungen lassen gesamtgesellschaftlich das Bedürfnis nach Stabilität und individuell das Bedürfnis nach Sicherheit steigen. Der Einfluß der Alten auf die gesellschaftlichen Orientierungen wird ebenso zunehmen wie ihr Einfluß auf das öffentliche Leben und die Kultur. Abgesehen von ihren spezifischen Alteninteressen werden sie aber - jeweils mit einer entsprechenden Zeitverzögerung - ähnlich differenzierte Werthaltungen vertreten wie die Gesamtbevölkerung.

Jenseits dieser Trends kann nur eine breite Palette verschiedener Wertmuster ausgemacht werden, die sich vielleicht - mit dem gebotenen Mut zur Vereinfachung - sehr grob in fünf Gruppen zusammenfassen lassen.

a) *Leistungsorientiert* werden vor allem die im harten Kern der Produktions-, Dienstleistungs- und Verwaltungssysteme Tätigen sein. Sie orientieren sich an Karriere und materiellen Werten. Die Identifikation mit ihrer Arbeit ist oft nicht inhaltlich, sondern wegen der erzwungenen Wechsel und Anpassungen formal. Sie stehen technischen Innovationen positiv gegenüber. Ihr Anteil an der Bevölkerung geht jedoch zurück.

b) Dagegen wird der prozentuale Anteil der *Konsum- oder Freizeitorientierten* eher zunehmen. Vor allem die Inhaber von relativ sicheren Arbeitsplätzen ohne besondere Aufstiegschancen werden ihren Lebenssinn eher im Genuß und in Freiheitssurrogaten sehen als in der Karriere oder dem Erwerb materieller Werte. Sie stehen technischen Innovationen indifferent gegenüber.

c) *Alternative Wertmuster* werden gegenüber heute zunehmen und sich vor allem bei Beschäftigten in den Bereichen Ausbildung, Wissenschaft und Kultur, industrieferner Dienstleistungen sowie der anwachsenden 'Alternativwirtschaft' finden. Außerdem sind zu dieser Gruppe viele gesellschaftliche Randgruppen zu rechnen. So heterogen wie die Gruppe selbst sind auch die Orientierungen an gesellschaftlichen Utopien, der Natur, Spiritualität oder Esoterik. Allen gemeinsam ist jedoch die skeptische bis ablehnende Haltung gegenüber (groß)technischen Innovationen.

d) *Frustriert*, unzufrieden und ohne Hoffnung werden die sein, die vom gesellschaftlichen Reichtum ausgegrenzt werden. Die Arbeitslosen, die Empfänger sozialer Leistun-

gen, die Inhaber unsicherer, schlechtbezahlter Jobs können sich weder Konsum leisten noch haben sie die Chance, durch Leistung aufzusteigen. Ihnen fehlt jede positive Orientierung. Technischen Innovationen, die in der Vergangenheit häufig ihre Situation mitverursacht haben, stehen sie entweder gleichgültig oder skeptisch gegenüber.

e) *Radikale, militante* Konfliktlösungen der ökonomischen und ökologischen Krise werden von einer begrenzten, aber aktiven Minderheit verfolgt. Die erzwungenen gesellschaftlichen Veränderungen werden am rechten Rand des politischen Spektrums neofaschistischen Gruppen und am linken Rand einer autonomen Systemopposition Zulauf verschaffen. Die Grenzen 'grüner' Reformpolitik werden deutlich geworden sein. Sie wird einen Teil ihrer bisherigen Integrationskraft verlieren. Technische Innovationen werden von diesen radikalen Gruppen militant bekämpft.

4. Die Entwicklung der IuK-Technik

Unter Annahme dieser Randbedingungen dürften in den kommenden Jahren und Jahrzehnten die in diesem Kapitel dargestellten IuK-Techniken entwickelt und zur Nutzung bereitgestellt werden. Die wahrscheinlichen Anwendungsformen dieser Techniken sind Gegenstand des fünften Kapitels.

Hardware

Die IuK-Forschung und -Entwicklung wird in allen technischen Bereichen weitere Verbesserungen erzielen. Rechner und Speicher werden noch erheblich leistungsfähiger, kleiner und billiger werden. Trotz zunehmender Leistung benötigen sie immer weniger Rohstoffe und Energie. Die Hardware-Produktion erfolgt zunehmend rechnergestützt und ermöglicht komplexere und höher integrierte Schaltelemente. Die heutigen Verfahren der Chipherstellung werden hinsichtlich der Integrationsdichte zwar an physikalische Grenzen stoßen. Mit Hilfe neuer Rechnerkonzepte und neuer Materialien werden dennoch weitere Leistungssteigerungen möglich. Neben den Standard-Bauelementen wird Systemwissen zunehmend in anwendungsspezifischen Schaltungen integriert.

Die Kapazität von Speicherbausteinen wird durch höhere Integrationsdichte und neue Chipmaterialien von gegenwärtig einem Megabit bis auf etwa 64 Megabit (8 Mio. Zeichen pro Speicherbaustein, der nur wenige Millimeter groß ist) im Jahr 2000 angehoben. In ähnlichem Umfang wird die Zugriffsgeschwindigkeit steigen. Bis dahin sind als Sekundärspeicher auch optische Platten ähnlich den heutigen CD-Platten verfügbar, die - anders als zur Zeit - mehrfach beschrieben werden und Milliarden von Zeichen speichern können.

In der Verarbeitungstechnik wird die Leistungsfähigkeit der Prozessoren bis zum Jahr 2000 um etwa zwei Größenordnungen steigen. Durch höher integrierte und schnellere Chips werden PCs die Rechenleistung heutiger Großrechner anbieten. Prozessoren aus neuen Halbleitermaterialien wie z.B. Gallium-Arsenid werden Großssysteme um etwa das Hundertfache schneller machen. Mit Hilfe von supraleitenden Materialien wird für bestimmte Rechner der Widerstand von Funktionselementen auf Chips fast 'auf Null' reduziert. Die dadurch verringerte Wärmeentwicklung erlaubt es, Bauelemente dichter zu packen. Bis zum Jahr 2020 könnten elektronische durch optische, vielleicht sogar durch bio-chemische Bauelemente ersetzt und dadurch in ihrer Leistung weiter gesteigert werden.

Die Speicherkapazität und die Rechnergeschwindigkeit werden darüber hinaus durch neue Systemarchitekturen verbessert. Beispielsweise ist der heute am Anfang stehende parallele Einsatz vieler Prozessoren bis zum Jahr 2000 produktionsreif. Dann wird es möglich sein, verschiedenartige Teilaufgaben von verschiedenen Prozessoren gleichzei-

tig bearbeiten zu lassen und die Ergebnisse zusammenzuführen. Durch die technischen Verfahren der Höchstintegration werden auch Ein-Chip-Prozessoren mit der Leistungsfähigkeit heutiger PCs verfügbar sein. Sie werden in tragbaren PCs oder zur Steuerung komplexer Geräte eingesetzt.

Software

Parallel zum Preisverfall der Hardware wird der Kostenanteil der Software an der IuK-Technik ansteigen. Dies und die wachsende Komplexität der Aufgabenstellungen üben einen starken Druck aus, durch verbessertes Software-Engineering Software schneller, billiger und besser herzustellen.

Die Softwareentwicklung wird von Programmiersprachen zu immer höheren, der natürlichen Sprache näheren Auftragssprachen übergehen, die es erlauben, dem Rechner unmittelbar mitzuteilen, welche Aufgabe gelöst werden soll, ohne daß im Detail spezifiziert werden muß, wie sie gelöst werden soll. Die Übertragbarkeit eines Programms von einer Anlage auf eine andere wird durch spezielle Programmiersysteme ermöglicht. Daneben kann ein solcher Austausch durch 'virtuelle Maschinen' unterstützt werden. Mit Hilfe eines entsprechenden Programms führt ein Rechner B Befehle so aus, wie dies auf der Hardware der Maschine A der Fall sein würde. Dadurch kann eine Aufgabe unabhängig vom konkreten Hardwaresystem bearbeitet und die Abhängigkeit von einem Hersteller erheblich verringert werden.

Neue oder verbesserte Werkzeuge des Computer Aided Software Engineering (CASE) wie Beschreibungsmittel, Prüfhilfen oder Modulbibliotheken werden den Software-Entwicklungsprozeß verbessern. Eine vollautomatische Softwareerzeugung wird allerdings nicht möglich sein, da zumindest die Funktionsanforderungen von Menschen in einer Spezifikation festgelegt werden müssen.

Netze/Infrastruktur

In der Übermittlungstechnik wird durch verbesserte elektrische und optische Leitungen die Übertragungskapazität erheblich gesteigert. Die Übermittlungssysteme arbeiten digital. Dadurch wird es möglich, verschiedene Informationstypen - Sprache, Text, Bild, Daten - in der gleichen Form darzustellen und zu übermitteln. Diese Integration erlaubt, alle Informationstypen zu kombinieren. Die Normung von Übertragungsprotokollen ermöglicht technisch offene, von jedem gegen Entgelt benutzbare Netze.

TELEKOM wird bis zum Jahr *2000* das derzeitige Fernmeldenetz Zug um Zug zu einem Integrated Services Digital Network (ISDN) ausbauen und flächendeckend anbieten. Etwa die Hälfte der 6000 Vermittlungsstellen und etwa ein Viertel der 27 Mio. Hauptanschlüsse werden bereits digitalisiert sein. Auf dem Markt werden Komforttelefone ange-

boten, mit denen neue Dienstemerkmale wie Anklopfen, Registrieren ankommender Gespräche, Rufumleitung, automatischer Rückruf, Einzelgebührennachweis und Identifizieren genutzt werden können. Außerdem werden Multifunktionsterminals genutzt, eine Kombination aus Telefon und Bildschirmgerät, durch die Festbild-, Sprach- und Datenübertragung kombiniert werden können. Neben den schon heute bestehenden Telekommunikationsdiensten werden beispielsweise ein verbessertes Btx, langsames Bewegtbild, eine Kombination von Teletex und Telefax (Textfax) und Fernmeß- und -wirkdienste (Temex) von TELEKOM und anderen Unternehmen angeboten. Aufbauend auf diesen Standarddiensten herrscht eine starke Konkurrenz im Angebot von Verschlüsselungs-, Sprachspeicher-, Bildspeicher-, Mailbox-, Datenbank- und ähnlichen Diensten.

Parallel zur ISDN-Integration wird TELEKOM die Glasfasernetze weiter ausbauen und auf dieser Basis mit der Zusammenfassung aller Dienste in einem einheitlichen Breitband-Universalnetz (IBFN) beginnen. Dessen höhere Leistungsfähigkeit ermöglicht, alle Formen der Individual- und Massenkommunikation (Radio/TV) in einem einzigen Netz zusammenzufassen. Das IBFN wird zunächst durch Erweiterung der ISDN-Technik um Breitbandvermittlungseinrichtungen und später durch Integration auf der Vermittlungsebene realisiert. Bei einem flächendeckenden Angebot werden bis zu einer Million Nutzer an die Breitbandindividualkommunikation angeschlossen sein. Parallel hierzu werden auch die Kupferkoaxialkabelnetze weiter ausgebaut, um bereits vor dem Jahr 2000 Kabelfernsehen bei Nachfrage schnell zur Verfügung stellen zu können.

Bis zum Jahr *2020* wird die Netzintegration weiter fortschreiten. Zu erwarten ist, daß im Schmalband-ISDN alle Vermittlungsstellen und 80% der Anschlüsse digitalisiert sind. Durch die hohe Anschlußdichte werden die ISDN-Dienste attraktiver und vermehrt genutzt. Etwa ein Drittel der Anschlüsse wird breitbandig sein. Dadurch werden z.B. Bildfernsprechen, Videokonferenzen, Bildabruf- und schnelle Datenübertragung möglich sein. Glasfaserverkabelung wird flächendeckend angeboten, es werden jedoch noch lange nicht alle Haushalte angeschlossen sein.

Bis *2000* wird ein einheitliches europaweites digitales Netz für mobile Telekommunikation mit einer Kapazität für Millionen von Teilnehmern entstehen. Tragbare Systeme mit der Leistungsfähigkeit heutiger Großrechner werden über dieses Netz von jedem Platz aus Programme abrufen oder übermitteln können. Diese Mobilität ermöglicht neue ortsunabhängige Anwendungsformen in Arbeit und Freizeit.

Fortschritte in der Laser-, Satelliten-, Funk- und Antennentechnik werden bis zum Jahr *2000* die gleichzeitig zu nutzenden Fernsprech- und Fernsehkanäle pro Satellit (heute 12000 bzw. 4) vervielfachen und deren Leistungsfähigkeit erhöhen. Die neuen Medium-Power-Satelliten werden sowohl für die Programmverbreitung zu den Kopfstationen der Kabelnetze als auch für die Individualkommunikation genutzt. Antennen für den Direktempfang müssen nicht mehr die Form von Schüsseln haben, sondern können als flexibler Streifen zum Beispiel auch an Fahrzeugen oder tragbaren Geräten angebracht werden. Mittelfristig wird die Satellitenkommunikation in eine Angebotslücke stoßen, da

sie auch bei geringer Teilnehmerdichte eine schnelle Einführung von Breitbanddiensten ermöglicht. Sie wird daher für die Übertragung von Bewegtbildern, die schnelle Datenübertragung und die Massenkommunikation, insbesondere für den mobilen Empfang von TV-Sendungen eine große Bedeutung erlangen. Für die erdgebundene Individualkommunikation in der Bundesrepublik und Europa wird sie allerdings keine ernsthafte Konkurrenz sein: Wegen der ausgebauten Telekommunikationssysteme besteht hierfür kein Bedürfnis und die relativ wenigen Kanäle auf den Satelliten könnte diese auch nicht ersetzen.

Die Erhöhung der Transportkapazitäten für Raumflüge ermöglichen es in der Zeit bis *2020*, dort große multifunktionale Relaisstationen zu errichten. Wegen der fortschreitenden Glasfaserverkabelung wird ihre Bedeutung für die Telekommunikation allerdings zurückgehen. Sie werden vor allem für die transkontinentale Kommunikation, für die Fernerkundung und für Leitsysteme von Schiffen, Flugzeugen und Fahrzeugen eingesetzt.

Die Leistungsverbesserungen der Hardware und standardisierte Systemschnittstellen bieten die Möglichkeit, Systeme zu dezentralisieren und zu vernetzen. Informationsverarbeitung und übermittlung können zunehmend verbunden werden. Dies ermöglicht große Datenbank-Systeme, die über offene Netze schnellen Zugriff auf Informationen, deren beliebige Verknüpfung und Auswertung erlauben. Betreiber großer Rechenzentren werden die Möglichkeit nutzen, Aufträge zwischen ihren Rechnern auszutauschen, um Kapazitätslücken und -überschüsse auszugleichen oder günstige Rechenzeit einzukaufen. Eine solche Lastverteilung wird mittels Satellitenverbindungen auch international verwirklicht.

Bis zum Jahr *2000* sind Probleme verteilter Systeme (etwa die Synchronisation von Prozessen) bis zur Anwendungsreife gelöst. Kommerzielle Anwender betreiben private Local Area Networks (LAN), auf denen verteilte Anwendungen mit verteilter Verarbeitungsleistung gerechnet werden. Bei Bedarf werden zusätzliche Kapazitäten eines großen Hintergrundrechners in Anspruch genommen. Kleinere Unternehmen nutzen solche größeren Rechnerleistungen bei kommerziellen Anbietern. Neben den allgemein zugänglichen Diensten gibt es auch geschlossene Benutzerkreise für spezielle Anwendungen.

Mensch-Maschine-Schnittstelle

Verbesserte Systemzugänge werden in Zukunft die Bedienungsfreundlichkeit und damit auch die Akzeptanz der IuK-Techniken spürbar erhöhen. Bereits heute werden Tastaturen angeboten, die durch Software auf Flüssigkeits-Kristallanzeigen erzeugt und verändert werden können. Bis zum Jahr *2000* wird es möglich sein, IuK-Systeme durch eine der natürlichen Sprache ähnliche Tastatureingabe anzusprechen. Verschiedene Informationssysteme werden mit einer universellen Anfragesprache genutzt werden können. Lediglich ausgefallene Wünsche müssen in einer Spezialsprache formuliert werden. Die

Benutzerschnittstellen werden flexibel gestaltet. Fachleute passen sie sich ihren Wünschen selbst an. Weniger versierte Personen nutzen Geräte, die ihr Ausgabeverhalten mit Methoden der 'künstlichen Intelligenz' an die Qualifikationen des Benutzers automatisch anpassen und ihn führen. Als neuer Systemzugang wird die Eingabe gesprochener Sprache erschlossen. Statt der heutigen etwa nur 400 Worte können bis zum Jahr 2000 gesprochene Worte aus Fachtexten sprecherabhängig erkannt werden. Bis zum Jahr *2020* wird der Sprachumfang erweitert und sprecherunabhängig analysiert werden. Nicht alle Mensch-Maschine-Kontakte werden jedoch 'natürlichsprachlich' sein können; zumindest Spezialprobleme werden weiterhin formal beschrieben werden müssen. Auch werden zwischen einem Dialog mit einer 'natürlichsprachlichen' Schnittstelle und einer umgangssprachlichen Kommunikation unter Menschen schon deshalb immer Unterschiede bestehen, weil nur in dieser Mimik, Gestik, Stimmungen und andere den Kontext und die Atmosphäre einer Kommunikation begründende Umstände erfaßt werden können.

Als Ausgabegeräte werden im Jahr *2000* neben qualitativ verbesserten Großbildschirmen auch flache Flüssigkristall-Bildschirme und Plasma-Displays eingesetzt, die hochauflösende Graphik beherrschen. Wo dies sinnvoll erscheint, werden Informationen in Sprache ausgegeben. Hardcopies werden relativ preiswert mit Farblaserdruckern hergestellt.

Die Mikroperipherik-Komponenten, die den Kontakt zwischen Rechner und Umwelt herstellen, werden durch Digitalisierung und neue Materialien leistungsfähiger. Neue Sensoren verbessern die automatische Erfassung von Umgebungsgrößen, neue Aktoren erhöhen die Geschwindigkeit und Präzision von Regelungs- und Steuerungssystemen. Fortschritte in der Aufbau- und Verbindungstechnik erhöhen die Zuverlässigkeit der zu Systemen verbundenen Bauelemente. Dadurch werden die Einsatzmöglichkeiten von Rechnern in der Fließfertigung, in Fertigungszentren und die Manipulationsmöglichkeiten von Robotern verbessert

Prozeßsteuerung

Die Fortschritte in der Mikroperipherik verbessern auch die Möglichkeiten der Prozeßsteuerung. Diese kontrolliert und regelt Abläufe in technischen Anlagen automatisch und erfordert nur prüfende oder regulierende menschliche Tätigkeiten. Die vielen einzubeziehenden Umgebungsgrößen und Randbedingungen ergeben oft sehr komplexe Problemstellungen, die bisher nicht ausreichend zu lösen waren. Da oft mehrere Aufgaben gleichzeitig, aber in Abhängigkeit voneinander abgearbeitet werden müssen, besteht die Notwendigkeit, parallele Prozesse zu synchronisieren. Durch automatische Unterstützung und verbesserte Sprachmittel zum Programmieren werden bis zum Jahr 2000 wichtige Softwareprobleme gelöst sein.

Datenbanken

In diesem traditionellen Bereich der Informationstechnik wird der Funktionsumfang bis zum Jahr *2000* beträchtlich erweitert werden. Neben formatierten Daten können auch unformatierte Texte, Sprache und Bildinformationen gespeichert und abgefragt werden. Zur Abfrage von Fachinformationen wird aber immer noch Fachkenntnis und Strukturwissen erforderlich sein. Bis zum Jahr *2020* wird der Zugang zu Informationen durch 'Information Retrieval Systeme', zum Teil auf Volltextbasis, erheblich erleichtert, die die Auswertung von Texten automatisch unterstützen. Durch Methoden der 'künstlichen Intelligenz' kann das Informationssystem auch einem relativ unkundigen Laien Fachkenntnisse anbieten, indem es sich dessen Informationsniveau anpaßt.

'Künstliche Intelligenz'

Wesentliche Fortschritte werden in der Entwicklung 'künstlicher Intelligenz' (KI) möglich sein. Allerdings werden einem universellen Einsatz von KI-Systemen auch um das Jahr *2000* noch viele Hürden entgegenstehen. Probleme der Wissensakquisition, der Modellierung, der Formalisierung und der Komplexität bzw. der Umfang der zu bearbeitenden Informationen stellen nach wie vor Grenzen der Anwendung dar. Bis zum Jahr 2020 werden weitere Verbesserungen erreicht. Aber auch sie werden nur beschränkte Anwendungen auf begrenzten Gebieten ermöglichen, vermutlich jedoch keine 'Weltwissenssysteme'.

Sprachverstehende Systeme werden im kommenden Jahrzehnt sprecherabhängige Fachtexte weitgehend und sprecherunabhängige eingeschränkt verstehen und einen 'natürlichsprachlichen' Dialog führen können. Über das Erfassen natürlicher Sprache hinaus werden KI-Systeme in abgegrenzten Gebieten ein 'kognitives', jedoch nie ein einfühlendes Verständnis erreichen können. In 20 bis 30 Jahren dürften Computer technische oder wissenschaftliche Texte verstehen und auch übersetzen können. Die Spracherkennung könnte dann selbst bei fließendem Text sprecherunabhängig möglich sein. Dialekte und Umgangssprache werden allerdings nur beschränkt erfaßt werden können.

Bis zum Jahr 2000 werden *'bildverstehende' Systeme* bereits relativ komplexe Gebilde erkennen und bewegte Bilder verarbeiten können. Danach sind sogar bild- und sprachverstehende Systeme zu erwarten, die sowohl visuelle Informationen als auch sprachliche Informationen verarbeiten und eine mit dem Fernsehauge beobachtete Situation bewegter Bilder sprachlich darstellen können. Die automatische Analyse von Bildern wird jedoch nicht ganzheitlich, sondern jeweils nur auf einem Ausschnittsniveau, und die von natürlicher Umgebung nur sehr beschränkt möglich sein.

Expertensysteme werden im nächsten Jahrzehnt in der Lage sein, in vielen begrenzten Wissenschafts- und Technikgebieten das Wissen eines guten Experten zur Verfü-

gung zu stellen. Kombiniert mit Systemen zur Sprachein- und -ausgabe ermöglichen sie Schnittstellen, die sich den Kenntnissen des Benutzers anpassen können. Sie bestehen aus einer 'Wissensbank', in der Fachkräfte die Informationen des Wissensgebiets ansammeln, und aus einem 'Inferenz-System', das die zur Aufgabenlösung relevanten Informationen aus der Datenbank holt und logisch verknüpft. Durch die Entwicklung bereichsspezifischer Expertensystemhüllen (Shells) wird die Produktion von Expertensystemen erheblich erleichtert. Expertensysteme werden um 2000 sogar beginnen, selbständig Wissen zu erwerben und aus Fehlern zu lernen. Zum Teil können sie untereinander kombiniert werden und ihr Wissen austauschen. In zwei oder drei Jahrzehnten werden diese Entwicklungen ausgereift und integraler Bestandteil vieler technischer Produkte sein. Diese könnten je nach eigener Komplexität mit einer gewissen 'Eigenintelligenz' versehen sein, die es ihnen gestattet, sich selbst zu kontrollieren, die Zusammenarbeit mit übergeordneten Systemen zu koordinieren und mit dem Menschen 'natürlichsprachlich' zu kommunizieren.

Deduktionssystemen wird es um das Jahr 2000 möglich sein, auch relativ schwierige mathematische Beweise automatisch zu erbringen und an der Erstellung von Programmen mitzuwirken. Komplexere Programme werden auf ihre Übereinstimmung mit der Spezifikation aber erst nach dem Jahr 2000 verifiziert werden können. Eine vollständige Verifikation hochkomplexer Programmsysteme wird auch danach noch nicht möglich sein. Deduktionssysteme vermögen in jedem Fall nur Widersprüche zwischen dem Programm und den formalisierten Anforderungen an dieses, nicht jedoch Fehler in den weiterhin von Menschen zu erstellenden Anforderungen zu erkennen.

Durch die Kombination der KI-Fortschritte in der Bild- und Wissensverarbeitung mit motorischen Komponenten könnten bereits im nächsten Jahrzehnt die ersten leicht umrüstbaren KI-*Roboter* zum Einsatz kommen und in vollautomatischen Fabrikationsanlagen integriert werden. In der Zeit zwischen 2010 und 2020 könnten dann auch autonome mobile Roboter für eine breitere Anwendung in einfach strukturierter Umgebung 'reif' sein.

Probleme des Einsatzes von Informationstechnik

Interne Probleme der Informatik und Randbedingungen der Einsatzumgebung werden auch künftig die Einsatzmöglichkeiten von IuK-Systemen beschränken. Diese Schranken werden sich zwar mit der Entwicklung der Anwendungssysteme und gesellschaftlichen Anpassungsprozessen verschieben. Dennoch werden IuK-Technikanwendungen nicht unbegrenzt realisiert werden können. Oft werden allerdings die Grenzen und Probleme von den Entwicklern der Technik nicht gesehen. Sie machen sich dann aber als negative Rückkopplungen immer wieder bemerkbar.

Die Informatik arbeitet als Ingenieurwissenschaft mit naturwissenschaftlichen Methoden und unterliegt daher den grundsätzlichen erkenntnistheoretischen Schwierigkeiten der Naturwissenschaften. Zum einen ist immer zu fragen, ob das Analysieren der Wirk-

lichkeit und ihre Synthetisierung in einem Modell der komplexen 'objektiven' Realität gerecht wird. Zum anderen könnte das Verständnis von Naturzusammenhängen als eindeutig kausalen Beziehungen - wie es der sequentiellen Bearbeitung von Aufgaben in einem Rechner zugrundeliegt - nicht in jedem Fall der Realität von Wechselwirkungen entsprechen.

Eine weitere Schwierigkeit hat mathematischen Ursprung: Aus einem von Gödel bewiesenen Satz folgt, daß es Klassen von Problemen gibt, deren Lösung sich einer Berechnung entzieht. Ein Beispiel ist etwa, für beliebige Programmstücke zu zeigen, daß sie die gleichen Ergebnisse liefern (funktional äquivalent sind). Andere Probleme sind zwar theoretisch, aber nicht praktisch lösbar. Eigentlich könnte ein Computer zum Beispiel das Problem eines Kaufmanns lösen, der 30 Städte besuchen muß und dafür die kürzeste Wegstrecke sucht. Aber für diese Rechenaufgabe benötigte der Computer selbst bei einer Millionstel Sekunde pro Prüfvorgang einige Milliarden Jahre. Zwar sind auch für solche Problemstellungen Lösungen errechenbar. Sie setzen aber oft eine Eingrenzung des Problembereichs, das Akzeptieren von Teil- oder Näherungslösungen oder die Anwendung nicht-deterministischer Verfahren voraus. Die Entscheidung über sinnvolle Einschränkungen hängt vom jeweiligen Problem ab und kann deshalb nur selten automatisch getroffen werden.

Praktische Probleme der Informatik ergeben sich auch aus dem Modellcharakter ihrer Systeme. Weil sie durch Abstraktion aus der Wirklichkeit konstruiert werden, ergeben sich zum einen Schwierigkeiten aus der Rollentrennung zwischen Entwickler und Anwender von Programmen. Denn in der Regel fehlt dem Informatiker das Fach- und Erfahrungswissen des Anwenders. Zum anderen hängt die Bedeutung von Einflußgrößen als relevant oder irrelevant erst von der Bewertung des künftigen Benutzers ab. Subjektive Bewertungen wie etwa die 'Eignung' eines Menschen können nur sehr unvollständig quantitativ dargestellt werden. Zum dritten überfordert die Komplexität der Wirklichkeit oft entweder die Analysefähigkeit der Bearbeiter oder das Komplexitätsniveau des Modells. Schließlich können sich aus der Größe von Systementwicklungen Probleme in der Projektorganisation ergeben: Niemand mehr überblickt das gesamte Projekt.

Voraussetzung einer informationstechnischen Aufgabenlösung ist die exakte Analyse und Beschreibung der relevanten Sachverhalte. In der Regel wird hierfür ein quantitatives Modell der Wirklichkeit benötigt. Dazu ist es oft notwendig, qualitative in quantitative Maßstäbe umzuwandeln oder subjektives Wissen, Fühlen und Meinen explizit zu machen und in Klassen einzuteilen. Die zu modellierenden Wirklichkeiten sperren sich aber häufig gegen eine solche Formalisierung. Sie müssen folglich entweder an die Notwendigkeiten des EDV-Systeme angepaßt werden oder entziehen sich einer solchen Bearbeitung. Für viele gesellschaftliche Probleme, die durch subjektives Erleben, durch Erfahrungen, durch Intuitionen, durch Werthaltungen oder durch Freiheitsstreben geprägt sind, wird sich zeigen, daß eine informationstechnische Bearbeitung unangemessen ist.

Entwicklungsmöglichkeiten jenseits von 2020

Wir erleben erst den Anfang umwälzender technischer Entwicklungen. Der heute eingeleitete dynamische Prozeß rasanten technischen Wandels wird noch weit über das Jahr 2020 hinausgetrieben. Um anzudeuten, wohin dieser Weg führen könnte, seien jenseits unseres Zukunftsbildes noch einige 'Farbtupfer' aus der Palette technischer Visionen gesetzt.

Bereits heute gibt es Versuche, Bau- und Funktionsprinzipien des Gehirns in sogenannten neuronalen Netzwerken nachzuahmen. Statt einer Zentraleinheit bei herkömmlichen Computern führen mehrere tausend Prozessoren, als synthetische Gehirnzellen zu einem neuronalen Netz vielfältig verknüpft, die Aufgaben aus. Die Speicherplätze sind gleichmäßig über das Netz verteilt, so daß in unmittelbarer Nähe eines Prozessors auch ein Speicher vorhanden ist. Statt in einer Sequenz von Instruktionen wie in herkömmlichen Computern programmiert zu werden, würde ein solches Netz anhand von Einzelfällen 'trainiert'. In nicht völlig vorhersagbarer Weise würden die gewünschten Funktionen durch Selbstorganisation der Verbindungspunkte während des Lernvorgangs festgelegt. Solche neuronalen Netzwerke könnten für Aufgaben eingesetzt werden, die Kreativität und hohe Flexibilität erfordern. Mit ihrer Hilfe könnten mobile Roboter gesteuert, künstliche Augen und Ohren entwickelt oder endlich die Informationsflut in einer 'Informationsgesellschaft' bewältigt werden.

Ein weiterer qualitativer Techniksprung gelänge, wenn auf der Basis chemischer und biologischer Prozesse Rechner aufgebaut werden könnten. Moleküle würde nahezu verlustfrei durch die Weitergabe von Elektronen schalten, Zellen könnten in ihren Genen gewaltige Informationsmengen abspeichern. Die 'natürliche' Vermehrung in Nährflüssigkeit würde teure Produktionsstraßen und hochempfindliche Maschinen ersetzen. Speicher, Verarbeitungskapazitäten und Daten könnten für Pfennigbeträge reproduziert werden.

Vielleicht gelingt es sogar in ferner Zukunft, die Nervenbahnen von Menschen mit der Übertragungstechnik zu koppeln. Der Mensch liehe dem Computer seine Sinnesorgane, seine Phantasie und Kreativität, der Rechner dem Menschen seine Speicher- und Verarbeitungskapazität. Mensch und Maschine, Pilot und Flugzeug, Wissenschaftler und Datenbank wären eine höchst effiziente Einheit.

5. Bereichsspezifische Anwendungen

Die IuK-Techniken werden je nach Anwendungsfeld den Markt in sehr unterschiedlicher Weise durchdringen. Für die Geschwindigkeit und Breite ihrer Diffusion sind vor allem folgende Faktoren relevant:

Unterstützend werden wirken:

- die wirtschaftliche Macht der IuK-Industrie, die alles daran setzen wird, die für den Absatz ihrer Produkte günstigsten Rahmenbedingungen zu schaffen;
- die wirtschaftliche Konkurrenz, die ab einer gewissen Marktreife der Produkte einen Nachfragesog schafft, weil die Nutzung der IuK-Technik Konkurrenzvorteile verspricht;
- die generationsbedingte Zunahme der Akzeptanz, die zu einer breiten Nutzung im privaten Bereich beiträgt;
- die Integration unterschiedlicher Informationstypen durch die Digitalisierung, die zu einem Entwicklungssprung in den Anwendungsmöglichkeiten der IuK-Technik führen wird;
- faktische Anschluß- und Benutzungszwänge, die dadurch entstehen, daß ab einer gewissen Marktdurchdringung diejenigen benachteiligt oder gar ausgegrenzt werden, die eine allgemein akzeptierte IuK-Technik nicht nutzen.

Hemmend werden dagegen wirken:

- die durch den Einsatz der IuK-Technik mitverursachte strukturelle Arbeitslosigkeit, die gewerkschaftlichen Widerstand hervorruft;
- mangelnde Qualifikationsvoraussetzungen und fehlende organisatorische Strukturen, die gegen Beharrungswünsche und bürokratischen Traditionalismus erst geschaffen werden müssen;
- eine ungenügende Berücksichtigung des sozialen Umfelds von Technikanwendungen, die zu Akzeptanzproblemen führt;
- Datenschutzinteressen, die versuchen, bestimmte Anwendungsformen zu verhindern bzw. zu modifizieren;
- Unmut über Großtechnik, den die psychischen und sozialen Folgekosten der IuK-Nutzung in bestimmten gesellschaftlichen Schichten hervorrufen und der zur Ablehnung von verzichtbaren IuK-Techniken führt.

In ihrer Auswirkung auf die Zukunftsentwicklung werden sich die fördernden Kräfte als wesentlich stärker erweisen. Hinter ihnen stehen die härteren Interessen. Der Widerstand der Gewerkschaften und des Datenschutzes werden nur kurzfristige Verzögerungen und oberflächliche Modifikationen bewirken. Da ihr Einfluß zunehmend schwindet, werden sie den Trend zur breiten Durchsetzung der IuK-Techniken nicht verändern. Allerdings wird die unterschiedliche sektorale, regionale und zeitliche Verteilung der hemmenden und fördernden Elemente zu großen Ungleichzeitigkeiten in der Diffusion führen. Klein- und Mittelbetriebe, mit nur regionalen Märkten werden die Technik in anderer Weise nutzen als Unternehmen, die auf dem Weltmarkt konkurrieren. Zu allen im folgenden aufgezeig-

ten Trendentwicklungen wird es immer auch schwächere Gegenströmungen geben. In etlichen Bereichen werden daher auch traditionelle Strukturen erhalten bleiben, und es wird sogar Inseln der 'Alternativwirtschaft' geben, in denen Leben und Arbeiten ohne intensive Nutzung moderner Technik möglich ist oder deren alternative Einsatzmöglichkeiten erprobt werden.

In welcher Weise die dargestellten technischen Möglichkeiten realisiert werden, wird vor allem durch die gesellschaftlichen Interessen und Konflikte in den jeweiligen Anwendungsbereichen bestimmt. Unter der Annahme der genannten Randbedingungen sind in einigen beispielhaft gewählten Gesellschaftsbereichen die folgenden Anwendungen zu erwarten:

Produktion

In der industriellen Fertigung werden IuK-Techniken in Zukunft weiter verstärkt genutzt werden, um die Produktivität zu steigern, den wachsenden Anforderungen des Marktes an Produktqualität und -Variation zu genügen und die Produktion so zu flexibilisieren, daß auf die rasche Veränderung der Nachfrage zeit- und kostengerecht reagiert werden kann.

Bis zum Jahr 2000 sollen durch Einsatz von IuK-Techniken die industrielle Fertigung weiter automatisiert und die bisherigen 'Rationalisierungsinseln' vernetzt werden. Die bestehenden Teillösungen für einzelne Unternehmensabteilungen können aber wegen der fehlenden Kompatibilität und der unterschiedlichen Funktionalität nicht einfach verknüpft werden. Vielmehr sind neue integrierende Systemkonzepte notwendig. Erste Vernetzungserfolge können allerdings erzielt werden. Durch Vernetzung von CAD und NC-Maschinen-Programmierung oder von Bestellwesen, Fertigungsplanung und Lagerhaltung können die Durchlaufzeiten verkürzt, die Lagerhaltung verringert und dadurch die Kapitalbindung reduziert werden. Diese Wirkungen werden noch unterstützt durch die fortschreitende Vernetzung großer Hersteller und ihrer Zulieferer. Deren so gesteuerte 'Just-in-Time'-Produktion erlaubt den Herstellern, nahezu ohne Lagerbestände zu produzieren.

Expertensysteme werden integraler Bestandteil dieser Vernetzungsstrategie sein. Sie finden Anwendung in der Fehlersuche, -diagnose und -beseitigung sowie in der Ablaufplanung und Prozeßabwicklung oder -überwachung. Vor allem große Unternehmen der Elektro- und Elektronikindustrie und aus den Bereichen Stahl, Chemie, Maschinen- und Fahrzeugbau werden die finanziellen Barrieren überwinden können, um Expertensysteme und ihr notwendiges Umfeld zu entwickeln. Auch der Konstruktionsprozeß erfolgt rechnergestützt. CAD-Programme sind erheblich verbessert: Konstruktionsroutinen sind weitgehend automatisiert, Expertensysteme und Anschlüsse an wissenschaftliche Datenbanken liefern Hintergrundwissen und neueste technische Daten. Ein weiteres wichtiges Einsatzgebiet für Expertensysteme ist die Prozeßsteuerung und -überwachung. Sie interpretieren die Fülle von Signalen, die Meßgeräte etwa in Chemie- oder Atomkraftwerken

liefern, lösen bei Unregelmäßigkeiten Alarm aus und veranlassen erste Gegenmaßnahmen.

Durch Automatisierung der Produktion wird versucht, die kapitalintensiven Fertigungseinrichtungen zumindest zeitweise völlig automatisch zu betreiben, um - bei sinkender Arbeitszeit - ihre Nutzungsdauer ohne zusätzliche Personalkosten zu verlängern und so die Stückkosten zu senken. In der Serienfertigung und in der Fließproduktion ist dieses Ziel durch den Einsatz von Robotern und anderen Automaten weitgehend, in der Auftragsfertigung teilweise erreicht. In der Massenfertigung ermöglicht der Robotereinsatz eine Flexibilisierung der Produktion. Gleichzeitig wurde das Einsatzfeld von Robotern ausgeweitet. Durch eine robotergerechte Konstruktion der Teile und Planung der Arbeitsabläufe sowie eine Verbesserung der Roboter selbst fertigen diese nicht mehr nur Einzelteile, sondern montieren sie auch zusammen. Probleme bereiten vor allem noch die Verknüpfung von Teilautomatisierungen und der Materialtransport.

Bis zum Jahr *2020* wird die betriebliche und überbetriebliche Vernetzung noch weiter vorangetrieben. Das Konzept der rechnerintegrierten Produktion (CIM - Computer Integrated Manufacturing) ist weitgehend verwirklicht. Es ist gelungen, aufgabenorientierte Gesamtsysteme zu realisieren, die eine gemeinsame Datenbasis und die Kompatibilität aller Funktionen sicherstellen. Vom Auftragseingang über Konstruktion, Produktionsplanung- und -steuerung, Materialwirtschaft, Fertigung, Montage bis zum Versand wird alles zentral geregelt, gesteuert und überwacht. Alle erforderlichen Informationen für die Bearbeitung eines Auftrags werden im Rechner verarbeitet und stehen in Echtzeit an jeder gewünschten Stelle zu Verfügung.

An einer weitergehenden Vernetzung (CAI Computer Aided Industry), die auch die übrigen Unternehmensfunktionen, vom Marketing und Vertrieb über die Buchhaltung, das Finanz- und Personalwesen bis hin zur strategischen Unternehmensplanung mit Hilfe von Expertensystemen einbezieht, wird gearbeitet.

'Intelligente', leicht umrüstbare Roboter haben einen weiteren Automatisierungsschub bewirkt. Sie sind mit Fernsehaugen und sonstigen Sensoren ausgerüstet und fähig, Muster zu erkennen, und können sich in eindeutig strukturierter Umgebung frei bewegen. Dadurch wird in bestimmten Bereichen der Materialtransport automatisierbar. Allerdings werden die automatischen Fabriken des Jahres 2020 den Bedürfnissen der Roboter und nicht die Roboter den bisher für Menschen gemachten Arbeitsplätzen angepaßt sein. Sie werden also eher ein Gebilde von hunderten fest eingebauter mechanischer Arme sein, die durch Computer gesteuert und überwacht werden. Die gegenüber heute sehr reduzierten Lager sind 'chaotisch' organisiert, von Rechnern verwaltet und von Robotern bedient.

Expertensysteme sind inzwischen die Standardform, technisch komplexe Systeme zu dokumentieren. Dies erleichtert den Umgang mit technischen Produkten von der Konstruktion bis zum Einsatz. Viele höherwertige Produkte sind mit 'Eigenintelligenz' ausgestattet. Sie enthalten kleine Expertensysteme, die ihre Bedienung erläutern, Wartungs-

hinweise geben, sich bei Störungen selbst diagnostizieren und den Reparateur anweisen. Bei trotzdem verbleibenden Schwierigkeiten hilft der Teleservice des Herstellers.

In der biochemischen Industrie werden IuK-Systeme für bio- und gentechnische Produktionsabläufe genutzt. Das Design von Enzymen etwa zur Entwicklung und Herstellung von Medikamenten basiert auf CAD-Methoden, die Produktionsprozesse werden von Computern gesteuert und die Genkartierung von Pflanzen, Tieren und Organismen erfolgt mit Hilfe von Datenbanken und ermöglicht gezielte manipulative Eingriffe.

Verwaltung

Während im Produktionsbereich die Produktivität bisher vor allem durch Technisierung gesteigert wurde, ist in der staatlichen und privatwirtschaftlichen Verwaltung die Leistungsfähigkeit in erster Linie durch eine Erhöhung des Personalstamms erreicht worden. Die Technisierung der Informationsverarbeitung verspricht daher, ein großes Rationalisierungspotential zu erschließen. Der Konkurrenzdruck und das Bedürfnis nach rationellem Informationsmanagement werden einen starken Druck zur Nutzung der IuK-Techniken ausüben. Wegen der fehlenden Konkurrenz wird dieser in der öffentlichen Verwaltung allerdings etwas geringer sein.

Um das Jahr *2000* werden viele der verschiedenen Datenverarbeitungssysteme, die in der Verwaltung genutzt werden, zu Rechnernetzen mit einem Großrechner im Hintergrund zusammengefaßt sein. Die Bearbeitung von Vorgängen findet am Arbeitsplatz statt. Fehlende Daten oder Programme liefert die zentrale Daten- und Programmbank. Der Trend, die intellektuellen Gehalte von der Fertigung abzutrennen und in die Arbeitsvorbereitung zu verlagern, wird durch die IuK-Technik verstärkt. Sie ermöglicht, Teilfunktionen aus dem Betrieb auszulagern. Sie werden im privatwirtschaftlichen Bereich, soweit dies nicht aus Konkurrenzgründen ausgeschlossen ist, zunehmend entweder von Großunternehmen, die Verwaltungsaufgaben zum Teil weltweit erledigen, oder von kleineren 'Service-Rechenzentren' übernommen, die beliebigen Kunden vor allem aus dem Mittelstand gegen Gebühren Rechnerkapazität und Programme anbieten. Der Zugang zu den Zentren erfolgt mit Hilfe von - meist privaten - Telekommunikationsdiensten.

Auch in der öffentlichen Verwaltung wird die Informationsverarbeitung in vernetzten Systemen zusammengefaßt, die die Rechner der einzelnen Behörden und Abteilungen mit 'Informationstechnischen Zentren' verbinden. In geeigneten Bereichen (z.B. Haushaltswesen) werden ressortübergreifende Systeme eingesetzt. An den Arbeitsplätzen werden PCs genutzt, die die Sachbearbeiter führen und unterstützen. Die Kompatibilität der verschiedenen Systeme soll durch neu errichtete Koordinationsstellen oder von Systembeauftragten sichergestellt werden.

Viele bisher getrennte Arbeiten in der Verwaltung (z.B. Erfassung, Bearbeitung, Berechnung, Durchsetzung usw.) werden an den IuK-Sachbearbeiter-Arbeitsplätzen zusammengefaßt. Die Sachbearbeiter können dadurch alle anfallenden Vorgänge unter

Führung von (Verwaltungs-) Datenbanken, Informations- und Expertensystemen selbständig bearbeiten. Da diese Hilfssysteme ständig aktualisiert und beispielsweise an neue Gesetze und Verordnungen angepaßt werden, sind die Verwaltungsentscheidungen stets auf dem aktuellen Stand. Texterfassende Scanner ermöglichen es, die eingehende Briefpost in die elektronischen Bürosysteme aufzunehmen und automatisch an den richtigen Platz zu verteilen. Unter Nutzung von Textbausteinen bringen die Sachbearbeiter ihre Ergebnisse auch gleich selbst in Schriftform. Die Zugriffskompetenzen auf die in den zentralen Systemen gespeicherten Informationen sind aufgabenbezogen begrenzt und hierarchisch gegliedert: Jeder Sachbearbeiter erhält nur die seinem spezifischen Aufgabenbereich entsprechenden Informationen. Auf der Führungsebene bestehen dagegen umfassende Zugriffsrechte. Hier stehen 'Hintergrundsysteme' zur Verfügung, die es ermöglichen sollen, große Datenmengen zu verwalten und den Bestand, die Planung und den Vollzug aktuell zu überblicken.

Auch die Kommunikation zwischen Bürger bzw. Kunde und Verwaltung wird durch die IuK-Technik geprägt. Um sie besser nutzen zu können, wird die Formalisierung vorerst weiter zunehmen. Durch die IuK-technische Ausstattung werden die Verwaltungsmitarbeiter in die Lage versetzt, einzelfallbezogene Entscheidungen unmittelbar zu fällen und zu präsentieren. Lediglich in 'Spezialfällen', die in dem Verwaltungsprogramm nicht berücksichtigt sind, ist die Vorlage an einen Vorgesetzten erforderlich. Soweit Anträge oder Anfragen auf elektronischem Weg gestellt werden, antwortet die Verwaltung mit Hilfe der IuK-Technik.

Um das Jahr *2020* wird die elektronische Kommunikation mit Verwaltungen zum Regelfall werden. Sie wird sich allmählich durchsetzen, weil sie kostengünstiger, bequemer und zeitsparender ist. Viele formalisierte Verfahren können automatisch bearbeitet und abgewickelt werden. Die Entscheidungen werden elektronisch zugestellt. Bürger, die nicht über die notwendigen IuK-Geräte oder -kenntnisse verfügen, können an zentralen Stellen öffentliche Terminals benutzen bzw. Bürgerbüros konsultieren.

Zur Simulation in der Planung, zur Entscheidungsvorbereitung und in Routinefällen auch zur Entscheidung werden Expertensysteme breit eingesetzt. Vor allem in der steuernden Verwaltung werden sie genutzt, um unter verschiedenen Entscheidungsalternativen nach vorgegebenen Zielen die optimale zu finden.

In der Phase bis etwa *2000* führt die steigende Produktivität der Verwaltung kaum zu Entlassungen, sondern ermöglicht eine Ausweitung der Aufgaben und eine Reduzierung des Personals durch natürliche Fluktuation und zeitweilige Einstellungsstops. Danach jedoch steht durch die 'Televerwaltung' und die 'Selbstverwaltung' der Bürger bzw. Kunden im direkten elektronischen Dialog mit den Verwaltungs-DV-Systemen ein massiver Abbau von Arbeitsplätzen bevor.

Der steigende Problemdruck wachsender Kriminalitätsraten, vermutlich wiederkehrende Terror- und Antiterrorismuskampagnen sowie präventive Strategien für gesellschaftliche Instabilität werden die Behörden der inneren Sicherheit dazu drängen, die

Möglichkeiten der IuK-Technik für ihre Zwecke zu nutzen. Sie werden bis zum Jahr *2000* ihre Datenbanken modernisieren und auf der Basis des ISDN zu einem integrierten Informationsverbund aller Polizeien ausbauen. Zur Informationsgewinnung nutzen sie zunehmend den Fernzugriff auf elektronische Datenbestände anderer Behörden. Neue elektronische Fahndungsmethoden wie Raster- oder Gitternetzfahndung können dadurch leichter praktiziert werden. Maschinenlesbare Ausweise beschleunigen Kontrollen und werden daher auch zur Erfassung von großen Massen, etwa bei Demonstrationen eingesetzt. Die Digitalisierung der Telekommunikation, die eine Zwischenspeicherung der Nutzungs- und Inhaltsdaten erforderlich macht, verbessert zugleich die Möglichkeiten ihrer Überwachung. Zu deren Rationalisierung könnten Kommunikationskanäle direkt zu den Polizeirechnern durchgeschaltet werden. Diese wären künftig in der Lage, nicht nur den Telefonverkehr, sondern jeden Austausch von Sprache, Daten, Texten und Bildern sowie jeden Telekommunikationsdienst (Btx, Temex, Mailbox etc.) zu kontrollieren.

Bis zum Jahr *2020* werden Methoden der 'künstlichen Intelligenz' den Behörden helfen, ihre nahezu vollständig elektronisch geführten Aktenbestände auszuwerten. Durch die zu erwartenden Fortschritte der Spracherkennung und -verarbeitung kann die Überwachung der Telekommunikation weitgehend automatisch erfolgen und dadurch erheblich effektiver werden. Mit Hilfe dieser Verfahren könnte die Kommunikation der zu überwachenden Teilnehmer maschinell vorausgewertet werden, um die für Sicherheitszwecke irrelevanten Teile gleich auszusondern. In ähnlicher Weise unterstützen die Methoden der Mustererkennung und -verarbeitung die Videoüberwachung.

Dienstleistung

Auch im Dienstleistungsbereich werden bei sinkenden Wachstumsraten Rationalisierungszwänge zu einer Fortsetzung der technischen Informationsverarbeitung führen. Da hier die Personalkosten teilweise bis zu 80% der Betriebskosten ausmachen, liegt es nahe, dem Konkurrenzdruck durch Einsatz von IuK-Techniken zu begegnen. Einen weiteren Einsparungseffekt verspricht die elektronische Verlagerung von Arbeit auf die Kunden.

Die *Banken* werden bis um das Jahr 2000 neben ihrem klassischen Geld- und Anlagengeschäft ihre Tätigkeit auch auf 'bankfremde' Bereiche wie z.B. Versicherungen, Rentenberatung oder Immobilien ausdehnen. Für diese Aufgabenausweitung werden sie jedoch kein zusätzliches Personal einstellen, sondern neue technische Systeme nutzen. Hierfür bietet sich vor allem der Zusammenschluß vorhandener Einzellösungen zu integrierten Gesamtkonzepten und der weitere Ausbau der EDV zu komplexen on-line-Systemen an. Im Zuge dieser Umstellung werden die Banken Btx-Banking ausbauen und die Daten- und Textverarbeitung mit der Sachbearbeitung zu papierarmen Bürosystemen integrieren. Einer dezentralen Verfügbarkeit der Daten wird eine zentralisierte Organisation der Datenverarbeitung gegenüberstehen. Geschäftsvorgänge und Arbeitsergebnisse

werden direkt in der zentralen Datenverarbeitung gespeichert und sind an den Arbeitsplätzen jederzeit verfügbar. Außerdem können die Sachbearbeiter auf Datenbanken und Expertensysteme zurückgreifen, die ihnen die Arbeit weitgehend vorstrukturieren und einzelne Vorgänge automatisch entscheiden. Das Schaltergeschäft wird unter Einsatz von PCs mit Hilfe spezieller Beratungsprogramme abgewickelt. Expertensysteme werden genutzt für die Prüfung der Kreditwürdigkeit, in der Anlagenberatung, in der Beratung zur Beteiligungspolitik der Kunden, in der Depotbetreuung, in der Geschäftsfeldgestaltung, im Cash Management und in der Überwachung der Bankgeschäfte. Die IuK-Technik erlaubt, die traditionelle Spartenorganisation in eine nach Kundengruppen orientierte Organisationsstruktur zu verändern.

Da sich der Trend zum bargeldlosen Zahlungsverkehr fortsetzen wird, müssen die DV-Systeme der verschiedenen Banken stärker vernetzt werden, um die Milliarden täglich anfallender Zahlungen abwickeln zu können. Der notwendige Datenaustausch findet über große Rechenzentren statt, die auf nationaler und internationaler Ebene bestehen. Ein Teil der Transaktionen wird unter Einsatz von Electronic Fund Transfer Systems (EFTS - "elektronisches Geld") oder ähnlicher Systeme durchgeführt. Da das internationale Bankgeschäft immer komplexer und schneller wird und Experten in diesem Feld knapp sind, besteht ein erheblicher Bedarf an automatischer Expertise.

Die Banken streben bis *2000* eine Intensivierung der Kundenselbstbedienung an. Dem Kunden werden personallose Schalterhallen mit frei zugänglichen Terminals und Geldautomaten angeboten, für die mit dem Argument der 24-stündigen Verfügbarkeit geworben wird. Solche automatischen Bankschalter können auch an Bahnhöfen, Einkaufszentren und ähnlichen zentralen Stellen eingerichtet werden. Für die Nutzung dieser SB-Konten bieten die Banken anfangs Sondervergünstigungen an und erreichen dadurch eine hohe Akzeptanz. Sind bis zum Jahr 2000 die SB-Konten für das Massengeschäft zum Regelfall geworden, werden die Gebühren wieder ansteigen. Im geschäftlichen Bereich werden Bankgeschäfte bereits weitgehend über Btx abgewickelt.

Eine ähnliche Einführungsstrategie führt zu einer weiten Verbreitung von Chipkarten als maschinenlesbarem Geldsubstitut. Die Banken werden - je nach Größe und Marktmacht - entweder eigene Kreditkarten einsetzen oder aber den Anschluß an bestehende Kreditkartensysteme suchen. Neben den Banken bietet der Handel eigene Chipkarten an. Diese verdrängen dabei mit Ausnahme von Briefschecks alle anderen Formen bargeldloser Zahlung (EC-Schecks) weitgehend. Der Besitz und der Umgang mit Chipkarten ist allgemein üblich und verbreitet. Die bargeldlose Zahlung hat sich in allen Bereichen durchgesetzt, in denen der SB-Anteil traditionell hoch ist oder klare Abrechnungsstrukturen herrschen wie an Automaten, in Tankstellen, Verbrauchermärkten, Kaufhäusern, Post, Bahn, Leihwagenbüros, Restaurants, Werkstätten.

Die Chipkarten werden mit einem Kennwort genutzt und gelten damit als gegen Verlust und Mißbrauch weitgehend gesichert. Direkte on-line-Buchungen wird es aus Kostengründen nur bei größeren Beträgen geben. Kleinere Beträge werden von dem auf der

Chipkarte abgespeicherten Guthaben 'abgebucht' oder nach Übermittlung des Vorgangs an die Bank des Kunden von dessen Konto abgezogen.

Um das Jahr *2020* wird Telebanking auch im Massengeschäft weit verbreitet sein. Dieser Trend wird unterstützt durch den Abbau der personalintensiven direkten Dienstleistungs- und Beratungsangebote und die Reduzierung der Zweigstellen. Gleichzeitig ermöglichen die elektronischen Bankgeschäfte erst eine Reduzierung des Filialnetzes. Bankberatungen übernehmen spezielle Expertensysteme, die von zu Hause aus angewählt werden können. Der Vorteil eines dichten Filialnetzes, den Großbanken und Sparkassen bisher hatten, wird durch diese Umstrukturierung an Bedeutung verlieren und kleineren Banken neue Konkurrenzchancen einräumen. Mehr als die örtliche Verfügbarkeit wird die Flexibilität und die Spezialisierung auf die Wünsche bestimmter Kundengruppen entscheidend sein.

Der elektronische Zahlungsverkehr hat das Bargeld in vielen Bereichen völlig verdrängt. Barzahlung ist hier nur noch unter erschwerten Bedingungen möglich. Allerdings wird es immer noch Geldstücke und Geldscheine geben - nicht nur, weil einige ältere Menschen nostalgisch daran festhalten, sondern vor allem als Zahlungsmittel der Schattenwirtschaft und des kriminellen Bereichs.

Um gegenüber anderen Anbietern konkurrenzfähig zu bleiben, müssen auch die *Versicherungen* ihre Verwaltungsabläufe durch den Einsatz von IuK-Techniken rationalisieren. Bis um das Jahr *2000* werden deshalb alle Verwaltungsdaten in zentralen DV-Systemen gespeichert sein. Die Verwaltungsarbeit erfolgt unter Einsatz dieser Datenbanken und Expertensysteme vollkommen 'papierlos'. Nur für die Korrespondenz mit den Versicherten wird noch auf 'normale' Briefe zurückgegriffen, die aus Textbausteinen erstellt werden. Die alte Spartenorganisation wird durch eine nach Marketinggesichtspunkten ausgerichtete kundenorientierte Organisationsstruktur ersetzt.

Vertreter und Agenturen werden stärker in die zentrale EDV einbezogen. Über Modems, Akustikkoppler und Btx haben sie direkten Zugriff auf die DV-Systeme und dokumentieren dort ihre Arbeitsergebnisse. Den Versicherten werden aber auch 'Televersicherungen' über Btx angeboten: Sie können sich direkt am Bildschirm über die Angebote informieren, Versicherungen abschließen oder verändern und Schadensmeldungen eingeben. Zur Erhöhung der Akzeptanz wird auch hier anfangs mit Vergünstigungen geworben.

Mit der Einführung der Kundenselbstbedienung wird ein entscheidender Schritt auf dem Weg zur automatischen Erledigung von Geschäftsvorgängen zurückgelegt. Um das Jahr *2020* wird die Kommunikation nur noch zwischen Versicherten und den verschiedensten Expertensystemen der Versicherungen für Beratung, Vertragsangelegenheiten und Schadensabwicklung erfolgen, ohne daß im Regelfall noch Sachbearbeiter eingeschaltet werden. Deren Eingreifen ist nur noch in unklaren Problem- oder Grenzfällen erforderlich.

Im *Handel* bauen die großen Unternehmen ihre marktbeherrschende Position aus, der Handel-Banken-Verbund wird stärker und der Versandhandel nimmt zu. Im Kampf um den kleiner werdenden Markt versuchen sie das IuK-immanente Rationalisierungspotential (Schätzungen gehen bis 40%) möglichst auszuschöpfen. Dabei kommt der DV-unterstützten Warenwirtschaft eine Schlüsselstellung zu. Kernstück der elektronischen Warenwirtschaft sind die on-line-Kassen und das automatische Lager- und Bestellwesen. Die Auswertung der anfallenden Daten ermöglicht es, schnell auf Markt- und Preisschwankungen zu reagieren. Um das Jahr *2000* haben kleine Filialen ihre Selbständigkeit weitgehend verloren und werden elektronisch an zentrale Niederlassungen oder an die Konzernspitzen angebunden und von dort 'mitverwaltet'. Viele Entscheidungskompetenzen werden auf DV-Systeme übertragen.

Ein weiterer Rationalisierungsschub geht mit der Einführung von Point-of-Sale-Systemen einher. Die Erfassung der Kundenidentifikation und der gekauften Produkte ermöglichen dem Handelsunternehmen präzise (anonymisierte) Verbraucher- und Warenprofile zu erstellen. Sie können so die Reaktionen jedes Haushalts oder einzelner Kundengruppen auf unterschiedliche Produkte, Promotionsmethoden, Werbemedien oder Preisgestaltungen orts- und zeitkongruent auswerten. Auf der Basis dieser Daten versuchen Marketingstrategen, das Verbraucherverhalten zielgenau zu beeinflussen.

Auch im Handel werden Umsatzsteigerungen durch elektronische Kundenselbstbedienung erwartet. Wie heute bereits in den USA wird TV-Shopping bis zum Jahr 2000 insbesondere in strukturschwachen Gebieten sehr an Beliebtheit gewinnen. Im Fernsehen wird in einer Werbesendung ein Produkt angeboten, über Telefon bestellt und in kürzester Zeit geliefert. Bis zum Jahr 2000 zurückhaltend, bis zum Jahr *2020* verstärkt werden Bestellungen im Versandhandel auch über Btx getätigt. Neben einem offenen Angebot für alle Kunden gibt es gezielte Angebote für bestimmte (zahlungskräftige) Verbrauchergruppen. Auch werden die verfügbaren Kundeninformationen für gezielte Werbeaktionen genutzt. Die elektronischen Vergleichsmöglichkeiten führen bei gleichartigen Produkten zu einer höheren Markt- und Preistransparenz - und damit auch zu einer Verschärfung der Konkurrenz. Die Handelsbetriebe haben ihre Verwaltungsaufgaben in einem EDV-gestützten Warenwirtschaftssystem zentralisiert, das Kassenwesen, Inventur, Lagerhaltung, Disposition, Personal, Finanz- und Rechnungswesen integriert. Verpackung und Auszeichnung wurden auf den Produzenten verlagert.

Teleshopping wird für unverderbliche Waren und solche ohne Beratungsbedarf wegen der Zeit- und Kostenersparnis weite Verbreitung finden. Die IuK-Technik ermöglicht, direkt beim Hersteller zu bestellen und von diesem direkt liefern zu lassen. Da so die Handelsspannen entfallen, wird von dieser Möglichkeit zumindest nach 2000 reger Gebrauch gemacht. Im Handel führt diese Umsatzeinbuße zu einem verschärftem Konkurrenzkampf.

Bis zum Jahr *2000* werden viele *Datenbanken* exklusive oder in besonderer Weise aufbereitete Daten kommerziell anbieten. Informationen können in einfachen standardi-

sierten Abfragesprachen on-line abgerufen werden. Für Unternehmen sind hauptsächlich technisch-wissenschaftliche Informationen sowie Wirtschafts- und spezielle Nachweisdatenbanken interessant. Wissenschaftler werden Literatur- und Faktensammlungen nutzen. Privathaushalte könnten Nachrichten oder Produkt- und Preisinformationen nachfragen. Nicht jeder wird jedoch Daten aus den kommerziellen Datenbanken abrufen können. Neben dem notwendigen Geld wird es vielen auch an dem immer noch erforderlichen Kontext- und Strukturwissen fehlen.

In den *übrigen Sektoren* des Dienstleistungsbereichs sind ähnliche Anwendungen der IuK-Techniken zu erwarten. Sie werden zum einen zum Erbringen der Dienstleistung und zum anderen von den Anbietern selbst genutzt. Steuerberater, Rechtsanwälte und Wirtschaftsprüfer etwa werden das für sie notwendige Wissen in den Wissensbanken ihrer Expertensysteme vorhalten bzw. sich telekommunikativ besorgen und durch die dazugehörige Inferenzmaschine verarbeiten. Ähnlich werden Softwarehäuser oder private Ingenieurbüros IuK-Techniken nutzen. Telekommunikation fördert das Wachstum qualifizierter Beratungsdienste. Die Aufwendungen für Software und deren Pflege werden künftig den weit überwiegenden Teil der EDV-Ausgaben ausmachen. Spezialisierte Unternehmen, die auch Möglichkeiten der telekommunikativen Fernwartung nutzen, finden hier einen neuen Markt. Kleinere Unternehmen profitieren davon, daß größere Betriebe Dienstleistungen auslagern.

Die durch Temex möglichen Fermeß- und Fernwirkdienste werden den Markt für Sicherungs- und Überwachungsunternehmen stark erweitern. Über Temex werden Klima- und Heizungsgeräte gesteuert und kontrolliert, über die Fläche verteilte Maschinen oder entfernt ablaufende technische Prozesse überwacht, Füllstände in Warenautomaten, Tanks oder sonstigen Behältern gemessen, die Beleuchtung von Gebäuden reguliert, Meßgeräte abgelesen, Notrufe übermittelt oder Brände und Einbrüche gemeldet.

Dienstleistungen werden in zunehmendem Maß vom heimischen Terminal aus in Anspruch genommen. Rechtsauskünfte, psychosoziale Beratung, Reiseauskünfte und -buchungen, Börsen- und Anlagenberatung, medizinische Ratschläge, Informationen zu Alltagsproblemen oder Sprachübersetzungen werden entweder von Expertensystemen erteilt oder in schwierigeren Fällen über Bildschirmdialog gegeben. Die Freizeitindustrie wird vor allem durch technisch unterstützte und sogar Naturerlebnisse simulierende Leistungen einen weiteren Aufschwung erleben. Neben den elektronisierten werden aber auch 'klassische' Dienstleistungen wie Kranken- oder Kinderbetreuung, Kunst- und Reperaturhandwerk bestehen bleiben.

Medien

Um das Jahr *2000* wird die Mehrzahl der geschäftlichen Telefonhauptanschlüsse ISDN-Anschlüsse sein. Private Haushalte nutzen die neuen über ISDN verfügbaren Dienste dagegen noch wenig. Am meisten nachgefragt wird noch der neue Btx- Dienst. Btx 2000

unterscheidet sich von früheren Versionen durch wesentlich kürzere Bildaufbauzeiten, einen Tonkanal und Kombinationsmöglichkeiten mit PCs, Bildplatten und anderen IuK-Techniken. Die verbesserte Technik hat die Akzeptanz des Mediums so weit erhöht, daß immerhin einige Millionen Haushalte, vor allem aus der Mittelschicht, Btx nutzen. Bezieher niedrigerer Einkommen werden diesen Dienst allerdings selten in Anspruch nehmen. Andere neue Dienste, wie etwa Bildfernsprechen über ISDN, Videoconferencing, Sprachspeicher- und Mailboxdienste und Funkruf, werden fast nur für geschäftliche Kommunikation genutzt oder von privaten Dienstleistungsunternehmen in speziellen Räumen angeboten.

Im Hörfunk und im Fernsehen bleiben zwar die öffentlich-rechtlichen Sendeanstalten erhalten, geraten aber gegenüber einer zunehmenden Anzahl privater Anbieter unter Druck, weil Zuschauer und Werbeeinnahmen begrenzt sind. Neben den heute schon bestehenden privaten überregionalen Programmen werden zwei oder drei weitere Programme über Satelliten ausgestrahlt und in die örtlichen Kabelverteilnetze eingespeist. Wer es sich leisten kann, wird diese und andere internationale Satellitenprogramme direkt über Parabolantennen empfangen.

Viele lokale oder regionale Sendungen werden ausgestrahlt, die 'Fenster' von großen bundes- oder europaweiten Rahmenprogrammen ausfüllen. Die Sendungen werden von Zeitungsverlagen oder eigenen Unternehmen meist unter Beteiligung der Kommunen produziert. Sie bieten überwiegend eine Programmischung aus lokaler Berichterstattung, Sportübertragungen, Musik, und Werbung an. In größeren Städten gibt es auch 'offene Kanäle', über die unterschiedliche Organisationen eigene Sendungen ausstrahlen können. Die Zulassung zu den 'offenen Kanälen', die Unbedenklichkeit der Inhalte der einzelnen Sendungen und die 'Ausgewogenheit' des gesamten Programms wird von pluralistisch zusammengesetzten Programmkomitees überwacht.

Unter den Printmedien werden die neuen spezialisierten Zeitschriften weiter zunehmen. Die neuen Satz- und Drucktechniken (desk top publishing) verringern den finanziellen Aufwand der Herstellung beträchtlich. Dadurch können auch Zeitschriften für einen lokal begrenzten oder inhaltlich beschränkten Interessentenkreis angeboten werden. Hingegen wird sich bei den Tageszeitungen der Konzentrationsprozeß fortsetzen, weil konkurrenzfähige Korrespondentennetze und Vertriebsstrukturen nur von größeren Verlagen unterhalten werden können.

Um das Jahr *2020* wird sich in den meisten Haushalten die Fernsehnische in eine Telematikecke verwandelt haben. An den ISDN-Hauptanschluß sind zumindest ein PC und ein Drucker angeschlossen. Der Fernseher wird durch ein gesondertes Breitbandkabel versorgt. Darüber hinaus können noch weitere IuK-Geräte angeschlossen und zu einem elektronischen 'Heiminformationssystem' integriert werden. Haushalte mit höherem Einkommen verfügen über einen IBFN-Anschluß. In ihren Telematikecken steht ein großdimensionierter Bildschirm für hochauflösendes dreidimensionales Fernsehen mit Raumklangatmosphäre. IBFN-Teilnehmer werden nur noch selten feste Fernsehprogramme

sehen, sondern ihre Programmfolge individuell gestalten. Sie rufen sich je nach Interesse Nachrichten, Kultursendungen, Magazine oder Shows aus dem breiten aktuell gesendeten Programm der Sendeanstalten ab (pay per view). Individuelles Pay-Video (jedem seinen Wunschfilm) wird es auch 2020 noch nicht geben, weil dies sogar das IBFN überlasten würde. Zum Telefonieren kann ein Bildkanal zugeschaltet werden (Bildfernsprechen). Videobesuche bei Verwandten und Freunden oder themenbezogene Videotreffs gelten als rationell und schick. Übergänge zwischen verwandten ISDN- und IBFN-Diensten sind realisiert. Viele Filme sind synthetisch. Sie werden von wenigen Designern anhand einer vom Autor entwickelten Idee erstellt. Besonders beliebt ist interaktives Fernsehen, bei dem sich die Zuschauer in das Filmgeschehen einschalten und den Filmausgang beeinflussen können.

Wer es sich leisten kann, hat die Wahl unter einer Fülle neuer elektronischer Dienstleitungen. Spezielle Programme stellen zu einem gewünschten Themengebiet Meldungen aus verschiedenen Pressediensten und Zeitungen zusammen. Ein 'automatischer Pressereferent' kann sogar morgens in 'natürlicher' Sprache kurz über die lokalen und globalen Neuigkeiten berichten und über die verschiedenen Kommentare informieren. Die Printmedien werden teilweise von elektronischen Medien ersetzt, jedoch nicht völlig verschwinden, da sie flexibler zu benutzen sind.

Bücher im traditionellen Sinn werden immer seltener produziert. Gefragt sind interaktive elektronische 'Bücher', die Textteile, Farbbilder, Filmsequenzen und Programme miteinander verbinden und bei Bedarf auch mit elektronischen Vorlesemaschinen gekoppelt werden können. Die einfache Benutzung und die Flexibilität im Umgang wird Bücher jedoch zumindest in der Belletristik erhalten. Wissenschaftliche Publikationen läßt man sich dagegen gegen eine Gebühr elektronisch übermitteln und bei Bedarf auf hochleistungsfähigen Laserdruckern ausdrucken.

Öffentliche Bibliotheken werden in Mediotheken verwandelt. Sie verleihen Videos, Bildplatten, Programme, elektronische, interaktive und konventionelle Bücher. Von der Telematikecke zu Hause können elektronische Bibliotheken angewählt werden, in denen Recherchesysteme helfen, interessante Literatur ausfindig zu machen. Etwas teurer kommt der "automatische Bibliothekar", der in natürlicher Sprache Benutzerwünsche aufnimmt und Literaturangebote unterbreitet.

Die Nutzung der neuen Medien wird nicht wenig kosten. Um auch die Haushalte mit niedrigem Einkommen nicht völlig aus der Informationsgesellschaft auszuschließen, wird ihnen ein Medienminimum garantiert. Hierzu gehört der ISDN-Anschluß, Kabelanschluß, ein Bildschirm, ein einfacher PC und ein Drucker sowie begrenzte Benutzungseinheiten verschiedener Grunddienste. Sie können auch das öffentlich-rechtliche Fernsehen kostenlos empfangen.

Bildung und Wissenschaft

Der Erfolg auf den Weltmärkten und die notwendige Akzeptanz für die Angebote des heimischen Marktes hängen entscheidend vom Qualifikationsniveau der Beschäftigten und Kunden ab. Bis zum Jahr *2000* ist daher für rund die Hälfte aller Beschäftigten eine Weiterbildung in der Nutzung von IuK-Techniken notwendig. Die sich schnell ändernden Anforderungen des Berufslebens machen für viele Erwerbstätige auch weiterhin eine häufige oder kontinuierliche Weiterbildung notwendig. Ebenso muß die Ausbildung Jugendlicher den künftigen Berufsanforderungen gerecht werden.

Um die Kosten zu senken und die Qualität zu steigern, werden IuK-Techniken bis zum Jahr *2000* auch im *Bildungsbereich* breite Anwendung finden. Dies gilt natürlich für die neue informationstechnische Grundbildung. Computer als Lernhilfen werden aber auch für repetitives Lernen oder zur Modellbildung in Sozial- und Naturwissenschaften eingesetzt. Für die Schüler werden mit solchen Simulationsmodellen komplexere und dadurch wirklichkeitsnähere Probleme zugänglich. In den Oberklassen werden Informationen über öffentliche Datenbanken beschafft.

Während die schulische Ausbildung weiterhin Domäne des Staates bleiben wird, bieten kommerzielle Unternehmen in Konkurrenz mit den Hochschulen eine breite Palette von Schulungs- und Weiterbildungsmöglichkeiten an. Sie nutzen alle zur Verfügung stehenden IuK-Techniken zum Fernunterricht. Dieser kann von den Nachfragern nach individuellen Bedingungen und Zeiten belegt werden. Die berufliche Weiterbildung kann so ohne zusätzliche Zeitverlust in der Freizeit erfolgen.

Der Trend zur Nutzung der IuK-Technik setzt sich im Bildungsbereich in der Zeit bis *2020* fort. In diesem Zeitraum kommen Expertensysteme zum Einsatz, die den Schüler führen und sich seinem Niveau und seiner Lerngeschwindigkeit individuell anpassen. Andere Lerninhalte werden durch interaktives Video vermittelt. Kollektive Wissensaneignung durch gemeinsame Übungen, Lehrervortrag oder Buchlektüre findet nur noch selten statt.

Die IuK-Technik-vermittelte Individualisierung des Lernens verändert die Funktion der Pädagogen und der Schulorganisation. Sie fordert und verstärkt das Eigenengagement des Lernenden. Quantifizierbare, berechenbare, modellhaft abbildbare Aspekte und abfragbares Wissen treten mehr in den Vordergrund. Der Lehrer wird von Wissensvermittlung entlastet und hätte mehr Zeit für die eigentlich pädagogischen Aufgaben, wenn nicht diese Zeit einer Rationalisierung der Lehrerarbeit zum Opfer fallen würde. Je nach Bundesland und Schultyp ergeben sich hier deutliche Unterschiede. Der Klassenverband und die Jahrgangsklassen verlieren ebenso an Bedeutung wie die Lehrpläne und die Abgrenzung der einzelnen Schulfächer.

Im *Wissenschaftsbetrieb* werden sich bis zum Jahr *2000* wesentliche Veränderungen vor allem im Informationszugang ergeben. Spezialwissen unterschiedlicher Fach- und Wissensgebiete wird mit Hilfe großer Datenbanken geordnet und bereitgehalten. In ihnen

sind Stichworte, Abstracts, Inhaltsverzeichnisse und Volltexte gespeichert. Sie werden Text, Graphik und Bilder verarbeiten und ausgeben können. Monographien und wissenschaftliche Aufsätze werden in der Regel nur noch elektronisch publiziert und lediglich bei Bedarf als Hardcopy ausgedruckt. Die elektronische Verfügbarkeit wissenschaftlicher Informationen an jedem Ort wird zu einer weiteren Spezialisierung und Zentralisierung wissenschaftlicher Bibliotheken führen. Der Zugang zu den Datenbanken wird über die Postdienste ermöglicht. Da sie kommerziell betrieben werden, wird aktuelle Fachinformation hoher Qualität zu einem neuen ökonomischen Faktor werden.

Durch die Entwicklung von Hochleistungsrechnern mit Parallelarchitektur und der passenden Software werden wesentlich verbesserte Simulationssysteme möglich. Sie finden vorwiegend für technisch-konstruktive und wissenschaftliche Aufgabenstellungen Anwendung. Die hohen Verarbeitungskapazitäten erlauben bereits um das Jahr 2000 realitätsnahe physikalische Modelle, die in vielen Bereichen empirische Versuche ersetzen können. Die Grenznen sozialwissenschaftlicher und ökomonischer Modelle liegen dagegen weniger im Bereich der Verarbeitungskapazität als vielmehr im Bereich der Formalisierbarkeit der untersuchten Probleme.

Um das Jahr *2020* sind aus diesen Datenbanken Wissenssysteme geworden, die wissen, was sie wissen, und vor allem, was sie nicht wissen. Sie können dem Suchenden Literaturhinweise geben, im Dialog aufgrund der bisher erfaßten Literatur das zu untersuchende Problem spezifizieren, selbständig Literaturrecherchen und -auswertungen vornehmen und wissenschaftliche Veröffentlichungen automatisch in fremde Sprachen übersetzen. Qualitativ hochwertige Forschung wird dadurch allerdings zunehmend von Mitteln für die Informationsbeschaffung abhängen. Die gleichartige Darstellung von Wissen ermöglicht es, sich die Wissensbestände auch anderer Disziplinen leichter anzueignen und interdisziplinäres Denken stärker zu etablieren.

Computer- oder Videokonferenzen unterstützen die Zusammenarbeit von Wissenschaftlern. Expertensysteme werden in allen Wissenschaftsbereichen Anfragen beantworten, Thesen überprüfen, Vorschläge für noch zu erstellende Dissertationen unterbreiten. In der Mathematik können sie automatische Beweise liefern, in der Psychologie Verhaltens- und Entscheidungsmodelle und Simulationsmöglichkeiten zur Verfügung stellen, in den Sozialwissenschaften komplexe Simulationen und Szenarien herstellen, in der Rechtswissenschaft das Präjudizienmaterial strukturieren oder Analogien bilden und in den Natur- und Ingenieurwissenschaften zur Wissensdarstellung, zur Simulation, zur Konsistenzprüfung und zur Verifikation von Thesen eingesetzt werden. Die oben genannten Probleme der Modellbildung und ihrer unvermeidlichen Kontext- und Realitätseinbußen werden diesen Anwendungen Grenzen setzen und immer wieder zu Rückschlägen führen. Dennoch sind Rechnerunterstützung und Expertensysteme aus dem Wissenschaftsbetrieb nicht mehr wegzudenken - und zahlreiche Fachgebiete von ihrem Einsatz abhängig.

Medizin

Die Zunahme von Zivilisationskrankheiten wie Allergien, von psychosozialen Erkrankungen und von Aids wird zu Kostensteigerungen im Gesundheitswesen führen. Hinzu kommen der vermehrte Einsatz teurer Spezialgeräte sowie Preissteigerungen für pharmazeutische Produkte. Die relative Zunahme älterer Menschen führt zu einem höheren Bedarf an Gesundheitsdienstleistungen. Gleichzeitig sinkt die Zahl der Erwerbstätigen, die die Finanzierung des Gesundheitswesens sichern können. Dem dadurch entstehenden Kostendruck begegnen die Träger durch Rationalisierungen und Einsparungen mit Hilfe von IuK-Techniken, Teilautomatisierung und 'Selbstversorgung' der Patienten, um nach Möglichkeit kostenneutrale Verbesserungen der medizinischen Versorgung zu erreichen.

Bis zum Jahr *2000* werden die Möglichkeiten der Diagnose, der Therapieplanung und -überwachung, der Intensivmedizin, der Labormedizin und der Prothetik durch IuK-Technik erheblich verbessert. So reduzieren zum Beispiel neue Verfahren der Bilderzeugung, Aufbereitung und -interpretation die Strahlenbelastung der Patienten. Mit dreidimensionalen Bilddarstellungen und Computersimulationen werden schwierige Operationen gezielt vorbereitet.

Nahezu alle Krankenhäuser und viele Arztpraxen sind mit EDV-Systemen ausgestattet und nutzen diese vor allem zur Rationalisierung der Verwaltung. Medizinische Expertensysteme werden in wenigen Arztpraxen, in einigen Krankenhäusern und in fast allen Forschungseinrichtungen genutzt. Integrierte Krankenhausinformationssysteme, die Patientendaten, Krankheitsgeschichten und Expertensysteme zur Entscheidungsunterstützung nutzen, befinden sich im Aufbau. Die Anwendung computergestützter Hilfsmittel schreitet in allen medizinischen Fachgebieten voran. In der Forschung werden für viele Krankheitsgruppen epidemiologische Datenbanken aufgebaut, um Krankheitsursachen und Entstehungszusammenhänge von Krankheitsbildern besser erforschen zu können.

Der Sozialversicherungsausweis wird mit einem Speicherchip versehen sein, auf dem alle Versicherungs- und lebenswichtigen Gesundheitsdaten gespeichert sind. Er enthält außerdem Hinweise, wo weitere Diagnosedaten und die gesamte Krankheitsgeschichte abgerufen werden können. Die Krankenkassen versuchen, den steigenden Kostendruck vor allem dadurch aufzufangen, daß sie die Abrechnungsdaten zu Arzt- und Versichertenkonten zusammenfassen. Mit Hilfe von Durchschnittswerten kontrollieren sie das Abrechnungsverhalten der Ärzte wie auch die Leistungsforderungen der Versicherten und halten sie bei Überschreitung von Grenzwerten zu zweckmäßigem und wirtschaftlichem Verhalten an.

Um das Jahr *2020* wird die Medizintechnik mit Hilfe von Prozessoren Prothesen für Augen, Ohren und Muskeln anbieten, die die Funktionen dieser Organe eingeschränkt erfüllen können. Die Ärzte stützen sich in der Beratung und Behandlung zunehmend auf Expertensysteme, die in der medizinischen Forschung dialogartig, in der medizinischen Praxis jedoch hintergrundbegleitend und entscheidungskontrollierend arbeiten. Einige

Schadensersatzprozesse haben dazu geführt, daß Expertensysteme in solchen Fällen obligatorisch genutzt werden, in denen der Arzt wegen der hochkomplexen Materie nicht mehr allein die Verantwortung übernehmen möchte.

Integrierte Krankenhausinformationssysteme stellen Patientendaten für die Verwaltung zur Verfügung, führen gleichzeitig aber auch die telekommunikative Erstdiagnose durch und unterstützen den behandelnden Arzt oder das spezialisierte Expertensystem: Sie stellen die Daten eines Patienten und dessen Krankheitsgeschichte in jeweils geeigneter Form dar, beziehen aus medizinischen Wissenssystemen das erforderliche Faktenwissen, überprüfen die Medikamentierung auf Verträglichkeit, Nebenwirkungen und Allergien und kontrollieren den Therapieverlauf. Medizinische Datenbanken, die im Dialog mit dem Patienten Telediagnosen erstellen, werden wegen der hohen Komplexität des erforderlichen Fach- und Strukturwissens auch bis zum Jahr 2020 nicht verfügbar sein. Medienkonzerne bieten jedoch medizinische Beratung als Telematikdienste an und werben gezielt für bestimmte Medikamente.

Besonderer Wert wird auf die medizinische Prävention gelegt. Zum einen geben Krankenkassen und Gesundheitsbehörden Empfehlungen, etwa Arbeitsplätze gesundheitsverträglicher einzurichten und andere Gesundheitsgefährdungen zu reduzieren. Zum anderen wird auf der Basis der vollständigen Krankheitsgeschichten, weiteren Lebensdaten des Patienten und seiner Verwandten und Vorfahren sowie den Erkenntnissen aus epidemiologischen Krankheitsregistern versucht, individuelle Krankheitsrisiken jedes einzelnen Versicherten zu erkennen und für ihn einen speziellen Präventionskatalog zu erstellen. Dieser kann vom Verbot, an bestimmten belastenden Arbeitsplätzen zu arbeiten, bis hin zum 'Gebot' spezieller Verhaltensweisen in der Privatsphäre reichen. Wer gegen den individuellen Präventionskatalog grob und bewußt verstößt, verliert ganz oder teilweise seinen Versicherungsschutz.

Verkehr

Trotz der Möglichkeiten von Videokonferenzen für die geschäftliche Kommunikation, elektronischer Heimarbeit und vieler Teletransaktionen wird der Straßenverkehr bis zum Jahr *2000* weiter zunehmen. Dies liegt zum einen daran, daß die elektronischen Substitute noch nicht breitflächig genutzt werden, zum anderen aber auch an den unattraktiven Nahverkehrssystemen, an dem im Gegensatz zu diesen weiter ausgebauten dichten Straßen- und Autobahnnetz und an dem steigenden Bedürfnis, in der Freizeit in Naturschutzgebiete und Erholungsparks auszuweichen. Schließlich wirkt auch noch immer das von dem Auto vermittelte Gefühl der Unabhängigkeit verhaltensbestimmend.

An Knotenpunkten wird die Masse des Verkehrs nur noch durch interaktive Verkehrsleitsysteme gesteuert werden können. Diese erfassen über Sensoren die Verkehrsdichte an allen Hauptverkehrswegen und zeigen auf Anzeigetafeln die optimalen Umleitungen an. Nahezu alle Neuwagen werden mit Bordcomputern ausgestattet sein, die über den

Zustand des Fahrzeugs, notwendige Wartungen und Reparaturen und über Fehlverhalten des Fahrers informieren. Manche Fahrzeuge sind mit Planungssystemen ausgerüstet, die nach den Wünschen des Fahrers bezüglich Reiseziel, Geschwindigkeit, Höchstdauer der Reise usw. Fahrtrouten vorschlagen. Aktuelle Verkehrsflußdaten empfangen sie über Funk. An unfallträchtigen Stellen werden Erfassungssysteme die Kennzeichen von Verkehrssündern, die Ampeln mißachten oder die Geschwindigkeitsgrenzen überschreiten, automatisch registrieren und den Versand von elektronisch erstellten Bußgeldbescheiden veranlassen.

Auch zur Ausrüstung von Schiffen, Flugzeugen und Eisenbahnen gehört verstärkt IuK-Technik. Ihre Verläßlichkeit, Sicherheit und Energieeffizienz wird hierdurch erheblich gesteigert. Technisch wäre es grundsätzlich schon möglich, sie vollautomatisch fahren zu lassen. Wegen der nicht auszuschließenden Störung durch Umwelteinflüsse werden jedoch auf der Brücke, im Cockpit und im Leitstand Spezialisten zur Verfügung stehen, die in Ausnahmefällen eingreifen können.

Der Flugverkehr wird in der Bundesrepublik bis zum Jahr 2000 verdoppelt werden. Da bereits heute die Kapazität der Flughäfen ausgeschöpft ist und der Bau neuer Flughäfen am Widerstand der lärmgeplagten Bevölkerung scheitert, wird der einzige Ausweg in einer durch IuK-Technik ermöglichten dichteren Abfolge von Starts und Landungen gesehen. Der Bahnverkehr mit Hochgeschwindigkeitszügen auf den Hauptstrecken und mit zeitkritischen Gütertransporten im Rahmen der neuen Logistikkonzepte in der Produktion (Just-in-Time) nimmt zu, während der Verkehr auf den Nebenstrecken weiter ausgedünnt wird. Sowohl der Einsatz von Flugzeugen und Zügen als auch der Verkehrsfluß von Gütern und Personen werden über integrierte Computernetze gesteuert.

Um das Jahr *2020* wird der Verkehr wieder leicht abgenommen haben. Dies ist vor allem auf den Bevölkerungsrückgang, die gesellschaftliche Altersstruktur und steigende Energiepreise zurückzuführen. Eher ambivalent wirkt sich hingegen die Telearbeit aus. Einerseits reduziert sie tatsächlich das Verkehrsaufkommen zwischen Wohnung und Arbeitsplatz. Andererseits betrifft die Abnahme vor allem den öffentlichen Nahverkehr, der deshalb noch weiter ausgedünnt wird. Der Verkehr zur Versorgung der verstreut liegenden Arbeitsplätze nimmt jedoch ebenso zu wie der kompensierende Individualverkehr zum Einkaufen, für Besuche oder Ausflüge.

Die Fortschritte der Mustererkennung werden es ermöglichen,Fahrzeuge mit Selbststeuerungen anzubieten. Diese erlauben dem Fahrer, die Steuerung auf besonders gekennzeichneten (geradlinigen und unkomplizierten) Strecken dem Bordcomputer zu überlassen. Er selbst kann sich während dieser Zeit bequem zurücklehnen und beispielsweise (elektronische) Zeitung lesen. Nur von Zeit zu Zeit wird er vom Bordcomputer mit freundlicher Stimme aufgefordert, das Steuer zu übernehmen, weil er nun den besonders gekennzeichneten Bereich verläßt. Überall selbststeuernde Fahrzeuge werden aufgrund der verbleibenden Schwierigkeiten bei der Musterverarbeitung allerdings noch lange auf sich warten lassen.

U-Bahnen, Spurbusse und Züge werden in der Regel vollautomatisch gesteuert. Bahn- und Flugverkehr konkurrieren in den mittleren Entfernungen weiterhin miteinander. Zwischen den europäischen Großstädten verkehren Hochgeschwindigkeitszüge, die wegen ihrer Schnelligkeit automatisch gesteuert werden müssen. Die Kapazitäten im Luftverkehr werden durch höhere Geschwindigkeiten, gesamteuropäische Koordination der Flugbewegungen und radargesteuerten automatischen Landeanflug weiter erhöht.

Nahrungsmittelproduktion

Der Konkurrenzdruck ausländischer Nahrungsmittelproduzenten nimmt bis zum Jahr 2000 weiter zu. Für eine wirtschaftliche Betriebsführung ist eine immer größere landwirtschaftliche Fläche notwendig. Daher halten auch das 'Bauernsterben' und der Konzentrationsprozeß in der Landwirtschaft an. Die Produktivität der Nahrungsmittelerzeugung kann aus ökologischen Gründen nur noch sehr begrenzt durch chemische Produkte und größere Landmaschinen gesteigert werden. Nur für wenige Landwirte besteht ein Markt für teure Produkte aus dem arbeitsintensiven ökologischen Landbau. Die Mehrzahl versucht, ihre Erträge zu steigern, indem sie biotechnologisch optimierte Pflanzen und Produkte einsetzt und Arbeitskräfte, Maschinen, Saatgut, Dünge- und Pflanzenschutzmittel mit Hilfe IuK-gesteuerter Informationsverarbeitung effizienter nutzt.

Im computerunterstützten integrierten Pflanzenbau (CIPP) werden Menschen zunehmend durch Meß- und Regelungssysteme, Simulations- und Expertensysteme sowie Automaten unterstützt und, wo möglich, auch ersetzt. Über die mobile Auswertung von Bodenproben, Flugzeug- oder Satellitenaufnahmen wird für das einzelne Feld aus dem Chlorophyllgehalt in den Pflanzen der Bedarf an Stickstoffdüngung errechnet. Der Bordcomputer des Traktors dosiert exakt die Mengenverteilung. Ebenso steuert der Hofrechner die Dosierung der Pflanzenschutzmittel nach den über Btx abrufbaren Angaben zentral geführter Schädlingswarndienste. Der Einsatz von Menschen und Maschinen erfolgt unter Auswertung von Wetterprognosen, die durch Simulationen auf Supercomputern erheblich leistungsfähiger geworden sind. Luftverschmutzung, Wasser- und Bodenverseuchung führen dazu, daß immer größere Teile der Pflanzenproduktion, insbesondere im Gemüse- und Obstbau, nach holländischem Beispiel 'vollverkapselt' stattfinden und die geschlossenen Versorgungs- und Entsorgungs'kreisläufe'von Computern gesteuert werden. In der computerintegrierten Viehzucht wird über Simulationsmodelle einzeltierbezogen die optimale Fütterung veranlaßt und in Abhängigkeit von den aktuellen Marktpreisen der Verkaufs- und Schlachttermin bestimmt.

Zwar verbessern im Gegensatz zu anderen Weltregionen bis zum Jahr *2020* die Klimaverschiebungen durch die CO_2-Aufheizung der Atmosphäre die Produktionsbedingungen deutscher Landwirte. Dennoch werden wegen des Bevölkerungsrückgangs ihre Wettbewerbschancen nicht besser. Durch erste Landeinbußen haben an der norddeutschen Küste viele Landwirte ihren Hof verloren. Um weitere Produktionssteigerungen zu

ermöglichen, werden die integrierten Planungs- und Steuerungssysteme noch stärker genutzt - bis hin zum Einsatz von Robotern: In hochspezialisierten Plantagen werden Automaten den gesamten Produktionsprozeß vom Einpflanzen über die Ernte bis zum Verpacken und Abtransport ausführen und überwachen. Speziell hierfür vorbereitete Felder werden fahrerlos bearbeitet. Auch in der Viehzucht kommt IuK-Technik zum Einsatz: Die Tiere werden automtisch gefüttert, gemolken und geschlachtet.

Umweltschutz und Ressourceneinsparung

Fossile Energieträger und viele andere Ressourcen werden zunehmend knapp und teuer. Die negativen Auswirkungen von Produktion und Konsum für die Umwelt steigen an. Das öffentliche Bewußtsein um Umweltrisiken und die Gefahren fossiler und atomarer Energieversorgung wird stärker. Energieeinsparung wird als der einzig sinnvolle Weg erkannt, der drohenden Klimakatastrophe zu entgehen. Der gesellschaftliche Druck zur Nutzung regenerativer Energieträger, zu Einsparungen von Ressourcen und Energie sowie zur Begrenzung von Emissionen läßt eine neue hochtechnologische Industrie- und Dienstleistungssparte entstehen. Durch abgestimmte staatliche Umweltnormen wird in diesem Sektor ein großer Markt für Meß- und Steuerungstechnik geschaffen.

Fortschritte in der Mikroelektronik verbessern bereits bis zum Jahr *2000* den Wirkungsgrad und die Wirtschaftlichkeit von Solaranlagen. Sie tragen dazu bei, daß sich energiesparende Produktversionen - vom Auto über Waschmaschinen bis hin zu Elektroloks - leichter auf dem Markt durchsetzen. Der Energieverbrauch der IuK-Technik selbst ist relativ gering und ließe sich in vielen Fällen durch Sonnenenergie decken. Ihre Nutzung ermöglicht zugleich, die Kraft-Wärme-Kopplung so zu verbessern, daß in vielen Bereichen der Energieerzeugung Abwärme auch zur Stromproduktion genutzt werden könnte. Bis zum Jahr 2000 werden aber die Energieversorgungsunternehmen noch in der Lage sein, ihre Gebietsmonopole und die bisherige Tarifstruktur weitgehend zu verteidigen, so daß die private Erzeugung von Strom und dessen Einspeisung ins Netz meist unwirtschaftlich bleiben wird. Eher wird der Preisdruck mit Hilfe 'intelligenter' Steuerungen zu rationeller Energienutzung in der Produktion oder im Transport führen.

IuK-Technik verbessert die Erfassung von Umweltfaktoren. 'Intelligente' Sensoren ermitteln mehr und genauere Umweltdaten, übermitteln aber nur die als relevant programmierten aggregierten Daten. Emissionswerte aus Schornsteinen oder Abwasserkanälen werden per Funk zeitgleich übertragen. Zur Erfassung der Immissionsbelastung wird mit dem Aufbau breiter Umweltinformationssysteme begonnen. Für radioaktive Strahlung und einige Luftschadstoffe wurde bereits ein flächendeckendes Fernüberwachungssystem installiert. Die schadstoffemittierenden Betriebe nutzen die Fortschritte der Meßtechnik allerdings auch - um die Grenzwerte kostenoptimal auszunutzen.

Bis zum Jahr *2020* werden der Anstieg der Energiepreise und der Druck der ökologischen Probleme eine gewisse Dezentralisierung der Energieversorgung und eine Verän-

derung der Tarifstrukturen unterstützen, die Energieeinsparungen stärker fördert. Die Steuerung der dezentralen Energieversorgungssysteme, der vielen kleinen Energiequellen und die Optimierung der Energieverteilung erfolgt mit Hilfe von Großrechnern und vernetzten dezentralen Computern.

Komplexe Umweltkontrollsysteme registrieren über viele Sensoren und Satelliten permanent die Schadstoffbelastung von Luft, Wasser und Boden, geben Alarm, wenn Grenzwerte überschritten werden, leiten Gegenmaßnahmen ein und erteilen Verhaltensempfehlungen an die Bevölkerung. Die registrierten Daten werden zusammen mit anderen umweltrelevanten Informationen in Umweltdatenbanken gespeichert und ausgewertet. Mit Simulationen an komplexen Modellen der ökologischen Kreisläufe wird versucht, die Folgen bestimmter Schadstoffbelastungen oder des Einsatzes neuer chemischer oder gentechnischer Produkte abzuschätzen. Simulationssysteme dienen als theoretisches 'Labor' für Versuche, die real zu riskant wären.

IuK-Technik ermöglicht Fortschritte im Umweltschutz. Durch die Kommerzialisierung von Information und Kommunikation kann sich wirtschaftliches Wachstum unabhängig vom Verbrauch materieller Ressourcen entwickeln. Durch IuK-Technik kann auch der Energieverbrauch und die Umweltbelastung anderer Techniken reduziert werden. Gleichzeitig aber verursacht die Herstellung von IuK-Produkten selbst Umweltbelastungen. Insbesondere in der Chip-Produktion fallen hochgiftige Substanzen an. In der Bilanz dürften IuK-Techniken im Umweltschutz gewisse Verbesserungen ermöglichen. Allein mit ihrem Einsatz können die ökologischen Krisen jedoch nicht bewältigt werden. Insbesondere verändern sie nicht die grundsätzlichen Konflikte zwischen privatwirtschaftlichen und ökologischen Interessen. Die IuK-Techniken werden daher vor allem eine Schlüsselrolle im Krisenmanagement der superindustrialisierten 'Risikogesellschaft' spielen.

6. Integration im Alltag

Die künftigen Anwendungsfelder der IuK-Technik wurden bisher jeweils nur für sich dargestellt. Die verschiedenen Anwendungsformen wirken jedoch zusammen, bedingen sich teilweise gegenseitig und beeinflussen in ihrer Gesamtheit das Leben der Gesellschaft und des einzelnen in stärkerem Maße, als dies durch eine auf ein Anwendungsfeld beschränkte Betrachtung sichtbar wird. Um diese Integration der IuK-Technik in das gesellschaftliche Leben deutlich zu machen, werden im folgenden quasi quer zu den beschriebenen Anwendungsfeldern exemplarisch die IuK-Anwendungen im Arbeitsleben und im privaten Alltag aus der Sicht des einzelnen dargestellt.

Arbeitsleben

Die *Fabrik* um das Jahr *2000* wird weitgehend automatisiert und von Robotern und NC-Maschinen geprägt sein. Aufgrund des günstigen Preis-Leistungsverhältnisses hat die Automatisierung Eingang in mittlere und kleinere Produktionsbetriebe gefunden. Die technisch-wirtschaftlichen Vorteile flexibler automatisierter Fabriken lassen herkömmlich ausgerüsteten Wettbewerbern kaum eine Marktchance. Arbeitsbelastungen durch körperlich schwere, gefährliche, ungesunde und monotone Arbeit werden abnehmen. Die Aufgaben der verbleibenden Beschäftigten liegen vorwiegend in der Überwachung und Kontrolle und verursachen vor allem seelisch-nervliche Belastungen. Doch selbst dort werden zunehmend Expertensysteme zu Fehlersuche, -diagnose und -beseitigung eingesetzt. Körperliche Arbeit ist nur noch in relativ wenigen Bereichen erforderlich, für die eine Automatisierung zu teuer oder technisch nicht möglich ist.

Durch die Automatisierung sind die Aufgaben der Konstruktion, der Produktionsplanung und der Produktionsüberwachung weiter angestiegen. Aber auch sie werden schon weitgehend mit Hilfe von IuK-Techniken ausgeführt. Zumindest die Konstruktions- und Administrationsroutinen erledigen Maschinen. So fallen vor allem Tätigkeiten der unteren und mittleren Qualifikationsstufen weg wie Schreibarbeiten, Sekretariate und bestimmte Sachbearbeitungen. Die verbleibenden Arbeiten erledigen der Konstrukteur und der Sachbearbeiter im technischen Büro am Bildschirm.

Die durchschnittliche Wochenarbeitszeit beträgt 35 Stunden. Die Reduzierung der Arbeitszeit mußte allerdings durch ihre Flexibilisierung erkauft werden. Diese ermöglicht eine verbesserte Auslastung der Anlagen und Maschinen. Schicht-, Nacht-, Wochenend- und Feiertagsarbeit sowie Formen der variablen Arbeitszeit, des Job-sharing und der Ruf- und Arbeitsbereitschaft haben zugenommen. Während der Bereitschaftsdienste können sich die Arbeitnehmer zwar in vielen Fällen außerhalb des Betriebs oder zu Hause aufhalten. Sie müssen jedoch in der Lage sein, jederzeit auf elektronischen Abruf hin sofort in den Betrieb zu kommen.

Bis zum Jahr *2020* sind aus den nur teilweise automatisierten Fabriken überwiegend automatische Produktionsstätten geworden. Erforderlich für die Produktion selbst ist nur noch eine relativ kleine Gruppe hochtrainierter Spezialisten. Sie überwachen die automatischen Prozesse und tragen die Verantwortung für die planmäßige Funktionsweise des komplexen technischen Systems. Sie werden von Expertensystemen unterstützt, die durch die permanente Auswertung der Maschinendaten Fehler oft schon vor dem Ausfall der Maschinen erkennen können. Bei Störungen müssen die Kontrolleure ihre Kenntnisse sofort einsetzen können, um die Produktionsunterbrechungen möglichst gering zu halten. Für diese Beschäftigten ist eine ständige Weiterbildung unumgänglich. Außer diesen hochspezialisierten Kontrolleuren sind in der Fabrik 2020 nur wenige 'Hilfsarbeiter' beschäftigt. Sie arbeiten in nicht automatisierbaren Bereichen den Maschinen zu. Für sie gibt es in der betrieblichen Hierarchie keine Aufstiegschancen. Da sie nur angelernt sind, haben sie auch keine Alternativen, falls sie den psychischen und physischen Bedingungen der weitgehend monotonen Arbeit nicht mehr gewachsen sind.

Die Durchschnittsarbeitszeit beträgt nur noch 30 Stunden. Die flexiblen Arbeitszeitformen haben erneut zugenommen. Die permanente Anwesenheit im Betrieb ist allerdings für viele Überwachungs- und Kontrollaufgaben, aber auch für viele Tätigkeiten in der Konstruktion und der Produktionsplanung nicht mehr notwendig. Sie lassen sich vielmehr vom heimischen Terminal aus erledigen. In einigen Fällen können die Beschäftigten sogar Fehler von zu Hause aus diagnostizieren und beseitigen. Nur soweit dies nicht gelingt, ist der Einsatz von Montagetrupps vor Ort notwendig.

Die Arbeit im *Büro* ist um das Jahr *2000* bereits stark durch IuK-Techniken geprägt. Äußeres Kennzeichen dieser Entwicklung ist der allgegenwärtige Bildschirm. Die Sachbearbeiter werden in ihrer Arbeit weitgehend durch Computerprogramme geführt und durch Textverarbeitung und Informationssysteme mit aufgabenbezogenen Zugriffsmöglichkeiten unterstützt. Teilweise werden Entscheidungskompetenzen auf den Computer übertragen. In vielen Bereichen erfolgt die Arbeit völlig 'papierlos'. Sprechschreiber, Scanner, elektronische Post, Datenfernübertragung und Sachbearbeiterprogramme werden die Büroarbeit erheblich verringern. Betroffen sind z.B. Assistenztätigkeiten, Archiv, Kasse, Buchhaltung, Revision, Beratung, Berichterstellung, Personal- und Bestellwesen, Schreibarbeiten, Datenerfassung und -aufbereitung, Lagerverwaltung. Von dem verbleibenden Rest ist ein - noch nicht sehr großer - Teil als Telearbeit in Nachbarschaftsbüros oder in die Wohnungen von Beschäftigten ausgelagert.

Auch im Verwaltungsbereich ist die Verkürzung der Arbeitszeit mit ihrer Flexibilisierung verbunden. Durch Teilzeitarbeit, Gleitzeit, Job-sharing und variable Arbeitszeit versuchen die Arbeitgeber, Produktivitätssteigerungen zu erzielen. In einigen Bürobereichen ist es möglich, einen Vollzeitarbeitsplatz mit mehreren Teilzeitarbeitskräften zu besetzen, die jeweils ausgeruht die Arbeit für kurze Zeit ausführen und deshalb zu gesteigerten Leistungen in der Lage sind. Spitzenbelastungen werden durch abrufbereite Mitarbeiter mit variabler Arbeitszeit aufgefangen. Durch diese Arbeitszeitformen schrumpft die be-

triebliche Stammbelegschaft und wird durch Arbeitskräfte mit Teilzeit- oder befristeten Arbeitsverträgen ergänzt.

Bis zum Jahr *2020* setzt sich der Trend zur Telearbeit fort. Diese Form der Tätigkeit wird für die Unternehmer zunehmend attraktiv, weil die Geräte- sowie die Anschluß- und Übertragungskosten relativ niedrig sind, die Einrichtung eines Arbeitsplatzes in der Zentrale aber relativ teuer ist. Neben der 'einfachen' Sachbearbeitung wird auch hochqualifizierte Verwaltungsarbeit in Form von Telearbeit erbracht. Die Kommunikation zwischen den dezentralen Telearbeitsplätzen und der Zentrale erfolgt papierlos.

Im Büro selbst hat die Formalisierung der Tätigkeiten weiter zugenommen. Auch der Umfang der Aufgaben, die der einzelne Beschäftigte zu erledigen hat, ist angewachsen. Für die Aufgabenverteilung gilt eher das Prinzip der Integration als das des Taylorismus. Die Sachbearbeiter werden interaktiv durch Expertensysteme geführt. Ihre Fälle bearbeiten sie mittels individuell angepaßter Sprechschreiber. Spezielle Schreibdienste gibt es nicht mehr. Durch die Nutzung der IuK-Technik entstehen auch neue Berufe, so der Datenbankrechercheur, der Dokumentator oder der Kommunikationsberater, die jedoch nur von wenigen ergriffen werden können.

In allen Bereichen des Arbeitslebens werden die in IuK-Systemen anfallenden Informationen auch zur Personaladministration, kontrolle und -planung in umfassenden *Personalinformationssystemen* verarbeitet und ausgewertet. Über die Betriebsdatenerfassung werden die Arbeitsleistungen und -fehler einzelner Beschäftigter, Gruppen, Abteilungen und Betriebsteile erfaßt und verglichen. Profilabgleiche zwischen Arbeitsplatzerfordernissen und den Leistungsmerkmalen des Beschäftigten erlauben, an den einzelnen Arbeitsplätzen immer den jeweils Leistungsfähigsten einzusetzen. Innerhalb der Betriebe dient eine Chipkarte als Stempelkarte, als Zugangsschlüssel und als Bargeld. Zeiterfassung, Anwesenheits- und Zugangskontrollen sowie die Kommunikationsdatenerfassung sind ebenfalls in das Personalinformationssystem integriert. 'Persönliche Kalender' repräsentieren für die Personalabteilung das komplette bisherige Arbeitsleben des Beschäftigten. Dessen individuelle und zu Statistiken aggregierte Daten werden von Expertensystemen für die Prognose und Steuerung des Personalbedarfs und der Personalbewegungen ausgewertet.

Zur Verwaltung der bis zum Jahr *2000* hohen Arbeitslosenquote und der strukturellen Arbeitsmarktunterschiede setzt auch die *Arbeitsverwaltung und -vermittlung* IuK-Techniken ein. Die Arbeitsvermittlung erfolgt unter Einsatz von on-line-Systemen, die sowohl Arbeitsstellen als auch Arbeitssuchende nachweisen. Die notwendigen Informationen werden von Arbeitgebern und Arbeitslosen mit Fragebögen erhoben und über Lesegeräte unmittelbar in das System eingegeben. Auch die direkte Eingabe über Btx ist möglich. In Standardfällen erfolgt die Vermittlung automatisiert. Das Vermittlungssystem gleicht automatisch die Qualifikationen der Arbeitssuchenden und die Anforderungen der Arbeitsplätze ab und verschickt an die 'passenden' Bewerber Aufforderungen, sich vorzustellen. Offene Stellen werden außerdem über Btx angeboten. Diese Seiten können von

zu Hause oder von in den Arbeitsämtern aufgestellten Terminals kostenlos abgerufen werden. Die Einschaltung von Sachbearbeitern in die Arbeitsvermittlung ist nur noch notwendig, wenn Sonderqualifikationen gesucht oder angeboten werden. Darüber hinaus stehen sie für Beratungen zur Verfügung.

Auch für die immer wichtigere berufliche Weiterbildung stehen im Bereich der Arbeitsverwaltung ausgebaute Beratungs- und Schulungssysteme zur Verfügung. Sie werden von Sachbearbeitern benutzt, um Berufsanfängern, Langzeitarbeitslosen und Umschülern - orientiert an den jeweiligen Qualifikationsanforderungen und Bewerberfähigkeiten - Hinweise zu Aus- und Weiterbildungsmöglichkeiten zu geben.

Diese Entwicklungslinie wird sich bis zum Jahr *2020* trotz der durch den Bevölkerungsrückgang entspannteren Situation am Arbeitsmarkt weiter ausprägen. Mit der Verbreitung von Btx wird ein immer größerer Teil der Arbeitsverwaltung elektronisch ohne unmittelbaren Kontakt abgewickelt. Sowohl die Meldung der Arbeitslosigkeit als auch das Angebot offener Stellen werden telekommunikativ in das System eingegeben. Dieses weist automatisch die Unterstützungszahlungen an, vergleicht Anforderungs- und Qualifikationsprofile, vermittelt die offenen Stellen und unterstützt in Standardfällen auch die elektronischen Vertragsverhandlungen bzw. -abschlüsse. In Arbeitsämtern stehen für eine erste Vorstellung Videokonferenzstudios zur Verfügung. Die vollelektronische Arbeitsvermittlung ist eine wichtige Voraussetzung für das Funktionieren des Teilzeit-Arbeitsmarktes, der inzwischen ein beachtliches Volumen erreicht hat. Für die Vergabe von Arbeit wird die räumliche Entfernung weniger bedeutsam.

Alltagssituationen

Um zu zeigen, wie sehr oder wie wenig IuK-Technik den Alltag um das Jahr *2020* beeinflussen dürfte, werden fünf Alltagssituationen dargestellt. Sie sollen in ihrer Unterschiedlichkeit die zu erwartenden Diversifikationen in der Techniknutzung zum Ausdruck bringen. Jede Rolle kombiniert bestimmte Faktoren für die jeweilige Lebenssituation - wie Wohnverhältnisse, soziale Beziehungen, Arbeitssituation, Freizeitgestaltung oder Kommunikationsmöglichkeiten. Selbstverständlich sind auch weitgehend andere als die gewählten Kombinationen möglich.

Hans Peter Stürle, Vertriebsingenieur

Herr Stürle ist Diplomingenieur im Maschinenbau und Angestellter eines mittleren Unternehmens der Investitionsgüterindustrie. Er betreut selbständig Projekte und begleitet diese von der Ausschreibung über die Spezifikation, Konstruktion, Fertigung und Anpassung bis hin zur Inbetriebnahme und Wartung. Zu seinen Aufgaben gehört auch die Marktbeobachtung. Veränderte Anforderungen werden in Absprache mit Marketing und

Produktentwurf analysiert und umgesetzt. In seiner Arbeitseinteilung ist er frei. Er muß lediglich sicherstellen, daß er für das Unternehmen und die Kunden jederzeit leicht erreichbar ist. Mit Hilfe des IBFN-Anschlusses im Unternehmen und zu Hause, die er über Rufweitergabe koppeln kann, sowie des Funktelefons ist dies keine Schwierigkeit. Zudem bietet ihm der IBFN-Anschluß einen leistungsfähigen Zugang zu den Datenbanken und Expertensystemen seines Unternehmens, so daß er einen Großteil seiner Aufgaben auch zu Hause erledigen kann. Das spart mehrere Fahrten pro Woche.

Die Bezahlung ist sehr gut. Die Arbeit macht Herrn Stürle Spaß. So belasten ihn auch einige Überstunden kaum, wenn ein Termin drängt. Lediglich die Rufbereitschaft und die gelegentlichen Anforderungen am Abend und am Wochenende sind lästig, weil sie immer dann erfolgen, wenn er gerade mit Freunden seine Freizeit so richtig genießen will. In der Regel arbeitet er knapp über 40 Stunden pro Woche - für seinen Tätigkeitsbereich ist er der einzige Spezialist im Unternehmen. Da er etwas außerhalb der Stadt wohnt und dienstlich - trotz IBFN und Videokonferenzen - oft unterwegs ist, fährt er einen sportlichen Wagen der gehobenen Mittelklasse. Das eingebaute Verkehrsinformationssystem unterstützt ihn bei der Streckenplanung und leitet ihn um Staus herum. Die Sonderausstattung mit Autopilot und Abstandsradar für Autobahnen hat die Firma finanziert. So kann er Fahrtzeiten effizienter nutzen.

Hans Peter Stürle hat seinen Haushalt gemäß seinen technischen Neigungen gut durchorganisiert. Besonders stolz ist er darauf, daß die Küchenarbeit von der automatischen Küchenzeile fast restlos erledigt wird. Die war zwar nicht billig, spart ihm aber auf Dauer viel Zeit. Das Kochexpertensystem klärt mit ihm auf der Grundlage der Tiefkühltruhenverwaltung die Speisenfolge und gibt ihm Anweisungen, welche Zutaten notwendig sind. Das Anrichten der Speisen erfolgt dann weitgehend automatisch. Besonders bequem findet es Herr Stürle, daß er die Küchengeräte - oder auch seine Sauna - über den Fernwirkdienst bereits vom Büro- oder Autotelefon aus anstellen kann. Einmal pro Woche werden Tiefkühlprodukte angeliefert. Lediglich frische Lebensmittel muß er 'um die Ecke' einkaufen. Wenn er exklusiv essen möchte, sucht er ein Spezialitätenrestaurant auf.

Herr Stürle lebt allein - für eine Familie wäre auch nicht viel Zeit. Schließlich steht er unter einem hohen Anspruch: immer den Stand der Technik zu kennen. Abends wählt er sich deshalb häufig ein telekommunikatives interaktives Fortbildungsprogramm. Sein Unternehmen honoriert die hohe Weiterbildungsbereitschaft, indem er zweimal im Jahr zur Teilnahme an Verkaufsleiterkursen in naturnahen attraktiven Schulungszentren freigestellt wird.

Neben einem Beziehungstraining, an dem er regelmäßig teilnimmt, ist es ihm wichtig, Freunde zu sehen. So wählt er mit seinem Bildtelefon abends den einen oder anderen Bekannten an oder hält Kontakt zu seiner Mutter. Eine große, vierwöchige Auslandsreise vermittelt ihm jedes Jahr Einblick in eine fremde Kultur und bietet Erholung vom beruflichen Alltag.

Klaus Müller, Student

Protokoll Beziehungsberatung
- WG Beckstr. 47 -

Zusammensetzung:
- Klaus Müller, 23 J., Archäologiestudent
- Peter Schmidt, 27 J., Student der Erziehungswissenschaften und der Psychologie
- Walter Bärmann, 22 J., Maschinenbaustudent
- Lothar Peters, 22 J., Architekturstudent, z.Z. Zivildienstleistender.

Ausgangssituation der Beratung: Initiative und Anfrage von P. Schmidt mit Zustimmung der WG-Mitglieder. Konfliktauslöser ist die Rechnernutzung für Studium und Alltag und die entstandene Kommunikationsarmut ...

Lebenssituation von K. Müller: Seit 2 1/2 Jahren Student, vor einem Jahr Wechsel von Architektur zu Archäologie. Studiert aus Interesse, ohne konkrete Perspektive. Der Arbeitsmarkt für Archäologen ist sehr begrenzt. Trägt mit zu seiner Orientierungslosigkeit bei. Jobbt als Verteilfahrer einer Teleshopping-Kette dreimal wöchentlich. Existenzsicherung durch staatlichen Studentenkredit. Freizeitinteressen: Kneipen, Selbsterfahrungsgruppe, Kontakt zu Archäologen in Italien (Praktikumsfreundschaft) über Mailbox, Italienischkurs, Italienurlaub.

Studiensituation: Wechselt ins dritte Semester, hat Spaß und will an Ausgrabungsexkursionen teilnehmen. Das Faktenstudium will er möglichst schnell absolvieren. Die dauernden Datenbankabfragen ist er leid. Daher versucht er, den Prüfungsstoff vor allem mit interaktiven Lernprogrammen zu erarbeiten.

Rolle in der WG: Hauptmieter der Wohnung, Eltern bürgen.

Selbsteinschätzung: faires Verhalten zu anderen, allerdings unterschiedlich gute Kontakte, stark studienorientiert. Eher Freunde außerhalb, wenig Zeit für das WG-Leben, zum Teil wegen Job.

Fremdeinschätzung: macht das Nötigste, nicht oft zu sprechen, weil weg oder vor dem Terminal. Stellt den PC und den ISDN-Anschluß auch den anderen zur Verfügung. ...

Vermutung: Studienentscheidung unsicher, Konflikt zu Lothar (studiert Architektur weiter), Psychische Belastung wegen Schulden und schlechter Berufsaussicht, unpersönliche Beziehung innerhalb der WG, deshalb Orientierung nach außen. ...

Konfliktauslöser: Um für sein Archäologiestudium zur Fernuniversität wechseln zu können, hat Klaus ein 'Volksterminal' mit ISDN-Anschluß beantragt. Diese 'Technisierung' wurde zu Beginn von den anderen abgelehnt. Inzwischen hat sie aber eine eigentümliche Eigendynamik entwickelt. Das Terminal wird nicht nur von Klaus, sondern auch von Lothar und Walter für Studienzwecke genutzt. Außerdem werden die Rezeptberatung, der Umweltinfodienst und die alternative regionale Telezeitung in Anspruch genommen. Die

WG-Mitglieder nutzen überdies die Job-Angebote und die "Flohmarktnachrichten" im Btx. Neuerdings bestellen sie sogar Lebensmittel-Sonderangebote über Teleshopping. Und auch den zeitraubenden Weg zur Bank sparen sie sich inzwischen. Klaus wickelt einen großen Teil seines privaten und Behördenschriftverkehrs über den Computer ab. Streit entstand besonders ....

Michaela Koch, Rentnerin

R.T.: "Guten Tag Frau Koch, mein Name ist Renate Tabich. Wir befragen im Auftrag der Zentrumsleitung die Bewohner, um uns zu versichern, daß sie sich bei uns wohlfühlen. Wenn Sie Zeit haben, würde ich Sie jetzt gern interviewen."

M.K.: "Ja gern, kommen Sie doch rein. Ich finde es sehr gut, daß die Leitung sich um uns kümmert. ... Möchten Sie eine Tasse Kaffee?"

R.T.: Ja gern. ... Können Sie mir zunächst einige Angaben zu Ihrer Person machen?"

M.K.: "Nächste Woche feiere ich meinen 67. Geburtstag. ... Ich habe eine Witwenpension und eine kleine Zusatzversorgung aus früheren zeitvariablen und Halbtagstätigkeiten. Hier ins Zentrum Schönblick bin ich ein Jahr nach dem Tod meines Mannes gezogen, das ist jetzt 3 1/2 Jahre her. Er starb an einem Herzinfarkt während eines Allergieanfalls."

R.T.: "Das war sicher eine schwere Zeit für Sie?"

M.K.: "Am Anfang war es sehr schwer. Aber unsere Kinder haben mich betreut. Auf dem projizierten Bild sehen Sie sie. Wir haben uns oft gegenseitig besucht. Außerdem sehen wir uns oft über das Bildtelefon. Und dann habe ich ein altes Hobby weitergeführt: Ich batike mehrmals die Woche - in verschiedenen Techniken. ..."

R.T.: "Kommen wir nochmal zu unserem Interview. Was unternehmen Sie hier im Haus und außerhalb?"

M.K.: "Das Angebot hier ist ja so vielfältig - da muß ich mir einiges auswählen. Zur Gymnastik gehe ich einmal die Woche. Dann gibt es die Vortragsreihe, die wir im Multimediaraum anschauen, die mit den Filmen über fremde Länder, die von der städtischen Medienbibliothek überspielt werden. Manchmal nutze ich dort auch den elektronischen Berichtdienst 'Buntes aus aller Welt'. Ja, und mittwochs treffe ich mich mit fünf Mitbewohnerinnen zum Spielkreis. Ab und zu fahre ich auch bei den Tagesausflügen mit. Und im Mai bin ich jedes Jahr zwei Wochen im Karstgebirge der Oberpfalz. Dort kann man die Hotels noch bezahlen."

R.T.: "Sie sind ja sehr aktiv. Welche Rolle spielt für Sie der Multivisionsprojektor und sind Sie mit dem Angebot an Telekommunikationsdiensten zufrieden?"

M.K.: "Noch Kaffee? Naja, ich wähle mir öfter abends einen Film oder sehe mir Videos von der Familie an, die mein Mann noch gedreht hat. ... Das Bildtelefon - meine Kinder sagen oft, es sei besetzt. Es wäre schön, wenn Sie das verbessern könnten."

R.T.: "Ja, das haben schon mehrere Bewohner gesagt. Sind Sie denn sonst mit der Versorgung zufrieden?"

M.K.: "Doch ja! Viele Kleinigkeiten kann man ja hier im Zemtrumsladen kaufen und den Rest bekomme ich per Teleshopping. Kleider kaufe ich allerdings lieber in der Stadt. Mit dem Bus hinzufahren und sich was auszusuchen, ist abwechslungsreicher. Schön, daß man im Zentrumsladen unserer alten Gewohnheit gemäß noch mit Geld bezahlen kann. In der Stadt schauen sie einen verwundert an, wenn man statt der Chipkarte den Geldbeutel aus der Tasche holt. Viele nehmen gar kein Geld mehr. ... Da fällt mir noch ein - vielleicht könnten Sie noch einen Kommunikationsberater einstellen. Wir Alten kommen alle mit den telekommunikativen Kontakten zu Banken, Versicherungen und Behörden nicht so zurecht. Deshalb wenden wir uns alle an den Kommunikationsberater hier. Der ist aber so überlastet, daß man doch immer recht lange warten muß."

R.T. "Ich sehe, grundsätzlich sind Sie ganz zufrieden hier. Ich gehe jetzt zu Ihrer Nachbarin. Wenn Ihnen noch was einfällt - ich komme in den nächsten Wochen nochmal vorbei. Auf Wiedersehen - und danke für den Kaffee."

M.K.: "Auf Wiedersehen."

Christoph Bartel, Schüler

Christoph Bartel, S-Nr. 73-05 14. August 2020

Fachaufsatz: Wohnkultur und Kommunikation in der Familie

Aufgabe: In dem Fachaufsatz soll unter Zuhilfenahme des allgemeinen städtischen Informationssystems die eigene Familiensituation in Beziehung gesetzt werden zu den Ergebnissen der Bevölkerungsstatistik 2017 und der Studie "Familienstrukturen und Gesellschaftsentwicklung 2020".

1. Einige Untersuchungsergebnisse zur Familie

Nach der Bevölkerungsstatistik 2017* gibt es zur Zeit 1,1 Kinder je Haushalt oder 0,6 je erwachsenem Bundesbürger. 90% der Haushalte mit Kindern werden von den Gruppen Alleinerziehende, 1-Kind-Familie und 2-Kind-Familie gestellt. Sie werden als Kernhaushalte zusammengefaßt. Ihr Anteil an den Gesamthaushalten beträgt 64%. Kernhaushalte finden sich etwa zur Hälfte im weiteren Stadteinzugsbereich, und je ein Viertel im engeren Einzugsbereich und im Stadtkern.** Ca. 30 % der Kernhaushalte besitzen einen IBFN-Anschluß. Dabei steigt dieser Anteil, je weiter jemand von der Stadt entfernt wohnt. Die Bezugsgruppen für Kinder werden in ** mit sinkender Bedeutung aufgezählt: Haushaltsmitglieder, Schulbezugspersonen, Freunde.

2. Vergleich mit unserer Familie

Weil ich mit meiner Schwester und meinen Eltern zusammenwohne, sind wir ein Kernhaushalt. Wir wohnen im weiteren Einzugsbereich. Mein Vater fährt täglich zur Arbeit. Wir haben noch keinen IBFN-Anschluß. Er ist recht teuer und mein Vater sagt, daß ihm die Kabelprogramme ausreichen. Meine Mutter könnte ein Bildtelefon gebrauchen, um Anfragen nach Persönlichkeitsentwicklungsgruppen direkter zu beantworten und die psychologische Teleberatung gleich durchführen zu können. Sie ist sich aber unsicher, ob es ökonomisch wäre und betreut Kunden deshalb über Telemail, Telefon und Sprachspeicherung.

3. Kommunikation in der Familie

Mit meinen Eltern treffe ich mich immer beim Frühstück und beim Abendessen. Wenn ich an meinem eigenen Terminal Unterricht habe, bin ich den ganzen Tag zu Hause. Mein Vater ist dann oft im Büro. Meine Mutter sehe ich jedoch öfter. Sie macht Teleberatung und kocht. Außerdem sehen wir abends öfter Kabelfilme im Multivisionsprojektor. Wenn der Film uns Kindern nicht gefällt, schauen wir uns in unseren Zimmern ein anderes Programm oder Video-Clips an. Manchmal machen wir auch Telespiele oder versuchen, uns mit dem Terminal und einem Entwicklungsprogramm kleine elektronische Spielzeuge zu konstruieren.

An drei Tagen in der Woche fahre ich in die Schule. Wir arbeiten dort in unterschiedlichen Gruppen, mit einem pädagogischen Betreuer oder jeder für sich mit dem CAE-Programm (Computer Aided Education). Zwei Tage in der Woche lerne ich mit CAE zu Hause.

Ich bin in einem kleinen bundesweiten Oldtimer-Club. Wir sammeln Bilder, Filme oder Modellzeichnungen von Citroen-Modellen vor 1930. Die Bilder schicken wir uns über Telefax zu. Wenn wir einen IBFN-Anschluß hätten, könnten mir auch Filme direkt überspielt werden. Ab und zu machen wir Telekonferenzen, an denen ich ohne Bildkontakt teilnehme. TK-Dienste brauche ich auch, um diesen Aufsatz in die Schule zu übermitteln oder um Literatur dafür anzufordern. Manchmal benutzen wir auch einen öffentlichen Bildfernsprecher, um Verwandte zu sehen.

Literatur:

* Daten der Bevölkerungsstatistik 2017, Statistisches Bundesamt, Wiesbaden.
** Kyber/Netik: Familienstruktur und Gesellschaftsentwicklung 2020, Frankfurt.
(Recherchiert mit CAE-IR.)

Hildegard Härmann, Arbeitssuchende

Tagebuchnotizen

12.3.: Die Decke fällt mir auf den Kopf. Die Zwei-Zimmer-Wohnung ist zu klein für Carla und mich. Sie müßte ein richtiges Kinderzimmer haben. Aber eine größere Sozialwohnung ist nicht drin.

18.3.: ...Hoffentlich reicht die Sozialhilfe diesen Monat. .. Die Btx-Anzeige "Allgemeine Aushilfsdienste" hat in diesem Monat noch nichts gebracht.

22.3.: 3 Uhr morgens. Vom Baby-Sitten zurück. Carla schläft. Maiers kamen um 22 Uhr noch auf die Idee auszugehen und haben bei mir im Volksterminal angefragt. Gepaßt hat es mir nicht, aber ich brauche das Geld. Vielleicht klappt es dort öfter? Hoffentlich! Auf dem Rückweg dann noch in eine elektronische Ausweiskontrolle geraten. Die nehmen in letzter Zeit wieder zu.

25.3.: Die Selbsthilfegruppe hilft mir kaum - vielleicht der Sozialarbeiterin mit der ABM. Die Kasse wird nicht voller, die Wohnung nicht größer. Die anderen haben auch keine Perspektiven und wir bekommen nichts auf die Beine. Wir drehen uns alle im Kreis.

29.3.: Die Sonne scheint - heute ist ein erfolgreicher Tag: Zwei Wohnungsbetreuungen für die Urlaubszeit, eine sogar vier Wochen. Ich werde Carla vom Volksterminal loseisen und mit ihr im Park ein Eis essen. Feststimmung.

4.4.: Habe vorhin per Freieinheit im Lebensmittel-Infodienst geblättert. Tausende von Worten - aber alles unklar. Warum können sie nicht einfach schreiben, was man essen kann. Durch den Wissenschaftskram blickt keiner mehr durch. Immer diese Unsicherheit, was man bei der radioaktiven Verseuchung und der chemischen Vergiftung jeweils noch essen kann. Was wird mal aus Carla? Hoffentlich schafft sie die Schule gut.

7.4.: Arge Magenschmerzen. Aber die Lebensmittel müßten in Ordnung sein. Alles frisch. Es ist viel zu kalt hier. Die haben die ferngesteuerte Heizung wohl wieder nur nach dem Kalender programmiert.

8.4.: Patschnaß, aber zufrieden. Carla hat ne gute Note. Ich bin nach dem Blumengießen in einen Regenguß geraten. Der Magen ist wieder in Ordnung.

11.4.: Automatisches Vermittlungsangebot vom Arbeitsamtscomputer. Bei der Telebildvorstellung vom öffentlichen IBFN-Anschluß aus. Hat aber dem Chef wohl meine Nase nicht gefallen, oder daß ich eine Tochter hab. Schade. ... Der Magen ist nicht in Ordnung.

13.4.: Mein Magen spielt verrückt. Kann nicht zur Selbsthilfegruppe. Aber erstmal medizinische Teleberatung ... Die wollen einem immer nur Medikamente verkaufen. Ich glaub, ich gehe morgen zum Arzt, auch wenn ich einen Teil selbst zahlen muß.

14.4.: Der Arzt hat meine Sozialchipkarte in seinen Computer gesteckt. Meine Daten haben ihm nicht gefallen. Mir behagt es nicht, daß die Ärzte meine Untersuchungswerte immer in so ein Expertensystem eingeben. Das konnte diesmal auch nicht genau sagen, was es ist. Ich soll aber in der Apotheke Medikamente holen und morgen eine Folgediag-

nose anschließen. Ich weiß noch nicht, was es ist und bekomme Medikamente. Ich will meinen Körper nicht mit Chemie vollpumpen lassen. Aber die Schmerzen machen mich wahnsinnig.

15.4.: Die Schmerzen waren fast weg. Die zweite Folgediagnose heute vermutet mit 82% Wahrscheinlichkeit ein Magengeschwür. Psychosomatisch. Muß morgen mit Kontrastmittel in die Krankenhausdiagnose. Hoffentlich nichts Ernstes. Und was passiert mit Carla?

III. DIE VERLETZLICHKEIT DER 'INFORMATIONSGESELLSCHAFT'

7. IuK-technikspezifische Schadenstypen und Katastrophen

Am 6. Juli 1988 kamen bei einer Explosion auf der Nordsee-Bohrinsel "Piper Alpha" 166 Menschen ums Leben.[1] In Norwegen soll bis 1990 die erste völlig ferngesteuerte Bohrinsel fertiggestellt werden.[2] Menschenverluste wie auf "Piper Alpha" wird es dann nicht mehr geben.

Eine Unterschrift auf einem Scheck zu fälschen, bedarf eines Kugelschreibers und höchstens einer Stunde Übung. Die Decodierung einer elektronischen Unterschrift, mit dem Ziel diese zu fälschen, bedarf hingegen eines sehr schnellen Rechners für Tage oder Monate. Der Aufwand für einen Betrug wird dann erheblich größer.[3]

Von der Erhebung der Probe bis hin zur Bekanntgabe des Ergebnisses gab es in der manuellen Labormedizin lange Zeit eine Fehlerquote von rund 15%. Seitdem die Analysen überwiegend automatisch erstellt, ausgewertet, dokumentiert und übermittelt werden, konnte diese Fehlerrate auf 0,3% gesenkt werden.[4]

IuK-Technik kann Schadenspotentiale vermindern, Fehler vermeiden und Mißbrauch erschweren. Sie ist in vieler Hinsicht erheblich leistungsfähiger als der Mensch oder die konventionelle Technik. Sie vermag vielfach größere Mengen an Informationen in bedeutend kürzeren Zeiträumen zu verarbeiten und übermitteln. Im Jahr 2000 werden in einem wenige Millimeter großen Chip bis zu 64 Millionen bit (8 Millionen Buchstaben oder etwa 2000 Buchseiten) gespeichert werden. Glasfaserleitungen werden dann eine Übertragungsleistung von einer Milliarde bit/s (128 Millionen Buchstaben oder etwa 30 000 Buchseiten) erbringen.[5] Computer verarbeiten Informationen exakter, als Menschen dies können. Sie vergessen nicht, was sie einmal gespeichert haben, und kontrollieren die langweiligsten Vorgänge ohne jede Ermüdung. Routineaufgaben können daher durch IuK-Technik zuverlässiger erfüllt werden. IuK-Technik vermag so Verletzlichkeit zu reduzieren. Insoweit kann auf sie nicht verzichtet werden.

Wo aber Technik die Wirkungsmöglichkeiten des Menschen erhöht, steigert sie gleichzeitig die Möglichkeit von Schäden durch Fehler oder Mißbrauch dieser Technik. Wie dieses und die folgenden Kapitel zeigen werden, bietet die breite Anwendung der

---

1 S. hierzu z.B. Spiegel 28/1988, 164 ff.

2 S. FR v. 21.7.1988.

3 Dieses Beispiel nennt Goos GMD-Spiegel 3/4-1986, 31.

4 S. Vinsintin u.a. CM 9/1986, 23.

5 S. Informationstechnik 2000, Arbeitskreis Mikroelektronik 2.4; Goos GMD-Spiegel 3/4-1986, 30.

IuK-Technik nicht nur mehr Sicherheit, sondern schafft auch neue Risiken. IuK-Technik kann also beides: die Verletzlichkeit der Gesellschaft senken und sie erhöhen.

Wenn wir die Verletzlichkeit der 'Informationsgesellschaft',wie sie in dem vorangegangenen Zukunftsbild beschrieben wurde, untersuchen, geht es uns allerdings nicht um eine Variation des ewigen Abiturthemas: Technik - Fluch oder Segen? Wir zielen nicht auf eine allgemeine Saldierung der Vor- und Nachteile. Wir verstehen diese Technik nicht als ein unveränderliches Produkt, dessen Angebot uns zu einer 'Ja'- oder 'Nein'-Entscheidung zwingt. Es geht vielmehr um ihre Gestaltung, um den Versuch, ihre Vorteile zu nutzen und ihre Nachteile zu vermeiden.

Ob Nachteile hinsichtlich der Verletzlichkeit durch Gewinne an Komfort, Produktivität, Geschwindigkeit oder andere Vorteile der Techniknutzung ausgeglichen werden könnten, kann in einer Untersuchung zur Verletzlichkeit nicht abschließend beurteilt werden. Ebensowenig wollen wir andere Nachteile, die von einer breiten IuK-Techniknutzung erwartet werden - wie etwa mangelnde

soziale Beherrschbarkeit oder der Verlust an kultureller Vielfalt und sozialer Phantasie[6] an dieser Stelle bewerten. Denn: Ob wir die beschriebene Zukunft wollen sollen oder nicht, muß unter Berücksichtigung aller relevanten Kriterien entschieden werden. Welche Kriterien von Bedeutung sind, kann jedoch nur der demokratische Diskurs klären.[7] Die vorliegende Studie kann allerdings zu dieser Entscheidungsfindung einen wesentlichen Beitrag leisten. Sie beschreibt den Preis, der für den Weg in die 'Informationsgesellschaft' zu zahlen ist - und den sollte man bei jeder Reise kennen.

Wie verletzlich die 'Informationsgesellschaft' werden kann, hängt ab von der Größe potentieller Schäden und der Wahrscheinlichkeit ihres Eintretens. Während mögliche Fehler von IuK-Systemen und bewußte Schädigungen sowie zu erwartende Gegenmaßnahmen in den späteren Kapiteln diskutiert werden, untersucht dieses Kapitel, welche spezifischen Schäden und Katastrophen die IuK-Technik ermöglicht, und das anschließende Kapitel, welche Schäden möglich wären, wenn IuK-Systeme - aus welchem Grund auch immer - versagten. Das künftige Schadenspotential wird in diesen beiden Kapiteln als eigenständiger Risikobeitrag - unabhängig von der jeweiligen Wahrscheinlichkeit einer Schadensursache - betrachtet. Dieses Vorgehen rechtfertigt sich aus vier Gründen: Zum einen ändert sich die Wahrscheinlichkeit je nach Bedrohungssituation und Sicherungsniveau. Von daher ist es sinnvoll, unabhängig von deren ständigem Schwanken zu wissen, welche Schäden überhaupt möglich sind. Zum anderen ist das Maß notwendiger Sicherungsanstrengungen danach zu bestimmen, welche Schäden drohen, wenn die Sicherungen versagen. Drittens ist die Dringlichkeit von Maßnahmen zur Schadensbegrenzung und zur Reduzierung von Schadensfolgen vor allem abhängig von der Größe des möglichen Schadens. Und schließlich kann in vielen Fällen die Wahrscheinlichkeit

6 S. hierzu z.B. Kubicek 278 ff.; Mettler-Meibom 1987.

7 S. hierzu auch Alemann 1989.

eines Schadens nicht oder nur qualitativ bestimmt werden. Sein mögliches Ausmaß ist dann der einzige Anhaltspunkt zur Bewertung der Verletzlichkeit.

Für die künftige Verletzlichkeit der Gesellschaft ist vor allem die Frage von Bedeutung, ob die Informatisierung gegenüber heute zu anderen oder größeren Schäden führt. Um diese Frage beantworten zu können, müssen zunächst verschiedene Typen informationstechnisch induzierter Schäden bestimmt und in Beziehung zu Schadensmöglichkeiten der Gegenwart gesetzt werden. Mit diesem theoretischen Rüstzeug wird dann im folgenden Kapitel exemplarisch erörtert, wie sich infolge der gesellschaftlichen Abhängigkeit von dieser Technik das Schadenspotential in einigen Gesellschaftsbereichen entwickeln könnte.

Verlagerung und Reduzierung bekannter Schadensmöglichkeiten

In dem Maße, wie soziale Funktionen auf IuK-Systeme übertragen werden, können Schäden, die zuvor schon möglich waren, nun durch deren Mißbrauch verursacht werden. In diesem Fall wird das potentielle Schadensausmaß nicht beeinflußt: Nicht die Computernutzung erzeugt oder verändert Schadensmöglichkeiten, sondern die Tätigkeit, zu deren Steuerung oder Unterstützung IuK-Technik eingesetzt wird, bestimmt den Umfang möglicher Schäden.

Wenn zum Beispiel ein Bankangestellter per Computer das richtige Adresskonto einer Überweisung löscht und dafür seine Kontonummer einsetzt oder wenn ein Verwaltungssachbearbeiter für Kindergeldauszahlungen seinen Namen eingibt[8], dann sind die dadurch entstehenden Schäden die gleichen, wie sie durch Manipulation der traditionellen Buchhaltung entstanden wären.

Während der Reparatur eines Steuerungscomputers öffneten sich 1987 zwei Fluttore des Wasserkraftwerks von Alta im Norden Norwegens und eine drei Meter hohe Flutwelle ergoß sich in das Tal unterhalb des Staudamms.[9] Das Ausmaß des Schadens wäre das gleiche gewesen, wenn konventionelle Steuerungstechnik versagt hätte.

Es gibt also eine große Gruppe von Schadensmöglichkeiten, die sich durch IuK-Nutzung nicht verändern. Sie soll uns daher nicht weiter beschäftigen. Für sie liefert die Informatisierung keinen eigenen Schadensbeitrag. Sie ist für diesen Schadenstyp ausschließlich relevant für die Frage der Schadenswahrscheinlichkeit. Geschehen Betrügereien oder Überschwemmungen häufiger, weil Computer im Einsatz sind? Oder werden Schäden dadurch seltener? Für diesen Schadenstyp ist folglich die Frage zu stellen, wer zuverlässiger ist: Menschen, konventionelle Technik oder Computer. Erscheint es sinnvoller, einen Prozeß völlig, halb oder gar nicht zu automatisieren? Soll der Computer die Tätigkeiten von Menschen nur unterstützen, vorbereiten oder kontrollieren? Oder sollen ihm auch Entscheidungen übertragen werden? Antworten auf diese Fragen hängen ab von

8 S. hierzu z.B. die Fälle in Zimmerli KR 1987, 248, 265 und Sieber 1980, 47 ff.; ders. BB 1982, 1434; Sieg 316.

9 S. das in Oslo erscheinende Dagbladet v. 7.8.1987 - zit. nach Risk Digest Nr. 5.25 v. 7.8.1987, 2.

der Zuverlässigkeit und der Mißbrauchs-Sicherheit von IuK-Systemen und werden in den späteren Kapiteln behandelt.

Das Schadenspotential menschlicher Tätigkeiten kann durch IuK-Technik sogar geringer werden: Präzisere Prozeßsteuerung kann etwa eine Reduzierung des Energieeinsatzes ermöglichen. Die bei einem Unfall freigesetzte Energie wäre geringer. Eine Verteilung der Informationsverarbeitung kann dazu führen, daß durch ein Schadensereignis nur ein Teil der Informationen verloren geht. Durch Automatisierung werden viele Risikobereiche begrenzt oder beseitigt, in denen Menschen bisher tätig sein mußten. Beispiele hierfür könnten Bohrinseln, Bergwerke, Chemieanlagen, Fertigungsstätten oder atomtechnische Anlagen sein. Der Wegfall solch risikoreicher Arbeitsplätze ist ein hoher Gewinn, wenn die verbleibende Arbeit gerecht verteilt wird.

Allerdings ist zu fragen, wie zuverlässig und sicher die Automatik arbeitet und ob sie nicht neue Risiken schafft. Denn der Schadensreduzierung durch Schutz der bisher Beschäftigten könnte eine Risikosteigerung für die Allgemeinheit oder die Natur gegenüber stehen. So erhöht zum Beispiel der Einsatz von Robotern in strahlengefährdeten Bereichen das Risiko der Weiterverbreitung von atomwaffenfähigem Material. Denn die stark strahlenden Substanzen, die bisher dieses Material vor menschlichem Zugriff geschützt haben, können Robotern wenig anhaben. Oder ein anderes Beispiel: Der automatisierte Betrieb einer Chemieanlage wäre kein Gewinn, wenn dadurch die Wahrscheinlichkeit von Unfällen mit Freisetzungen von Giftstoffen anstiege.[10]

Die Nutzung der IuK-Technik kann also das potentielle Schadensausmaß bisheriger menschlicher Tätigkeiten unbeeinflußt lassen oder sogar verringern. Kann sie aber auch mögliche Schäden vergrößern? Wir wollen unsere Aufmerksamkeit nun den Typen von Schadensmöglichkeiten widmen, die durch den Einsatz von IuK-Technik verändert werden. Dabei betrachten wir nur die Schäden, die unmittelbar durch einen Fehler oder Mißbrauch von IuK-Systemen verursacht werden. Ihnen schließen sich meist Folgeschäden an, die dadurch entstehen, daß die soziale Funktion beeinträchtigt wird, die dem Technik-System übertragen wurde. Diese wollen wir jedoch nicht für die Bildung IuK-technikspezifischer Schadenstypen, sondern im Zusammenhang mit dem Katastrophenpotential der 'Informationsgesellschaft' berücksichtigen.

Neue Schadensverteilungen

IuK-Technik kann zu neuen Schadensverteilungen führen: Schäden, die bisher schon möglich waren, können sich zeit- und ortsunabhängig vielfach wiederholen. Dabei sind drei Typen zu unterscheiden:

Schäden können durch die IuK-Technik *kumuliert* auftreten (*Typ I: Kumulationsschaden*). Schäden werden vervielfacht, weil die neue Technik zu vielfachen, von einander

10 Methoden zur Schadensreduzierung als Sicherungsmaßnahme werden in Kapitel 9 und 12 erörtert.

unabhängigen Handlungen verleitet. Ein Beispiel sind die vielen Betrügereien an Geldausgabeautomaten, ein anderes das 'Hacken'.

So hat zum Beispiel die Cornell University in New York 1986 vor den vielen Hackern in ihrem Rechenzentrum kapituliert und ihre Verbindungen zu Computersystemen der wissenschaftlichen Welt gekappt.[11] Nimmt das 'Hackerwesen' zu, könnten 'Hackerschäden' an vielen Stellen gleichzeitig entstehen. Nachdem deutsche Hacker 136 Großrechner des SPAN-Netzes besucht und dort für sich 'Falltüren' eingebaut hatten, schätzen Fachleute allein den Aufwand zur 'Säuberung' jedes Rechners auf etwa 1 Mio. DM. Die Gesamtkosten dürften demnach etwa 140 Mio. DM betragen. Mögliche Schäden, die durch die Manipulation von Daten oder Programmen entstehen können, sind dabei noch nicht berücksichtigt. Hätten die Hacker spezifische kriminelle Absichten gehabt, hätte der Schaden um etliche Faktoren höher sein können.[12]

Noch stärker IuK-spezifisch ist der Schadenstyp, bei dem die Schadenshandlungen durch die Technik *multipliziert* werden (*Typ II: Multiplikationsschaden*): Das Risiko, von einem Expertensystem eine falsche Antwort zu bekommen, mag nicht größer sein als bei der persönlichen Befragung eines Experten. Der Schaden kann sich jedoch multiplizieren, wenn ein Expertensystem von vielen Anwendern gleichzeitig genutzt wird.

Einen ähnlich schadensverstärkenden Effekt hatte ein defekter Computer der amerikanischen Bundesverwaltung, der 1977 mehr als 15.000 Schecks an falsche Adressen verschickte. Ein Computer der US-Sozialversicherung hatte 1976 irrtümlich die Auszahlung von mehr als 600 Mio. $ veranlaßt.[13]

Diese Kumulations- und Multiplikationseffekte sind noch mit Schäden durch konventionelle Technik-Systeme vergleichbar: Ein falscher Wert in einem Lehrbuch, eine verrutschte Adressenliste, ein Konstruktionsfehler in einem Gerät oder eine falsch eingestellte Maschine können ähnliche Effekte bewirken. Der Unterschied liegt jedoch in den quantitativen und qualitativen Schadensaspekten. Werden Schecks manuell geschrieben, können nicht gleich 15.000 Anschriften verrutschen. Der Fehler in einem Lehrbuch bleibt eine isolierte Information und ist daher leicht erkennbar. Aber ein Fehler in einem Expertensystem geht in eine sehr komplexe Antwort ein und kann deshalb verborgen bleiben.

Völlig neu gegenüber aller bisherigen Technik ist jedoch die Möglichkeit, daß gleiche Schäden in entkoppelten Systemen *zum gleichen Zeitpunkt* auftreten (*Typ III: Kopplungsschaden*). Da IuK-Technik programmgesteuert ist, kann dieser Schaden bereits durch einen Programmfehler oder eine Softwaremanipulation hervorgerufen werden. Selbst entkoppelte und weitverteilte isolierte Systeme werden durch die gleiche Software sehr eng gekoppelt. Ein Fehler oder eine Beeinflussung von Programmen kann alle Nutzer

11 S. FR v. 27.1.1986.

12 S. hierzu z.B. DSB 9/1987, 1 ff., 10/1987, 1 ff.

13 S. Washington Post v. 9.5.1977 und Washington Star v. 17.6.1976 - zit. nach Bequai 10.

gleichermaßen treffen. Enthält das Betriebssystem eines verbreiteten Rechners eine 'logische Bombe', die dieses Programm zu einem bestimmten Zeitpunkt löscht, würden alle Anwendungen dieses Rechnertyps für unterschiedlichste Aufgaben mit einem Schlag ausfallen. Ein Großteil, wenn nicht alle IuK-Anwendungen in einem bestimmten Umkreis könnten gestört werden, wenn absichtlich oder unabsichtlich elektromagnetische Störungen verursacht werden. Und nicht nur einzelne Gerätetypen oder alle Geräte in einer Region, sondern alle IuK-Systeme, die nicht besonders 'gehärtet' sind - also 99% - fielen mit einem Schlag aus, wenn etwa durch die Zündung einer Atombombe in großer Höhe ein elektromagnetischer Puls erzeugt würde.

Größere Schadenspotentiale

IuK-Technik kann aber nicht nur zu einer neuen Ausbreitung von Schäden führen, sondern auch das Ausmaß einzelner Schäden erhöhen. Sie könnte sogar ganz neue Schadensmöglichkeiten schaffen, weil durch sie Prozesse oder Wirkungen möglich werden, die es bisher noch nicht gab. Handlungsgrenzen werden weiter hinausgeschoben, gleichzeitig aber neue, größere Schäden riskiert. Zwei Typen sind zu unterscheiden:

Bereits das Versagen eines einzelnen IuK-Systems kann einen höheren Schaden verursachen, weil von ihm größere Wirkungen auf die Umwelt ausgehen, Teilschäden sich zu größeren Schäden entwickeln oder gestiegene Abhängigkeiten zu größeren Schadensfolgen führen (*Typ IV: hoher Einzelschaden*). IuK-Technik kann dazu dienen, die bisherigen Grenzen von Raum, Zeit und Energie zu überwinden. Immer größere Informationsmengen werden auf immer kleinerem Raum gesammelt und in immer kürzerer Zeit übermittelt. Dadurch werden die Steuerungs- und Kontrolleistung von IuK-Systemen erhöht und technische Systeme noch schneller, stärker und größer. Autos, Züge und Flugzeuge können in kürzerer Zeit größere Strecken zurücklegen. Größere Energiemengen können wirkungsvoller erzeugt und umgesetzt werden. Je größer die funktionsgemäßen Wirkungen sind, desto größer sind auch die Schäden im Versagensfall.

Durch die Steigerung des elektronischen Geldumlaufs gegenüber dem papiergebundenen liegt der Schaden, den Computerkriminalität im Einzelfall verursacht, zwanzig- bis vierzigmal höher als bei konventionellen Delikten.[14] Der direkte durchschnittliche Schaden soll Anfang der 80er Jahre in den USA 3,3 Millionen Dollar und in der Bundesrepublik 1,5 Millionen Mark betragen haben.[15] Die jährlichen Verluste durch Computerkriminalität werden in den USA auf mehrere 100 Milliarden Dollar[16]

14 S. Abel/Schmölz 11.

15 S. Zimmerli/Liebl 22; Schönberg 92.

16 S. Abel/Schmölz 11.

und in der Bundesrepublik auf 15 Milliarden Mark geschätzt.[17] Die hohen Schäden sind also nicht selten.

Die Weiterentwicklung der IuK-Technik ermöglicht, auf immer kleinerem Raum mehr technische Funktionen zu integrieren und parallel oder in kürzerer zeitlicher Abfolge zu nutzen. Dadurch werden einfache und lineare Abläufe zunehmend durch hoch komplexe und eng gekoppelte Systeme ersetzt. Wie Perrow gezeigt hat, wirken hohe Komplexität und enge Kopplung jedoch schadenserhöhend. Mit zunehmender Komplexität steigt die Möglichkeit, daß Einzelfehler in unvorhersehbarer Weise miteinander interagieren. Enge räumliche und zeitliche Kopplung von Prozessen erhöht die Schadensfolgen, weil sich schädigende Ereignisse leichter 'fortpflanzen' können.[18]

In Zukunft werden immer größere Teile der Informationsverarbeitung, -speicherung und -übermittlung der IuK-Technik übertragen. Die Abhängigkeit nimmt zu, das Schadenspotential steigt. Ein Gradmesser hierfür sind Einschätzungen, wie lange ein Anwender bei einem Ausfall seines IuK-Systems noch weiterarbeiten könnte:

Nach einer 1987 veröffentlichten EG-weiten Umfrage unter Managern aus unterschiedlichsten Branchen können 20% der Unternehmen nur noch Stunden und 48% nur noch Tage weiterarbeiten, wenn die interne Datenverarbeitung versagt.[19] Nach einer Studie der Universität Minnesota von 1984 soll der 'Überlebenszeitraum' nach dem Ausfall des eigenen Rechenzentrums für Banken zwei Tage, für Vertriebsfirmen drei Tage, für Produktionsunternehmen fünf Tage und für Versicherungen fünfeinhalb Tage betragen.[20]

Werden IuK-Systeme miteinander vernetzt und sind von dieser Vernetzung abhängig, kann ein Technikausfall zu Schäden im gesamten Vernetzungskomplex führen (*Typ V: Komplexschäden*). Ein Schaden in einem Servicerechenzentrum, in einer ISDN-Nebenstellenanlage oder gar im Telekommunikationsnetz wirkt sich sehr schnell auf alle angeschlossenen Teilnehmer aus. Auch hier gilt wieder: Je stärker die Vernetzung, je enger die Koppelung und je höher die gesellschaftliche Abhängigkeit, desto größer kann ein Schaden sein.

Die Abhängigkeit von einer Vernetzung steigt, je mehr durch sie Redundanz abgebaut wird. Vernetzung kann Raum und Zeit und damit Kosten sparen. Ein ausgebautes Telekommunikationsnetz macht es überflüssig, Informationen in jeder Bibliothek zu sammeln, es genügt eine zentral vernetzte Datenbank. Durch eine computerintegrierte Fertigung erübrigen sich viele Lager und Konstruktionsbüros. Lagerzeit und -platz werden durch zeitgenaue Produktion und die Konstruktionsbüros durch eine zentrale CAD-Abteilung er-

17 S. Schönberg 92; Sicherheits-Berater 1986, 48: 3 - 4 Mrd.; Steiner, IO-Management-Zeitschrift 1988, 101: 40 Mrd. DM.

18 S. Perrow 107 ff., 131 ff.

19 S. Evens/Orr 12; s. hierzu auch Bschorr 119: 2 Tage; Zeit 44/1985, 25: im Durchschnitt 2 - 5 Tage.

20 Zit. nach Steinbach DuD 1985, 159 und Lindemann CW v. 27.4.1984, 1.

setzt. Fällt das Netz aus, kann niemand mehr die Produktion steuern, Konstruktionszeichnungen übermitteln oder Informationen abrufen.

Vernetzung vermag Prozesse enger zu verkoppeln. Wiederum kann sie Zeit und Raum und damit Kosten sparen, indem sie die Linearität von Abfolgen aufhebt und Puffer beseitigt. Verschiedene Informationsverarbeitungen können zeitgleich stattfinden und 'real time'-Wirkungen erzeugen. Dadurch sinken jedoch die Möglichkeiten, in den Prozeß einzugreifen, wenn ein Fehler entstanden ist. Er kann grundsätzlich mit der gleichen Geschwindigkeit und Raumüberwindung in einer Schadenskaskade fortwirken wie der intendierte Prozeß.[21]

Schließlich wächst das Schadenspotential, je mehr Anwendungen an ein Netz angeschlossen und in ihren Funktionen von diesem abhängig werden. Denn dadurch entstehen grundsätzlich mehr Möglichkeiten, daß ein Schaden andere Anwendungen beeinflußt oder auf diese übertragen wird.

Vernetzung kann aber auch Redundanz und Entkopplung schaffen und damit schadensmindernd wirken. Die Vervielfachung von Netzelementen erlaubt nämlich, beim Ausfall eines Netzknotens oder einer Übertragungsstrecke ohne Funktionsverlust auf andere umzuschalten. Werden Datenbestände und Datenverarbeitung dezentralisiert und von anderen entkoppelt, verteilt sich auch das Schadenspotential. Der Anschluß ans Netz erhöht die Chance, daß im Versagensfall ein anderes System die Funktionen des ausgefallenen übernehmen kann.

Diese fünf IuK-spezifischen Schadenstypen können jeweils für sich, aber auch vielfach vermischt vorkommen. Denkbar ist beispielsweise, daß die Kumulation von Schäden (Typ I) oder ein gemeinsamer Softwarefehler in Vermittlungsrechnern (Typ III) zum Ausfall eines Netzes (Typ V) und in der Folge zu vielen hohen Einzelschäden (Typ IV) führt.

Katastrophen

Diese Schäden können zu Katastrophen werden. Eine Katastrophe ist der Abschnitt eines Prozesses, in dem die schädigenden Wirkungen die kulturellen Schutzmechanismen zu deren Bewältigung übersteigen.[22] Ob der Zusammenbruch von Schutzmechanismen eine Katastrophe ist, hängt somit von der sozialen Einheit ab, auf die der Begriff bezogen wird. Was für eine Familie oder eine kleine Gruppe eine Katastrophe ist, muß es für eine Stadt oder ein Land noch lange nicht sein.[23] Wir wollen im folgenden mit dem Begriff Katastrophe nur solche Schadensprozesse bezeichnen, die für einen gewissen Zeitraum die Abwehrkräfte der gesamten Gesellschaft oder regionaler bzw. sektoraler Gesellschaftsteile, sie zu bewältigen, übersteigen. Schäden können zu Katastrophen werden,

21 S. hierzu auch Spiers 31; Debons 16.

22 S. hierzu auch Dombrowski 34; Clausen 43, 48.

23 S. Clausen 48f.

wenn sie auf eine Katastrophendisposition in ihrer Umgebung treffen.[24] Betrachten wir, aufgrund welcher Voraussetzungen IuK-spezifische Schäden zu einer gesellschaftlichen Katastrophe führen könnten.

Damit aus einem oder mehreren Schadensereignissen eine Katastrophe werden kann, ist zum ersten eine hohe und eng gekoppelte Verflechtung gesellschaftlicher Subsysteme erforderlich. In einer solchen Infrastruktur ist eine *dynamische Schadensabfolge* möglich, die sich wie Schockwellen in alle verflochtenen Systeme ausbreitet. Die Schadenswirkungen bleiben nicht lokal oder sektoral begrenzt, sondern sind immer gleich flächendeckend und systemübergreifend. Schadenswirkungen in benachbarten sozialen Systemen werden nicht gegenseitig aufgefangen, sondern durch die Rückwirkungen der jeweiligen Schäden wechselseitig verstärkt. Schadensverläufe mit einer solchen Dynamik und Komplexität können leicht die Möglichkeiten zu ihrer Bewältigung übersteigen.

Zum anderen muß die Gesellschaft von den betroffenen IuK-Systemen *in hohem Maße* abhängig sein. Denn dann fallen mit der Technik auch die ihr übertragenen gesellschaftlichen Funktionen aus. Je mehr der Umlauf des Geldes, die Herstellung von Gebrauchsgütern, die Steuerung des Verkehrs, die Verteilung von Lebensmitteln vernetzten IuK-Systemen übertragen ist, desto größer sind die Schäden, wenn diese Systeme versagen.

Die dritte Voraussetzung für eine Katastrophe ist, daß *funktionale Äquivalente* für die ausgefallene Technik *fehlen*, die deren soziale Funktionen übernehmen könnten.[25] Katastrophen können umso leichter bewältigt werden, je mehr Substitutionsmöglichkeiten für die ausgefallenen Funktionen bestehen.[26] Die Menschen müssen jedenfalls immer soviele 'zivilisatorische Stufen' zurückgehen, bis sie funktionale Äquivalente gefunden haben. Beim Ausfall der Telekommunikation müssen sie, um noch kommunizieren zu können, Briefe schreiben oder mit dem Auto fahren. Ist dies nicht möglich, weil der Verkehr zusammengebrochen ist, müssen sie noch eine Stufe weiter zurück und mit dem Fahrrad fahren oder zu Fuß gehen. Je weiter sie zurück müssen, umso weniger tauglich sind die Äquivalente, die Katastrophe zu bewältigen.

Schließlich müssen die Menschen über *Kenntnisse* und die Gesellschaft über eine passende *Infrastruktur* verfügen, um die vorhandenen funktionalen Äquivalente auch nutzen zu können. Sie sind umso hilfloser, je stärker sie auf die Technik vertraut haben und je ungewohnter sie im Umgang mit den 'Hilfskrücken' sind. Je stärker die Menschen ihre Kompetenzen auf die neue Technik ausgerichtet haben, je mehr die Gesellschaft die 'überflüssigen' Infrastrukturelemente der alten Technik eingespart hat, um so stärker wird sie die Katastrophe treffen.[27]

24 S. hierzu z.B. Frei 20.

25 S. hierzu Clausen/Dombrowski 295, 297.

26 S. Perrow 135.

27 S. hierzu z.B. Dombrowski 20, Clausen 59.

8. Abhängigkeiten und Schadenspotentiale in der 'informationsgesellschaft'

Nach dieser begrifflichen Vorklärung wollen wir uns der praktischen Frage zuwenden, welche Schäden und Schadensfolgen in der 'Informationsgesellschaft' möglich sind. Im begrenzten Rahmen dieser Untersuchung kann allerdings nur exemplarisch erörtert werden, inwieweit die IuK-spezifischen Schadenstypen in bestimmten Anwendungsbereichen Bedeutung erlangen können. Ebenso soll auch die Katastrophentauglichkeit dieser Gesellschaft lediglich an einem Beispiel betrachtet werden. Wir wollen deren Katastrophendisposition gedanklich testen, indem wir unterstellen, die Telekommunikation wäre zu großen Teilen ausgefallen. Eine ausführlichere Untersuchung dieser Fragen wäre eine lohnende Aufgabe für viele Forschungsprojekte.

Gesellschaftliche Abhängigkeit heute

Bereits heute übernehmen IuK-Systeme in vielen Bereichen gesellschaftliche Funktionen. Infolgedessen besteht bereits eine hohe Abhängigkeit von der automatischen Informationsverarbeitung und der Telekommunikation. Automatische Datenverarbeitung findet statt in der Produktion, in der Verwaltung, im Dienstleistungsbereich, in der Wissenschaft, in militärischen und anderen gesellschaftlichen Bereichen. Im Bereich der Prozeßsteuerung kann ein Ausfall der Steuerungssysteme sogar zu Gefahren für Leib und Leben großer Bevölkerungsteile führen. Die EDV hat jedoch andere Formen der Informationssammlung und -verarbeitung nicht völlig verdrängt. Soweit einzelne Verwaltungszweige oder Produktionslinien völlig von ihrem Funktionieren abhängig sind, bilden diese immer noch Inseln der Automatisierung. Noch existiert keine vollkommene Vernetzung aller Bereiche der Informationsverarbeitung. Daher bestehen für viele Formen der automatischen Datenverarbeitung im Notfall noch Substitutionsmöglichkeiten. Der Ausfall der DV führt dann nur zu Belästigungen und Verzögerungen, nicht aber zu einem völligen Funktionsausfall. Die Privathaushalte sind von der Informatisierung noch kaum erfaßt.

Für die Telekommunikation besteht eine allgemeine Abhängigkeit vom Fernsprechnetz und eine spezielle Abhängigkeit etlicher Unternehmen und Verwaltungen von der Datenübertragung. In den meisten Anwendungsfällen können sich Fernsprechen oder Datenübertragung gegenseitig ersetzen oder bei einem Ausfall durch die 'gelbe Post', durch Austausch von Datenträgern oder direkten Kontakt substituiert werden, so daß dieser nur komfortmindernd wirkt. In vielen Fällen, insbesondere im Bereich der Geschäftskommunikation ist aber die Telekommunikation inzwischen so zeitkritisch, daß auch ihr kurzfristiger Ausfall zu ernsthaften Schäden führt. Viele Verwaltungen und Unternehmen sind zudem von der Integrität und Vertraulichkeit der übermittelten Nachrich-

ten abhängig. Abgesehen vom Telefondienst ist der Privatbereich noch nicht und der Handel kaum in die Telekommunikation eingebunden.

Die Verwundbarkeit der Telekommunikation wird auch durch ihren Netzaufbau begrenzt. Durch die Vermaschung der Vermittlungsstellen auf der Fernebene des Fernsprechnetzes besteht eine hohe Ausfallsicherheit, da Ausfälle einer Verbindung von anderen mitübernommen werden können. Ein Totalausfall im Fernverkehr ist allenfalls im Bereich einer Knotenvermittlungsstelle und im Ortsverkehr im Anschlußbereich einer Ortsvermittlungsstelle denkbar. Im Datex-L-Netz gibt es allerdings nur 19 und im Datex-P-Netz nur 17 Vermittlungsstellen, so daß der Ausfall einer Vermittlungsstelle einen größeren Bereich von der Datenübertragung ausschließt. Im Datex- P-Netz ist sogar ein Totalausfall der programmgesteuerten Vermittlungssysteme denkbar.

Gesellschaftliche Abhängigkeit morgen

In einer aus dem heutigen Trend sich entwickelnden *künftigen* 'Informationsgesellschaft' wird die Abhängigkeit vom Funktionieren der automatischen Informationsverarbeitung und Telekommunikation und damit das potentielle Schadensausmaß noch beträchtlich ansteigen. Informationsverarbeitung und Telekommunikation werden in Umfang, Verbreitung und Bedeutung zunehmen, noch stärker in die Gesellschaft eindringen und zu einem vernetzten System zusammenwachsen. Dabei werden sie andere Formen der Informationssammlung, -verarbeitung und Kommunikation verdrängen und schließlich weitgehend ohne Alternativen und Substitutionsmöglichkeiten sein. Störungen in einem Bereich werden sich dann schnell auf andere Bereiche übertragen.

Es besteht eine IuK-gestützte Warenwirtschaft, die auf der völligen Vernetzung von Lieferanten, Zulieferern, Produzenten, Händlern, Kunden und Banken beruht. Vom Funktionieren der IuK-Systeme werden auch die Energieversorgung, die medizinische Versorgung, das gesamte Zahlungssystem, die wichtigsten Dienstleistungen, wissenschaftliche Organisationen, das Verkehrssystem, die staatliche Verwaltung, die politische Steuerung, die Medien sowie der Umweltschutz mehr oder weniger stark abhängig sein. Sehen wir uns die Abhängigkeit einiger dieser Anwendungsbereiche von IuK-Techniken näher an.

Prozeßsteuerung

Industriegesellschaften nutzen Techniksysteme mit sehr großen Schadenspotentialen. Die absichtliche oder fehlerhafte Freisetzung großer Energiemengen oder giftiger Substanzen aus diesen Industrieanlagen kann katastrophale Schäden bewirken.[1]

1 S. hierzu näher Roßnagel 1986, 340 ff.

Um die Größenordnungen solcher Schäden deutlich zu machen, sei auf einige Risikostudien verwiesen: Nach der Deutschen Risikostudie Kernkraftwerke können durch einen Kernschmelzunfall mit Dampfexplosion in einem 1300 MW-Reaktor bis zu 15.000 Menschen in relativ kurzer Zeit durch akutes Strahlensyndrom und 100.000 Menschen zu einem späteren Zeitpunkt durch Leukämie und Krebs getötet werden. Außerdem könnte eine Fläche von der doppelten Größe des Saarlandes verseucht und dadurch eine Umsiedlung von bis zu 2,9 Millionen Menschen notwendig werden.[2] Die Freisetzung einer Grundsubstanz für Pflanzenschutzmittel hat im Dezember 1984 in Bhopal/Indien rund 5.000 Todesopfer und etwa 80.000 Verletzte gefordert. In den kommenden Jahren werden noch Tausende an den Folgen der Vergiftung sterben. Über 1000 Menschen sind erblindet.[3] Nach einer Risikoanalyse des TÜV Rheinland würde zum Beispiel eine Explosion in einem 30 000-Liter-Phosgen-Tank bis zu 2 000 'Soforttote' und fast 20 000 zum Teil Schwerverletzte fordern.[4] Ein Unfall in den Tank- und Raffinerieanlagen auf der Insel Canvey in der Themse-Mündung könnte bis zu 18 000 Tote zur Folge haben.[5]

Das Schadenspotential von Chemiebetrieben, von Anlagen der Energieerzeugung und -verteilung oder anderen Produktionsstätten ist in erster Linie von den dort stattfindenden energiereichen und schadstoffhaltigen Prozessen abhängig. Steuern bei gleichem Komplexitätsgrad IuK-Systeme statt Menschen oder konventioneller Technik diese Prozesse, verändert dies für sich noch nicht das Schadenspotential, sondern erhöht oder senkt lediglich die Wahrscheinlichkeit ihres Eintritts. Softwaregesteuerte Sicherheitsleittechnik wurde beispielsweise für den Einsatz in Atomkraftwerken bisher als zu unzuverlässig angesehen. Wie in den meisten Steuerungs- und Kontrollsystemen soll sie jedoch aufgrund verbesserter Engineering-Techniken die festverdrahteten Leitsysteme zunehmend verdrängen.[6] Wird mit der Einführung der IuK-Technik auch die Architektur der Prozeßsteuerung verändert, kann eine höhere Komplexität und eine engere Kopplung die Sicherheit des Gesamtprozesses stärker von dem zuverlässigen Funktionieren der Steuerungstechnik abhängig machen.[7]

Während bisher die konventionelle und auch die elektronische Steuerungstechnik meist isoliert arbeitete und nur für die spezifische Anwendung entwickelt wurde, geht der Trend zu hierarchischen Steuerungsnetzen, die unter Verwendung standardisierter Module dezentral prozeßnahe Kleinrechner mit einem zentralen Großrechner verbinden.[8] Dadurch werden nun Multiplikations-(Typ II) oder Komplexschäden (Typ V) möglich, wenn etwa falsche Daten in vielen prozeßnahen Steuerungssystemen gleichermaßen verwendet werden oder Netzausfälle die 'Kommunikation' zwischen den Rechnern verhindern.

2 S. Gesellschaft für Reaktorsicherheit 165f., 206 ff., 218 ff.

3 S. z.B. Spiegel 17/1985, 134 ff.; FR v. 1.7.1985.

4 Zit. nach Koch/Vahrenholt 74 f.

5 S. Health and Safety Executive 33 ff.; zu weiteren Schadenspotentialen der Großtechnik s. z.B. Lagadec; Perrow.

6 S. hierzu z.B. Rauch/Mertens CM 5/1987, 56 ff.

7 S. hierzu näher Perrow 33 ff., 57 ff., 141 ff.; Andow 233 ff.

8 S. hierzu Gottschlich 39.

Diese Schäden bleiben in der Regel auf den Werkskomplex beschränkt, da das lokale Steuerungsnetz isoliert arbeitet. Durch die Standardisierung sind künftig aber auch Kopplungsschäden (Typ III) nicht mehr auszuschließen. Eine Manipulation in einem Basisprogramm des Steuerungsnetzes könnten viele energiereiche Prozesse und hochgiftige Substanzen gleichzeitig außer Kontrolle geraten lassen.

Einen spezifischen Beitrag zur Schadensentwicklung liefert die IuK-Technik dann, wenn im Vertrauen auf eine bessere Steuerungstechnik bisherige Grenzen überschritten werden. Es entspricht einem alten Ingenieurstraum, den Menschen als die Komponente, der sie mißtrauen, durch technische Geräte zu ersetzen, denen sie vertrauen oder die sie zumindest verstehen.[9] Durch die Selbststeuerung soll die Wirksamkeit der Technik erhöht werden. Technische Prozesse sollen noch kraftvoller, in noch kürzerer Zeit, auf noch engerem Raum oder in noch größeren Anlagen ablaufen. Hierfür müssen bisherige Sicherheitsreserven durch verbesserte Steuerungstechnik ersetzt werden. Mögliche Zuverlässigkeitsgewinne durch IuK-Technik werden durch die steigenden Schadensmöglichkeiten wieder 'verbraucht'. Automatisierung reduziert zwar das unmittelbare Risiko von Arbeitsunfällen. Die Sicherheit der Bevölkerung aber wird immer stärker von dem einwandfreien Funktionieren der Prozeßtechnik abhängig.

Verkehr

Der Personen- und Güterverkehr wird auch für eine 'Informationsgesellschaft' von zentraler Bedeutung sein. Zwar werden Informationen überwiegend elektronisch ausgetauscht, doch müssen Personen und Güter weiterhin transportiert werden. Eine Störung des Güterverkehrs könnte zu Engpässen in der Versorgung und zu Milliardenverlusten durch Produktionsausfälle führen - Gefahren, die durch die neuen logistischen Konzepte der zeitgenauen Lieferung im Warenwirtschafts- und Produktionsbereich noch gesteigert werden. Störungen des Personenverkehrs können zu Personenschäden und zum Verlust der Arbeitszeit führen. Wie wird dieses Schadenspotential von Verkehrsstörungen durch IuK- Technik beeinflußt?

Der *Autoverkehr* ist vor allem deswegen so gefährlich, weil die Kommunikation zwischen den Verkehrsteilnehmern angesichts ihrer Geschwindigkeit unzureichend ist. Ihr Verkehrsverhalten wird lediglich durch Blickkontakt und die gemeinsame Beachtung von Verkehrsregeln gelenkt. Die Sicherheit des Straßenverkehrs kann erheblich erhöht werden, wenn durch IuK-Technik die Kommunikation und die Informationsverarbeitung erhöht und beschleunigt wird: Über Verkehrsleitsysteme werden Staus vermieden. Abstandsradar ermöglicht das vollautomatische Konvoifahren auf der Autobahn. Infrarotsensoren erlauben schnelle Fahrt auch durch dickste Nebelbänke. Kommunikationsnetze zwischen den Fahrzeugrechnern untereinander, zur Leitzentrale und zu Mikrorechnern in

9 S. Wiener 164.

Baken an den Fahrstrecken erweitern den Wahrnehmungsbereich durch 'elektronischen Blickkontakt' und erhöhen die Reaktionsgeschwindigkeit. Übersieht der Fahrer einen Verkehrsteilnehmer oder reagiert er zu langsam, leitet der Computer innerhalb von Millisekunden die erforderliche Reaktion selbst ein.[10]

Angesichts von 8.000 bis 10.000 Verkehrstoten in jedem Jahr können Maßnahmen, die die Verkehrssicherheit steigern sollen, zunächst nur Unterstützung finden. Bei aller guten Absicht muß jedoch die Frage erlaubt sein, ob die IuK-Technik im Straßenverkehr nicht auch Schäden erhöhen kann, statt sie nur zu reduzieren. Die Abhängigkeit von der Technik steigt, insbesondere wenn Sicherheitsgewinne im Vertrauen auf die Technik durch höhere Geschwindigkeiten oder geringere Abstände wieder 'verbraucht' werden. So sollen zum Beispiel in einigen Jahren die Autos mit einem Convoy-Piloten ausgerüstet sein und dann auf der Autobahn bei Tempo 120 mit nur einem halben Meter Abstand automatisch Kolonne fahren können.[11] Manch einer träumt sogar bereits davon, mit 200 'Sachen' über die Autobahn zu 'brausen' - während er am Steuer schläft.[12] Engere Kopplung verbessert einerseits den Verkehrsfluß, erhöht aber andererseits das Schadenspotential. Wenn bei einem halben Meter Abstand, bei 200 km/h schlafend oder bei hoher Geschwindigkeit im Nebel die Technik versagt, gibt es keine Sicherheitsreserven mehr. Besonders gefährliche Folgen könnten Multiplikationsschäden (Typ II) verursachen - etwa wenn das Leitsystem an alle Bordrechner falsche Werte übermittelt. Kaum beherrschbar wären auch Kopplungsschäden (Typ III) - wenn viele Bordrechner oder Abstandssensoren zur gleichen Zeit versagten -, und katastrophal könnten sich Komplexschäden (Typ V) auswirken - wenn etwa das Leitnetz ausfiele.

Aber selbst ganz gewöhnliche, tagtäglich sich ereignende Unfälle könnten verheerende Folgen haben. Selbst wenn die Technik funktioniert und ohne jede Zeitverzögerung reagiert, kann sie die von der Geschwindigkeit abhängigen Bremswege nicht verkürzen. Kommt ein in Kolonne fahrendes Fahrzeug durch ein Hindernis - etwa ein von einer anderen Fahrbahn abgekommenes Fahrzeug - schneller zum Stehen, als es bremsen kann, ist ein massenhafter Auffahrunfall nicht mehr zu vermeiden.

Eine neue Schadensmöglichkeit kommt hinzu: Damit der Zentralrechner des Verkehrsleitsystems das Fahrzeug auf dem günstigsten Weg zum Ziel führen oder gar leiten kann, muß die jeweilige Position des Fahrzeuges bekannt sein. Wenn zur Identifizierung der Fahrzeuge gegenüber dem Leitsystem nicht jeder jedesmal vor Fahrtbeginn ein anderes Kennzeichen eingibt, sondern der Einfachheit halber jeweils sein amtliches Kennzeichen, dann ermöglicht das Leitsystem eine lückenlose Bewegungskontrolle.[13]

---

10 S. hierzu näher die Forschungen in dem EUREKA-Projekt "PROgraM for an European Traffic with Highest Efficiency and Unprecedended Safety" (PROMETHEUS) - s. z.B. die Berichte hierüber in Spiegel 17/1988, 259f., 25/1988, 72f.; Hausmann 15; Strampp 2.

11 S. Spiegel 17/1988, 259f.

12 S. Hausmann 15.

13 S. hierzu auch Spiegel 25/1988, 73.

Flugzeuge können durch weitere Automatisierung sicherer und effizienter werden. Um die höhere Effizienz zu nutzen, werden künftig - wie in der Vergangenheit auch - nach jeder weiteren Automatisierung an Flugzeug und Besatzung härtere Anforderungen gestellt. Die Maschine muß mit weniger Treibstoff auskommen, auch bei schlechterem Wetter und dichterem Luftverkehr fliegen und die Flugstrecken schneller zurücklegen. Gleichzeitig wird in neueren Verkehrsflugzeugen, wie der Boing 767 oder dem Airbus A320, der Bordingenieur durch Computer ersetzt. Aufgrund dieser Maßnahmen bleibt für die Crew immer weniger Zeit für Navigation, Kontakt zur Bodenkontrolle und die Handhabung des Systems. Also werden alle diese Tätigkeiten zunehmend automatisiert.[14] Die Komponenten des Systems Flugzeug werden dadurch enger gekoppelt. Bei Stör- oder Unfällen bestehen weniger oder keine Möglichkeiten zum Eingreifen[15] oder zur Regenerierung des Systems. Sicherheitsgewinne durch Automatisierung könnten so durch höhere Effizienzanforderungen wieder verloren gehen.

Der *Luftverkehr* in der Bundesrepublik und in Europa wird sich allein bis zum Jahr 2000 verdoppeln.[16] Da weitere Start- und Landebahnen wegen des zunehmenden Bürgerwiderstands kaum gebaut werden können, wird die Verdichtung des Luftverkehrs die Flugsicherung dazu zwingen, Flugzeuge direkt zu leiten. Nur so ist die heutige Frequenz - zum Beispiel 64 Starts und Landungen pro Stunde in Frankfurt - zu verdoppeln und der derzeitige Sicherheitsabstand bei Anflügen von drei bis fünf Meilen zu halbieren. Das höhere Risiko soll IuK-Technik abfangen. So ist zum Beispiel daran gedacht, durch Anflugleitsysteme den Landeanflug zu verkürzen und dadurch die Differenzen zwischen schnellen und langsamen Flugzeugen zu reduzieren.[17] Als weitere Maßnahme soll die Computerüberwachung und -leitung durch Eurocontrol in Brüssel verbessert und ausgebaut werden.[18] Nach dem Jahr 2000 ist zu erwarten, daß die Computer der Flugsicherung direkt über Funk die Flugleitcomputer an Bord programmieren.[19] Insgesamt wird die Sicherheit des Luftverkehrs noch stärker von IuK-Technik abhängig und mit ihrer Hilfe enger verkoppelt.

Dadurch steigt das Schadenspotential. Pannen wie im Juni 1987, als jeweils wegen eines Computerfehlers das Radarsystem des Logan International Airports in den USA für sechs Minuten und der Flugsicherungscomputer im schottischen Flughafen Prestwick völlig ausfielen, und im September 1987, als wegen eines Stromausfalls die Radarschir-

14 S. hierzu z.B. Wiener 164 ff.; Perrow 176 ff., 202f.; Lutterbeck 1984, 17f.

15 Das Flugkontrollsystem des Airbus A320 ermöglicht nicht nur automatisches Fliegen, sondern korrigiert sogar Flugfehler der Piloten. So hat es bei dem Absturz am 26.6.1988 bei Mühlhausen offensichtlich eine Fehlreaktion des Piloten korrigiert und eine 'sanfte Bauchlandung' ermöglicht - s. FR v. 23.7. 1988. Da Computeranweisungen den Pilotenbefehlen vorgehen, heißt dies aber auch, daß bei einem Versagen der Technik der Pilot nicht mehr korrigierend eingreifen kann.

16 So z.B. die Forderung des Deutschen Industrie- und Handelstages -s. FR v. 18.8.1988; s. auch FR v. 8.6.1988; Spiegel 14/1988, 26 ff., 29.

17 S. Perrow 203.

18 S. hierzu FR v. 8.6.1988; Spiegel 14/1988, 37.

19 S. hierzu Wiener 165f.

me aller Lotsen auf dem Flughafen Frankfurt für zwei Minuten erloschen[20], könnten verheerende Folgen haben. Die dichte Abfolge von Starts und Landungen und das Ersetzen von Sicherheitsreserven durch IuK-Technik kann bei deren Ausfall nicht nur zum Absturz eines Flugzeuges, sondern auch zum Zusammenstoß mehrerer Flugzeuge führen.[21] Doch nicht nur der Ausfall der IuK-Technik ist hoch schadensträchtig: Auch die Folgen eines geplatzten Reifens, eines verklemmten Fahrwerks, eines Maschinenschadens oder einer Sturmböe können wegen der höheren Flugdichte gravierender sein.

Der *Schienenverkehr*[22] soll ebenfalls durch IuK-Technik sicherer und effektiver werden. Zur Überwachung und Steuerung der Züge verfügen die Triebfahrzeuge der Deutschen Bundesbahn zunehmend über die 'induktive Sicherung' und die 'Linienzugbeeinflussung'. Jene kontrolliert ständig, ob Geschwindigkeitsbegrenzungen und Signalstellungen beachtet werden und löst im negativen Fall Zwangsbremsungen aus; diese verbindet über Linienleiter am Gleis den Zug mit der Streckenzentrale und übermittelt aktuelle Daten.[23] Durch beide wird der Lokführer von der Sicht auf Signale an der Strecke unabhängig, was immer höhere Geschwindigkeiten erlaubt. Werden sie ergänzt um leistungsfähige Verfahren der Mustererkennung, wird nach 2000 auf Hochgeschwindigkeitsstrecken mit erheblich schnelleren und automatisch gesteuerten Zügen zu rechnen sein.

Die Freigabe des Fahrwegs durch entsprechende Weichen- und Signalstellung erfolgt vollautomatisch über die dezentralen Stellwerksrechner. Ebenfalls dezentral sollen zukünftig die Gütertransporte gesteuert werden. Etwa 300 autarke Systeme in Knotenbahnhöfen sollen jeweils über die Daten verfügen, die für die Erfüllung der örtlichen Aufgaben notwendig sind, und zugbegleitend weiterübermitteln.[24] In dieses Transportsystem werden zum Beispiel die zentrale Datei über derzeit rund 900.000 Güterwagen[25], das 'Fahrzeuginformations- und Vormeldesystem' (FIV), das Daten über die Wagenladung, Versender, Empfänger und den Güterwagen enthält, sowie die 'Servicemeldung Wagenladung' (SMV), die dem Empfänger die Ankunft der Ladung voranmeldet, integriert.[26] Sie ermöglichen, die auf der Bahn befindlichen Güter in die neuen Logistikkonzepte mit aufzunehmen. Der Verkauf von Fahrkarten, Fahrplanauskünfte und Platzreservierungen werden effektiviert durch ein 'Kundenfreundliches Reise-, Informations- und Verkaufssystem' (KURS). Alle diese Systeme werden durch ein einheitliches bahneigenes ISDN vernetzt, das die bisherigen drei unterschiedlichen Bahnnetze ersetzen wird.[27]

---

20 S. Los Angeles Times v. 21.6.1987; FAZ v. 22.6.1987; Spiegel 14/1988, 30.

21 S. hierzu das Beispiel in Spiegel 14/1988, 30.

22 S. zum folgenden näher Pordesch Arbeitspapier 16.

23 S. hierzu näher Schwier BdW 1981, 102 ff.; Caesperlein/Thomas 221 ff.

24 S. hierzu z.B. Flugel/Knecht 594 ff.

25 S. hierzu z.B. Dahms 497 ff.

26 S. hierzu näher Grimm; Kübler 584.

27 S. hierzu z.B. Kuhbier/Wehner 37 ff.

Die Bahn ist heute schon ein sicheres Transportmittel. Die IuK-Technik könnte diese Sicherheit vor Unfällen noch weiter erhöhen. Gerade dies verführt aber auch zu einem höheren Schadenspotential. Denn erst die rechnergesteuerte Linienzugbeeinflussung macht Hochgeschwindigkeitszüge möglich. Die kinetische Energie eines Zuges nimmt mit der Geschwindigkeit prinzipiell quadratisch zu und verdoppelt sich beispielsweise in der Spanne von 140 auf 200 km/h. Verunglückt ein Zug trotz der Sicherheitsvorkehrungen bei 400 km/h, werden erheblich mehr Passagiere den Tod finden als bei den bisherigen Fahrgeschwindigkeiten. Zu einem derart hohen Einzelschaden (Typ IV) könnte es kommen, wenn zum Beispiel das Mustererkennungsverfahren in automatischen Triebwagen ein Hindernis nicht richtig erkennt. Mehrere solcher Unfälle könnten durch Multiplikationsschäden (Typ II) verursacht werden, wenn etwa von einem Stellwerksrechner an Weichen und Signale falsche Daten übermittelt würden. Noch gefährlicher könnten sich Kopplungsschäden (Typ III) oder Komplexschäden (Typ V) auswirken, wenn etwa alle oder viele Rechner in Stellwerken, Schienenübergängen oder Triebwagen gleichzeitig ausfielen oder das komplette Leitsystem für die automatisch gesteuerten Züge versagte.

Ein Ausfall des gesamten Verkehrssystems Bahn ist in der Regel ausgeschlossen, weil die Routendisposition dezentral durch die Stellwerke erfolgt und das 30.000 km lange Streckennetz auch bei Ausfall großer Teile erlaubt, den Güter- und Personenverkehr zumindest teilweise umzuleiten. Lediglich wenn alle Stellwerksrechner oder deren Software von einem einzigen Hersteller gefertigt würden, könnte durch ihren gleichzeitigen Ausfall (Kopplungsschaden - Typ III) der gesamte Bahnbetrieb lahmgelegt werden. Werden die manuell zu bedienenden 'Stelltische' als Sicherheitsreserve beibehalten und nicht eingespart, wären selbst in diesem Fall nur (allerdings erhebliche) Behinderungen zu erwarten. Fiele das einheitliche Bundesbahn-ISDN aus (Komplexschaden - Typ V), wären Schäden nicht ganz so gravierend wie beim Ausfall der Stellwerksrechner. Das funktionsfähige Streckennetz ließe immerhin noch Improvisationen zu. Der Ausfall wäre jedoch identisch mit dem Ende eines geordneten Bahnbetriebs.

Davon abgesehen kann es im Personenverkehr durch IuK-Schäden kaum zu Verkehrsengpässen kommen. Fällt zum Beispiel 'KURS' durch Kopplungsschäden (Typ III) oder Komplexschäden (Typ V) aus, so dürfte dies im wesentlichen nur zu Geld- und Vertrauensschäden bei der Bahn führen. Reisende hätten möglicherweise keinen Sitz-, Liege- oder Schlafplatz. Die Schaffner dürften nicht in der Lage sein, von allen Reisenden den Fahrpreis zu kassieren. Auf die (kostenlose) Reise selbst müßte aber wohl niemand verzichten.

Erheblich größer wird die Abhängigkeit von IuK-Systemen im Güterverkehr. Ohne elektronische Gütervormeldungen (FIV) müßten die Rangierarbeiten und die Zusammenstellung der Züge wieder durch umständliche Prozeduren anhand der Begleitpapiere, durch Sichtkontrolle der Wagenstellung oder durch Erfassung der an den Wagen befindlichen Daten durchgeführt werden. Die erheblichen Verspätungen könnten im Rahmen der neuen Logistikkonzepte schnell zu Produktionsunterbrechungen und Versorgungs-

engpässen führen. Noch gravierender wäre der Verlust der zentralen Fahrzeugdatei (hoher Einzelschaden - Typ IV). Ihre Rekonstruktion würde Monate dauern. In der Zwischenzeit aber wäre das FIV nicht funktionsfähig und die Leistungsfähigkeit des Gütertransportsystems Bahn drastisch reduziert. Dies würde der Bundesbahn erhebliche Einnahmeverluste bescheren, aber auch die Volkswirtschaft nachhaltig schädigen. Denn der Güterverkehr auf der Straße könnte nur einen geringen Teil der Transportausfälle auffangen.[28]

Landwirtschaft

Das Schadenspotential, das durch die Abhängigkeit von IuK-Systemen in der Landwirtschaft entstehen wird, ist demgegenüber gering.[29] Die Komplexität der Technik-Systeme ist niedrig und ihre Kopplung lose. Betroffen sind in der Regel nur einzelne landwirtschaftliche Betriebe. Vernetzungen entstehen zum einen durch Informationsdienste (Wetter, Schädlinge). Hier wären zwar durch falsche Informationen Multiplikationsschäden (Typ II) oder durch den Ausfall der Datenübertragung Komplexschäden (Typ V) möglich. Doch wirkt schadensmindernd, daß im ersten Fall in der Regel zeitliche Puffer zwischen Informationen und Reaktionen bestehen und im zweiten Fall mit Durchschnittswerten oder 'Bauernregeln' weitergearbeitet werden kann. Verflechtungen könnten sich zur Nahrungsmittelindustrie und zum -handel herausbilden. Auch wenn dort neue Logistikkonzepte zur Anwendung kommen, dürfte sich jedoch der Gegenstand selbst gegen eine allzu enge zeitliche Kopplung wehren. Nahrungsmittel in der Feldwirtschaft können einfach nicht zeitgenau und normgerecht produziert werden. Gravierende Schäden für die Allgemeinheit wären nur dann möglich, wenn die Landwirte relativ einheitliche Systeme im Einsatz hätten und diese durch einen Kopplungsschaden (Typ III) zur Erntezeit ausfielen.

Anders ist das künftige Schadenspotential vollcomputerisierter und roboterunterstützter Gemüsefabriken einzuschätzen. Da der Computer hier die Versorgung der Pflanzen reguliert, könnte bei einem Ausfall in relativ kurzer Zeit eine gesamte Produktionseinheit zusammenbrechen (hoher Einzelschaden Typ IV). Der höhere Automatisierungs- und Zentralisierungsgrad erschwert konventionelle schadensmindernde Maßnahmen. Je nach Diversifikation der Systeme könnten Kopplungsschäden (Typ III) oder Komplexschäden (Typ V) sogar die Jahresernte einer Region vernichten.

28 1987 beförderte die Bahn 278 Mio. t Güter und der Straßengüterfenverkehr 359 Mio. t - s. Deutsche Bundesbahn 13. Er müßte also ein Transportvolumen zusätzlich übernehmen, das vielleicht die Hälfte seiner normalen Kapazität erreicht.

29 S. zum folgenden näher Pordesch Arbeitspapier 16.

Gesundheitsversorgung

Die Informatisierung wird zu erheblichen Leistungssteigerungen der naturwissenschaftlich ausgerichteten kurativen Medizin führen. Neue Geräte verbessern Diagnose und Therapie, Expertensysteme erhöhen das aktuell verfügbare Wissen und neue Informationssysteme verbreitern die Basis und intensivieren den Fluß relevanter Krankheitsdaten.[30]

Informationstechnik in medizinischen Geräten soll die Behandlung unterstützen, indem sie deren Einwirkung auf den Patienten steuert oder auswertet. Fällt sie aus oder macht Fehler, kann dies die Gesundheit des Patienten beeinträchtigen. Die Berichte über solche Schäden nehmen zu:

So sind 1987 in den USA zwei Patienten zu Tode gekommen, weil ein Softwarefehler in einem radiotherapeutischen Bestrahlungsgerät zu einer vielfach höheren Bestrahlung geführt hat. In einem bestimmten Betriebszustand wurde ein erforderlicher Wolfram-Filter nicht vor den Elektronenstrahl geschoben.

Herzschrittmacher haben ausgesetzt, während sie vom Arzt neu eingestellt wurden. Ein Gerät, das mehrere Patienten gleichzeitig überwacht, soll diese verwechselt haben. Eine Insulinpumpe gab unvermutet zuviel von dem lebenswichtigen Hormon ab und aufgrund einer falschen Expertensystem- Diagnose erhielten Patienten vom Arzt eine Überdosis Medikamente verschrieben.[31]

Grundsätzlich wird das Schadenspotential durch die Funktion des Datenverarbeitungsgeräts und die Zahl der potentiell betroffenen Patienten bestimmt. IuK-spezifische Steigerungen von Schäden sind möglich, wenn größere Energiemengen auf den Patienten einwirken können, weil sie automatisch und sehr präzise gesteuert werden (hoher Einzelschaden - Typ IV). Sind medizinische Systeme weit verbreitet, können Multiplikationsschäden (Typ II) - Fehler in der Datenbasis eines Expertensystems führen bei vielen Patienten zu Fehldiagnosen - oder Kopplungsschäden (Typ III) - alle Dialysegeräte eines Herstellers arbeiten plötzlich doppelt so schnell - Schäden für Leben und Gesundheit vervielfachen.

Ein besonderes Schadenspotential kann sich ergeben, wenn nur mit Hilfe von IuK-Technik sehr risikoreiche medizinische oder pharmazeutische Forschungen möglich werden. Versagt etwa die Steuerungstechnik bei einem gentechnischen Versuch mit Retroviren oder führt ein Fehler im Auswertungsprogramm zu einer Fehleinschätzung der Gefährdung, könnten die Folgen katastrophal sein.

Krankenhausdokumentationssysteme beinhalten vom einzelnen her gesehen kein höheres Risiko, Patientendaten zu verwechseln, zu verfälschen oder auszuspähen, als die alte Patientenakte. Durch die elektronische Form der Sammlung, Auswertung und Übermittlung ergibt sich jedoch die besondere Möglichkeit von Multiplikationsschäden

30 S. z.B. Hammer/Roßnagel 1989.

31 S. hierzu z.B. Science News 133/88, 170 - zit. nach Schuh, Zeit 17/1988, 86; Brunnstein CW v. 8.4.1988, 12.

(Typ II), indem durch einen kleinen Programmfehler oder -befehl alle Daten verfälscht, vertauscht oder kopiert werden.

Produktion

"Die Abhängigkeit von der EDV wird jedenfalls von Tag zu Tag größer; dies gilt auch für Kleinbetriebe. Es entstehen Schnittstellen, bei deren teilweiser oder ganzer Zerstörung mit Betriebsausfällen von mehreren Tagen, Wochen, ja Monaten gerechnet werden muß. Der ... Mangel an Spezialisten führt zu Abhängigkeiten, die bis zur kriminellen Handlung ausgenutzt werden können. Wer nennt den Betrieb, der keine externen EDV-Berater hat?"[32]

So schildert der Leiter des Sicherheitsdienstes einer Industrieunternehmung in Zürich seine Sorgen durch die wachsende EDV-Abhängigkeit moderner Produktionsbetriebe. Fällt das eigene Rechenzentrum aus, so könnten - nach einer europaweiten Befragung der Manager von Fertigungsunternehmen - 16% nur noch wenige Stunden produzieren. 48% sahen immerhin noch die Möglichkeit, wenigstens für einige Tage weiterzuarbeiten.[33]

Diese hohe Abhängigkeit besteht bereits heute[34], obwohl die Automatisierung und Produktionssteuerung meist erst in einzelnen Inseln verwirklicht ist, neben numerisch gesteuerten Geräten oft noch konventionelle stehen, die Lager meist noch relativ groß und nach einer räumlichen Systematik geordnet sind, die Auftrags- und Konstruktionsdaten vielfach noch in Papierform oder in Form von Lochstreifen und Disketten durch den Betrieb fließen und das Personal noch gut ausgebildet ist und auf verschiedenen Arbeitsplätzen qualifiziert und flexibel eingesetzt werden kann. Fällt die Datenverarbeitung im Betrieb aus, können sich heute noch Maschinen und Facharbeiter weitgehend gegenseitig ersetzen. Auch bei einem Ausfall des Materialverwaltungssystems können die Lagerverwalter optisch noch einen gewissen Überblick behalten und weiterhin Material ein- und auslagern. Da die Daten noch in jedem Funktionsbereich vorhanden sind und ein Großteil des Wissens sich noch in den Köpfen der Mitarbeiter befindet, können sie weiterhin genutzt oder relativ schnell rekonstruiert werden. Zusammengenommen erlaubt das derzeitige Zwischenstadium in der Informatisierung der Produktion bei einem Ausfall des zentralen Rechners oder der Datenbank noch ein hohes Maß an Improvisation.[35]

Wird künftig die Produktion, wie in unserem Zukunftsbild beschrieben, in den meisten Fällen durch IuK-Systeme geplant, gesteuert, koordiniert und überwacht, erhöht sich die Abhängigkeit von IuK-Technik und das Schadenspotential bei ihrem Ausfall noch be-

32 Butti 122.

33 S. Evens/Orr 12.

34 S. hierzu SARK 124 ff.

35 Im folgenden beziehen wir uns weitgehend auf eine für uns erstellte Expertise von Wengel und Schneider 17 ff., 46.

trächtlich. Die an jedem Arbeitsplatz vorhandenen Computer werden hierarchisch mit einem Zentralrechner vernetzt sein. Auf diesem werden redundanzfrei die Daten für alle Aufgaben einheitlich zur Verfügung stehen. Die betriebswirtschaftlich-planerischen und technischen Funktionen im unmittelbaren Produktionsbereich werden immer stärker integriert. Der Materialdurchsatz wird entsprechend dem Just-in-Time-Konzept optimiert, indem die in der Produktion nachgefragte Menge zeitgenau innerhalb des Betriebs- und zwischen den Unternehmen bereitgestellt wird. Dadurch verringern sich die Umlauf- und Lagerbestände erheblich. Die relativ kleinen Hochregallager werden chaotisch geordnet, von einem Computer verwaltet und automatisch bedient.[36]

Die gesamte Produktion ist erheblich enger gekoppelt und hochgradig komplex. Teure Sicherheitsreserven durch Zeitpuffer, redundante Datenbestände, diversifizierte Produktionsanlagen und größere Lagerbestände werden ersetzt durch zeit-, raum- und kapitalsparende IuK-Technik. Der Preis ist eine hohe Störanfälligkeit des Gesamtsystems. Kleinere Störungen können sich wegen der engen zeitlichen Kopplung des Produktionsprozesses und des komplexen Ineinandergreifens seiner Teile leicht zu größeren Ausfällen kumulieren (Typ I). Kleine Manipulationen an den Produktionsdaten können große Schäden verursachen. Ein geringfügiger Fehler in den CAD-Geometriedaten etwa kann sich automatisch durch das Netz fortpflanzen und in mehreren Produktionsstätten nur Ausschuß verursachen (Multiplikationsschaden - Typ II). Ginge der zentrale, nur einmal vorhandene Daten- oder Programmbestand samt Sicherungskopien verloren, würde der dadurch verursachte Produktionsausfall die Wirtschaftskraft der meisten Unternehmen übersteigen (hoher Einzelschaden - Typ IV). Ein Ausfall der gesamten Produktion wäre auch die Folge, wenn der zentrale Rechner oder die Netzsteuerung ausfallen (Komplexschaden - Typ V)[37] oder wichtige Teilsysteme wegen gleicher Softwarefehler oder -manipulationen gleichzeitig versagen oder fehlerhaft funktionieren (Kopplungsschaden - Typ III).

Die hohe Systemintegration erschwert auch Regenerationsversuche. Aufgrund der Komplexität und engen Kopplung des Systems und der Polarisierung der Mitarbeiterqualifikationen[38] werden Improvisationen kaum mehr möglich sein. Die Maschinen können nur programmgesteuert genutzt werden. Doch selbst wenn die aktuellen Daten und Programme vorlägen, könnte nur kurzfristig weitergearbeitet werden. Denn die erforderlichen Teile könnten nicht dem Lager entnommen werden, weil außer dem Computer niemand weiß, wo sie zu finden sind. Die Diagnose und Behandlung selbst kleiner Fehler kann in einem so komplexen System Tage dauern. Noch aufwendiger kann es sein, gelöschte oder manipulierte Daten zu rekonstruieren und wieder an den aktuellen Produktionsstand heranzuführen. Sind alle Daten und Programme verloren, könnte nur versucht werden,

36 S. hierzu Wengel/Schneider; Scheer 1987, 1988; Wildemann; Klebe/Roth.

37 Sieber 2/122 berichtet von einem Fall, in dem nach einem Ausfall des Rechenzentrums nach 45 Minuten die gesamte Produktion eines großen Automobilunternehmens zusammengebrochen wäre.

38 S. hierzu Wengel/Schneider 29, 33, 35.

das computerintegrierte Produktionssystem noch einmal ganz von vorn aufzubauen. Ein Ausfall eines Rechenzentrums kann eventuell mit entsprechender Zeitverzögerung durch Ersatzrechenzentren abgedeckt werden.

Die durch IuK-Technik mögliche hochintegrierte Produktion und die neuen Logistikkonzepte sind jedoch nicht nur gegenüber IuK-spezifischen Fehlern oder Manipulationen sehr anfällig. Zeitverzögerungen im Verkehr durch höhere Gewalt, durch Unfälle oder durch Ausfall von verkehrssteuernder Technik können relativ schnell Produktionsstops verursachen. Schwerpunktstreiks gegen Zulieferer treffen die belieferten Unternehmen wegen ihrer verkleinerten Lager empfindlich. Das 'Just-in-Time-Konzept' kann ihnen aber noch aus einem weiteren Grund gefährlich werden - wenn nämlich der Computerhersteller selbst aus Kostengründen sein Ersatzteillager drastisch reduziert und fast nur noch auf Bestellung Ersatzteile herstellt. Wer dringend auf Ersatzteile angewiesen ist, kann sich dann nicht mehr darauf verlassen, daß das gesuchte Teil vorrätig ist. In Großbritannien stand 1987 aus diesem Grund die gesamte Produktion eines Unternehmens still, weil eine Steckkarte für 15 Pence nicht zu beschaffen war.[39]

In diesem Zusammenhang ist auf mögliche Folgeschäden hinzuweisen, die auch in allen anderen hier untersuchten Bereichen eintreten könnten.[40] Produktionsausfälle können neben dem unmittelbaren finanziellen Schaden für das Unternehmen auch zu Versorgungsschwierigkeiten bei anderen Unternehmen oder Verbrauchern führen. Dadurch wird das Bild des Unternehmens in der Öffentlichkeit beeinträchtigt und das Vertrauen der Geschäftspartner gestört. Wer kauft noch bei einer Firma, die keine pünktliche Lieferung garantieren kann. Gerade weil die schnelle Reaktion auf Kundenwünsche und die Durchlaufzeiten Ziel der computerintegrierten Fertigung und der neuen Logistikkonzepte ist, werden bereits Pannen und Verzögerungen große Nachteile im Konkurrenzkampf mit sich bringen. Für die entstehenden materiellen und immateriellen Verluste werden letztlich die Arbeitnehmer einzustehen haben.

Waren- und Geldwirtschaft

Warenwirtschaftssysteme sind hochintegrierte, hochkomplexe und eng gekoppelte Systeme zur zeitgenauen Verteilung von Gütern und Lebensmitteln. Sie simulieren die Warenflüsse zeitgleich in ihren Computermodellen und sind daher auf eine automatische Erfassung und Weiterleitung aller Vertriebs-, Verkaufs- und Lagerdaten angewiesen. Da sie allenfalls auf eine zentralisierte Feinsteuerung des Betriebsablaufs zielen, eine Beschleunigung des Warendurchlaufs durch zeitgenaue Planung nach dem Just-in-Time-Konzept anstreben und ihre Lager entsprechend verkleinern und computergesteuert chaotisch ordnen, haben sie vergleichbare Schadensprobleme wie die computerinteg-

39 S. Wong DuD 1987, 353.

40 S. hierzu auch Wong DuD 1987, 498f.; Evens/Orr 38; Wengel/Schneider 47.

rierte Produktion. Insoweit kann auf die bereits erörterten Möglichkeiten IuK-spezifischer Schäden und Schadensfolgen verwiesen werden.

Nach einer 1987 veröffentlichten EG-weiten Umfrage erwarten bereits heute 37% der Manager von Lebensmittelfirmen, daß sie bei einem Ausfall ihrer IuK-Systeme nur noch wenige Stunden effektiv weiterarbeiten könnten.[41] Da künftig sowohl die Integration der Warenwirtschaftssysteme erhöht und Teleshopping zunehmen wird als auch die Verflechtung von Handel und Banken durch Chipkarten und Point-of-Sale fortschreitet, wird die Versorgung der Bevölkerung mit Gütern und Lebensmitteln immer stärker vom zuverlässigen Funktionieren der eingesetzten IuK-Systeme abhängig. Fallen zentrale Rechnerkapazitäten oder die Kommunikationsverbindungen aus, könnten die Komplexschäden (Typ V) zu ernsthaften Versorgungsengpässen führen. Noch schlimmer, weil flächendeckend, wären die zu erwartenden Auswirkungen bei einem zeitgleichen Verlust von Standardprogrammen oder Datenbeständen. In diesem Fall könnte die Vertriebsstruktur der Warenwirtschaft völlig zusammenbrechen.[42]

Die Arbeitsprozesse und Dienstleistungen im *Bankgewerbe* sind in der 'Informationsgesellschaft' vollständig abhängig vom Funktionieren der informations- und kommunikationstechnischen Infrastruktur.[43] Während früher das Funktionieren des Dienstleistungsbetriebs überwiegend von direkter menschlicher Arbeitsleistung und Qualifikation abhing, können künftig Ausfälle oder Störungen der IuK-Systeme zu einem völligen Zusammenbruch aller Banktätigkeiten führen. Schadensverstärkend wirkt dabei, daß durch die Techniknutzung traditionelle Qualifikationen für eine überwiegend manuelle Bearbeitung nicht mehr vermittelt werden. Ohne Technik wird eine Fortführung der Betriebsabläufe und Leistungsprozesse kaum möglich sein. Außerdem könnten die Beschäftigten ohne Computerunterstützung den Geschäftsanfall weder qualitativ noch quantitativ bewältigen. Schauen wir uns die künftigen Abhängigkeiten für den internationalen Zahlungsverkehr, die interne Informationsverarbeitung und den Kundenkontakt etwas näher an.

Bereits heute werden täglich mehr als 1000 Milliarden Mark über den Erdball hin- und hergeschickt. Diese ungeheuren Geldbeträge fließen natürlich nicht in materieller Form. Hart- oder Papiergeld könnte nicht schnell genug transportiert werden. Was fließt, sind Informationen über Geld.[44] Der internationale Austausch dieser Informationen erfolgt überwiegend über ein geschlossenes Netz der 'Society for Worldwide Interbank Financial Telecommunication' (SWIFT).[45]

An dieser Gesellschaft mit Sitz in Brüssel sind derzeit mehr als 1.300 Kreditinstitute in 56 Ländern beteiligt. Diese Institute unterhielten Ende 1987 mehr als 2.400 Anschlüsse. Das SWIFT-Netzwerk

41 S. Evens/Orr 12.

42 S. hierzu auch SARK 122 ff.

43 Wir beziehen uns im folgenden vor allem auf eine für uns erstellte Expertise von Harmsen und Weiß.

44 S. z.B. Brunnstein BdW 1988, 98.

45 S. hierzu näher Jueterbock, Die Bank 1988, 269 ff.

besteht aus zwei Schaltzentralen in Amsterdam (Holland) und Culpepper (USA), in denen gegenwärtig vier bzw. zwei aktive Systeme eingesetzt werden. Jedes System besitzt eine Verarbeitungsleistung von rund 300.000 Nachrichten pro Tag. Die Banken errichten in eigener Verantwortung die Verbindung zu ihrem regionalen Konzentrator über Standleitungen. Die Konzentratoren stellen über internationale Mietleitungen die Verbindung zu den Schaltzentralen her. In der Bundesrepublik stehen für über 170 SWIFT-Teilnehmer zwei Konzentratoren zur Verfügung.

Das bisherige SWIFT-I-System stößt demnächst an seine Leistungsgrenze. Gegenwärtig wird daher ein SWIFT-II-System entwickelt.[46] Der internationale Zahlungsverkehr ist von diesen Computernetzen völlig abhängig. Angesichts der großen Summen und der hohen Zeitsensibilität der Transaktionen würde ein vollständiger oder nur teilweiser Ausfall des SWIFT-Netzes auch nur für Tage zu extrem hohen finanziellen Schäden führen (Komplexschäden - Typ V).

Die interne Informationsverarbeitung ist für alle Geschäftsbereiche von IuK-Technik abhängig. Dies gilt sowohl für das Buchungs- und Rechnungswesen und das Mengengeschäft im Kontokorrent und Sparverkehr als auch zunehmend für die qualifizierten Geschäftsbereiche wie Anlageberatung, Vermögensverwaltung oder Bau- und Geschäftsfinanzierung. Die Informationsverarbeitung erfolgt derzeit in den 391 Rechenzentren der deutschen Kreditwirtschaft. Die Geschäftsbanken betreiben eigene Rechenzentren. Die Sparkassen- und Kreditgenossenschaften haben gemeinsame Großrechenzentren als eigene Dienstleistungsunternehmen gegründet. Einige Beispiele sollen eine Vorstellungen von den Größenordnungen der Informationsverarbeitung vermitteln.

Im genossenschaftlichen Bereich gab es 1980 elf regionale Großrechenzentren. Die FIDUZIA AG beispielsweise betreute mit ihrem Netzwerk und ihrem Rechenzentrum in Karlsruhe 1985 insgesamt 298 Kreditinstitute mit einer Gesamtbilanzsumme von 52,3 Milliarden Mark und mit einem Kontenbestand von 9,8 Millionen Konten. Sie bearbeitete 1985 insgesamt 329,7 Millionen Buchungsposten, davon 95% im Dialog mit den 3.842 Terminals der 1.123 Zweigstellen der angeschlossenen Banken.

Im Sparkassenbereich gab es Ende 1985 zehn Verbandsrechenzentren, an die 497 (84%) von insgesamt 590 Sparkassen angeschlossen waren. Als ein Beispiel sei die 'dvg Datenverarbeitungsgesellschaft' in Hannover genannt. Sie versorgte Ende 1987 71 der 73 niedersächsischen Sparkassen mit einem Anteil von 90% der Bilanzsumme der niedersächsischen Sparkassenorganisation im direkten Verbund mit der Nord/Landesbank und der Bremer Landesbank. 1986 betreute sie 21,3 Millionen Konten. An ihre Rechner waren 7.974 Terminals angeschlossen.

Als Beispiel für die Großbanken sei die Commerzbank erwähnt, die in 793 Geschäftsstellen Ende 1985 2,66 Millionen Kunden betreute. Die Bilanzsumme 1985 betrug 82,6 Milliarden Mark. Vierzehn regionale Rechenzentren und zwei Rechenzentren von Tochtergesellschaften besorgen den Inlandszahlungsverkehr und die örtliche Kontoführung. Noch stärker zentralisiert ist die Datenverarbeitung in der Bank für Gemeinwirtschaft. Sie hat ein Datenfernverarbeitungsnetz aufgebaut, in dem alle 244 inländischen Geschäftsstellen online mit dem zentralen Rechenzentrum in Frankfurt verbunden sind.

46 S. hierzu Jueterbock, Die Bank 6/1988, 329 ff.

Künftig wird der Zentralisierungsgrad wohl weiter zunehmen. Außerdem wird daran gearbeitet, die Gironetze der verschiedenen Bankengruppen sowohl intern wie auch untereinander zu vernetzen. Dies ist eine der Voraussetzungen, um Point-of-Sale-Anwendungen in großem Maßstab sicher realisieren zu können. Beides wird das ohnehin schon hohe Schadenspotential weiter erhöhen.

Nach der bereits erwähnten EG-weiten Umfrage unter Managern schätzen 33% der Bankmanager, daß sie nach Ausfall der Datenverarbeitung ihre Geschäfte nur noch für Stunden weiterführen könnten. Jeder zweite Bankmanager war der Meinung, zumindest noch einige Tage weiterarbeiten zu können.[47] In Zukunft werden für Beratung und Textverarbeitung zwar intelligente Arbeitsplatzcomputer eingesetzt, die auch ohne zentrale Unterstützung noch eine gewisse Zeit arbeiten könnten. Für die überwiegenden Bankdienstleistungen wird jedoch der Zugriff auf zentrale Datensammlungen von vernetzten Terminals nötig sein: Die Kunden sollen ja unabhängig von einer bestimmten Filiale sein und in allen Zweigstellen ihre Bankgeschäfte erledigen können. Gingen die zentralen Datensätze samt Sicherungskopien verloren oder würden diese kopiert, träfe der Komplexschaden (Typ V) alle angeschlossenen Institute. Ebenso weitreichend wäre der Ausfall des Rechenzentrums oder des Netzes aufgrund eines Kopplungsschadens (Typ III) oder hohen Einzelschadens (Typ IV). Da die meisten Geschäftsvorgänge im Dialog mit dem Rechner abgewickelt werden, würde ein längerer Ausfall des Rechenzentrums das Unternehmen handlungsunfähig machen. Der Schaden könnte relativ leicht und in kurzer Frist unternehmensgefährdende Ausmaße erreichen.[48]

Welche Schäden bereits ein Computerfehler hervorrufen kann, zeigt ein Beispiel aus den USA: Die Bank of New York konnte im November 1985 keine Schuldtitel mehr weiterverkaufen, weil bei der Federal Reserve Bank ein Computerfehler aufgetreten war. Da sie ihren Kunden aber bereits die Gegenwerte für die an diesem Tag angenommenen Schuldtitel gutgeschrieben hatte, kam die Bank innerhalb weniger Stunden in beträchtliche Liquiditätsschwierigkeiten. Um eine Zahlungsunfähigkeit zu verhindern, mußte sie bei der US-Zentralbank einen Sonderkredit von 20 Milliarden Dollar aufnehmen.[49]

Der Schaden wird wegen der Verflechtung jedoch kaum auf eine einzelne Bank beschränkt bleiben. Simulationen zeigen zum Beispiel, daß der Ausfall wichtiger US-Bankrechner innerhalb weniger Tage auch verheerende Auswirkungen auf die Geldversorgung Europas hätte.[50]

47 S. Evens/Orr 12.

48 S. hierzu auch Reusch 75f.

49 S. Brunnstein BdW 1988, 98.

50 S. Brunnstein BdW 1988, 99.

Nach Mitteilung der 'California Banker Association' hat eine ihrer Banken vorausgesagt, daß bei einem Ausfall ihres Rechenzentrums die kalifornische Wirtschaft nach drei Tagen, die Wirtschaft der USA nach fünf Tagen und die Weltwirtschaft nach sieben Tagen Schaden erleiden würde.[51]

Aber nicht nur die Banken selbst wären betroffen, sondern auch ihre Kunden. So würden keine Gehalts- oder Rentenzahlungen mehr erfolgen, keine Daueraufträge mehr durchgeführt, keine Schecks mehr eingelöst und keine Kredite oder Sparguthaben mehr ausbezahlt. Viele Verträge würden wegen der fehlenden Finanzierung platzen oder könnten nicht vereinbart werden. Störungen des Bankbetriebs würden sich auf das gesamte Wirtschaftsleben auswirken.[52]

Da die Rechenzentren und Arbeitsplatzcomputer wegen der hohen Vernetzung mit standardisierten Programmen arbeiten, wäre ein gleichzeitiger Verlust der Datenbestände oder ein Ausfall wichtiger Programme in allen Anwendungen noch erheblich gravierender als die bisher genannten Schäden. Er könnte leicht in einem Wirtschaftschaos enden.

Auch in der Kundenbetreuung wird die Abhängigkeit vom zuverlässigen Funktionieren der IuK-Technik ansteigen. Geldausgabeautomaten, Automaten zum 'Auffüllen' von Chipkarten, Point-of-Sale und Btx-Banking, die künftig den Zahlungsverkehr zunehmend bestimmen werden, sind nur relativ sicher möglich, wenn europaweit alle beteiligten Banken und Bankengruppen ein einheitliches Verrechnungs- und Überwachungsverfahren sowie vernetzte Autorisierungs-, Sperr- und Transaktionsdateien einrichten.[53] Dadurch können zwar Schäden wie der folgende weitgehend vermieden werden:

Um die Jahreswende 1985/86 gelang es einem Kölner Computerfreak, bei 192 illegalen Auszahlungen aus Geldausgabeautomaten 78.500 Mark zu erbeuten. Er hatte an einen dieser Automaten vor den Eingabeschlitz für die Magnetstreifenkarte ein Gehäuse von 6,5 cm Tiefe montiert, in dem sich ein Magnetstreifen-Lesegerät mit Sender befand. Wenn arglose Bankkunden ihre Karte in den Leseschlitz steckten, empfing er über Funk nicht nur den kompletten auf der Magnetkarte gespeicherten Datensatz, sondern auch die geheime Identifikationsnummer, die der Kunde über die Tastatur eingegeben hatte. Die Magnetstreifendaten übertrug er dann auf Blankokarten und hob sich Geld ab.[54]

Fällt aber einer der zentralen Rechner oder das Vermittlungsnetz aus, ist regional bzw. national oder gar europaweit weder das Zahlen mit elektronischem Geld noch das Abheben von Papiergeld aus Automaten mehr möglich. Zum einen wären die Banken nicht bereit, ohne automatische Nachprüfung der Deckung das 'Kreditrisiko' zu übernehmen und zum anderen wäre das Volumen der Transaktionen nachträglich nicht zu bewältigen. Da die Infrastruktur für Point-of-Sale oder die Chipkarte aber nur rentabel ist, wenn sich

51 Zit. nach Steinbach DuD 1985, 159.

52 S. hierzu auch SARK 122.

53 S. Harmsen/Weiß 48f., 53f.

54 S. Harmsen/Weiß 46f. mwN.

sehr viele daran beteiligen, könnte durch ein solches Ereignis leicht der Zahlungsverkehr zusammenbrechen.

Wem es als Externem oder Insider gelingt, in ein Banksystem einzudringen und dort Daten zu verändern, kann andere schwer schädigen und sich bereichern. Da statt Papiergeld immer häufiger nur Informationen über Geld ausgetauscht werden, können künftig die Schadenssummen solcher Manipulationen drastisch ansteigen.[55] Beträchtliche finanzielle Schäden könnten einzelne auch erleiden, wenn ihre Chipkarte gefälscht oder auf ihren Namen Telebanking durchgeführt würde. Viel gravierender als die Einzelschäden wäre aber ein Vertrauensverlust in die vollständige Sicherheit des elektronischen Zahlungsverkehrs, wenn massenhafte Betrügereien dieser Art (Kumulationsschäden Typ I) bekannt würden. Viele Kontoinhaber könnten betrügerisch behaupten, bestimmte Transaktionen nicht getätigt zu haben. Der dadurch entstehende sekundäre Kumulationsschaden (Typ I) würde die Kreditinstitute noch erheblich härter treffen als der primäre Schaden durch die Manipulationen selbst.[56]

Der größte Schaden durch den elektronischen Zahlungsverkehr würde jedoch dadurch entstehen, daß die Institutionen, die für die Verwaltung und Ausgabe von kryptographischen Schlüsseln, Chipkarten, Transaktions- und persönlichen Geheimnummern zuständig sind, Schwächen in ihrem Sicherheitssystem aufweisen. Würden Tausende von Schlüsseln, Geheimnummern und dazu gehörende Kontonummern bekannt, könnten nicht nur viele Banken und Kunden Schäden erleiden, sondern auch die Akzeptanz des elektronischen Zahlungsverkehrs würde völlig erschüttert werden. Da es aber keinen ausreichenden Ersatz für diese Form des Geldaustausches mehr gibt, könnten sehr große betriebs- und volkswirtschaftliche Schäden die Folge sein.

Verwaltung

Die hocharbeitsteilige Gesellschaft ist auf eine stetige, wirksame und kalkulierbare Verwaltung existenziell angewiesen. Dabei nehmen die sozialen Funktionen, die auf die Verwaltung übertragen werden, stetig zu und werden gewichtiger. Eine Störung oder der Ausfall von Verwaltungsleistungen können daher leicht große Gesellschaftsgruppen oder die gesamte Gesellschaft schädigen.[57] Parallel zu dieser Entwicklung macht sich die Verwaltung immer mehr vom zuverlässigen und korrekten Funktionieren der IuK-Technik abhängig. Da künftig Verwaltungsinformationen nicht mehr manuell, sondern elektronisch verarbeitet und gespeichert werden, können große Informationssammlungen kopiert, ausgespäht oder manipuliert werden. Gingen sie verloren oder versagten die IuK-

55 Egli 147; s. zu den bereits heute hohen durchschittlichen Schadenssummen in diesem Kapitel unter hoher 'Einzelschaden'.

56 Dies gilt allerdings nur für den Fall, daß sie nicht alle Risiken auf ihre Kunden abgewälzt haben. Ob unter dieser Voraussetzung der elektronische Zahlungsverkehr hohe Akzeptanz erreicht, dürfte zweifelhaft sein.

57 S. hierzu auch Lenk 1982, 328 ff.

Systeme, könnten viele Behörden ihre Verwaltungstätigkeit einstellen. Schadensverstärkend käme hinzu, daß die Beamten gewohnt sind, ihre Arbeit nur technikunterstützt zu erledigen, und die Hintergründe der automatisierten Verwaltungsabläufe oft nicht mehr durchschauen. Im Notfall fehlen dann die Kenntnisse und Fähigkeiten, die Aufgaben auch manuell zu bewältigen.[58] Betrachten wir die spezifische Schadenspotential in der Verwaltung durch die IuK-Technik an einigen Beispielen aus der Sozialversicherung, der Justiz- und Polizeibehörden und der Finanzverwaltung etwas näher.[59]

Die Zusammenfassung vieler Daten in einem System könnte Kumulationsschäden (Typ I) ermöglichen, wenn jemand immer wieder Zugang zu der Datensammlung fände, und zu einem hohen Einzelschaden führen, wenn es jemandem gelänge, komplette Datensätze zu kopieren. Die Verwaltung verarbeitet meist personenbezogene, oft sogar höchst sensible Daten. Würden etwa intime Krankheitsdaten an Dritte (Versicherungen, Arbeitgeber, Arzneimittelverkäufer, Nachbarn) weitergegeben, könnten dem Betroffenen erhebliche Nachteile erwachsen. Noch gravierender könnte es sich für ihn auswirken, wenn die Daten zu Persönlichkeitsprofilen zusammengeführt und zur Verhaltensbeeinflussung des Einzelnen genutzt werden.[60] An kompletten Datensätzen könnten zum Beispiel ausländische Geheimdienste oder Werbeagenturen interessiert sein - diese etwa an den Daten der Finanzämter oder der Meldebehörden, jene zusätzlich an den Sammlungen des Bundeszentralregisters, des Kraftfahrtbundesamtes, des Bundeskriminalamts oder den Daten ihrer Landsleute im Ausländerzentralregister.[61] Würden geheime Daten in IuK- Systemen verarbeitet, gespeichert und übermittelt, wäre es möglich, daß ein einziger gezielter Geheimnisbruch eine so große Menge von Geheiminformationen offenbaren könnte, für die hunderte Spione Jahre gebraucht hätten, sie in einem verteilten Aktensystem auszuspionieren.[62]

Die Verwaltung, einzelne Bürger und die Allgemeinheit können erhebliche Nachteile erleiden, wenn Behördendaten manipuliert werden. Schäden sind denkbar durch gezielte Datenänderungen (hoher Einzelschaden - Typ IV), durch die automatische Vermehrung von Manipulationen (Multiplikationsschaden - Typ II) oder durch die gleichzeitige Veränderung von Programmen oder Datensätzen (Kopplungsschaden - Typ III). Die Folgen solcher Schäden könnten zum einen finanzieller Natur sein, wenn geldwerte Daten in der Finanzverwaltung, in der Sozialversicherung oder in den Behörden der Sozial- und Leistungsverwaltung verändert werden. Zum anderen können sie persönlicher Natur sein, wenn Daten zum Nachteil eines Bürgers verfälscht werden und er plötzlich mit einem erhöhten Steuerbescheid, einer Vorstrafe, einem Haftgesuch oder einem Führerscheinentzug konfrontiert würde. Sie könnten schließlich politischer Natur sein, wenn Basisda-

58 S. hierzu auch SARK 101 ff.

59 S. hierzu näher Wedde Arbeitspapier 9 und 21.

60 S. zu dieser Gefahr z.B. BVerfGE 65, 1 (42f.).

61 S. hierzu näher SARK 108, 117.

62 S. hierzu auch SARK 115.

ten für Planungen verfälscht oder unbrauchbar gemacht würden. Schon allein der Verdacht von Manipulationen, erst recht ihr Nachweis, kann äußerst umständliche und zeitraubende Überprüfungen Tausender Programme und Millionen von Datensätzen erforderlich machen.

Fallen Rechenzentren oder Verwaltungsnetze aus, kann dies zu hohen Einzelschäden (Typ IV) führen, wenn die Datenverarbeitung zentralisiert ist, oder große Komplexschäden (Typ V) verursachen, wenn die Datenverarbeitung verteilt und vernetzt ist. Das Schadenspotential wird erheblich reduziert, wenn autonome Rechnerkapazität auf die einzelnen Ämter verteilt wird, wie dies zum Beispiel in der Finanzverwaltung Nordrhein-Westfalens geplant oder künftig für die Meldeämter zu erwarten ist. Der Netz- oder Rechnerschaden an sich wird immer zeitlich befristet sein - entweder Tage, bis die Notfallvorsorge greift oder bis nach Wochen oder Monaten neue Hardwaresysteme aufgebaut sind. Dort, wo standardisierte Programmsysteme eingesetzt werden - wie etwa in den Ortskrankenkassen -, könnten zwischenzeitlich andere Rechenzentren aushelfen.

Dennoch dürfte in vielen Fällen das Schadensausmaß beträchtlich sein. Die Bundesversicherungsanstalt für Angestellte (BfA) mit ihren rund 16 Millionen Versicherten und 5 Millionen Rentnerkonten und ihren bis zu 500.000 Bearbeitungsfällen pro Tag könnte keinen dieser Fälle mehr bearbeiten. Die Zulassungsbehörden für Kraftfahrzeuge wären nicht mehr wie bisher in der Lage, rund 60.000 mal pro Tag auf die Daten des Kraftfahrtbundesamtes zuzugreifen oder dorthin Veränderungen zu melden.[63] Keine der derzeit täglich 6000 Anfragen und 6500 Mitteilungen an das Bundeszentralregister, das unter anderem eine zentrale Vorstrafendatei führt, könnte mehr bearbeitet werden. Polizeibehörden hätten keinen Zugriff mehr auf den INPOL-Datenbestand beim Bundeskriminalamt.

Erheblich schlimmer träfe die Verwaltung ein Verlust ihrer Datenbestände (hoher Einzelschaden - Typ IV). Unterstellt, die Dateien und Sicherungskopien würden zerstört, wäre sie lahmgelegt. Diese größte Schadensfolge könnte sogar eine dezentralisierte Datenverarbeitung treffen. Sofern nämlich verschiedene Verwaltungsbehörden oder -abteilungen einheitliche Standardsoftware benutzen, um die Datenverarbeitung kompatibel zu halten, wäre ein gleichzeitiger Ausfall aller Systeme (Kopplungsschaden - Typ III) nicht auszuschließen.

Zwar könnten die bereits bewilligten Renten, die von der Bundespost im Auftrag der Versicherungsträger ausgezahlt werden, auch weiterhin geleistet werden. Für die unmittelbar überwiesenen Renten aber fehlt dann die Kontonummer. Neubewilligungen, Versorgungsausgleiche oder Auskünfte müßten ebenfalls unterbleiben. Ohne Daten des Bundeszentralregisters wäre keine ordentliche Strafrechtspflege, ohne die Daten des Kraftfahrtbundesamtes nur noch wenige Zulassungen und keine elektronischen Fahrzeugüberprüfungen mehr möglich. Finanzämter könnten keine Zahlungen mehr einfor-

63 S. hierzu Brinkmann DÖV 1985, Bruns 1985.

dern, aber auch keine Rückerstattungen mehr leisten und die Polizei nur dann noch fahnden, wenn im Jahr 2020 das dickleibige und ewig überholte Fahndungsbuch immer noch existiert.

Eine Rekonstruktion der Datenbestände wäre freilich in vielen Fällen möglich. So könnten zum Beispiel die Träger der Sozialversicherung (Renten-, Kranken-, Arbeitslosen- und Unfallversicherungen) sich relativ leicht gegenseitig unterstützen, da sie künftig über die einheitliche Versicherungsnummer zu einer bundesweiten dezentralen Datenbank zusammenwachsen. Sie sammeln zumindest identische Grunddaten und könnten diese relativ leicht übermitteln. So sammelt die 'Datenstelle für die gesetzliche Rentenversicherung' (DSRV) in Würzburg, die die Vergabe der Versicherungsnummern kontrolliert, die Stammdatensätze aller 45 Millionen Versicherten.[64] Spezifische Verwaltungsdaten - etwa einzelne Gesundheitsleistungen in der Krankenversicherung oder der präzise Versicherungsverlauf über Jahrzehnte hinweg in der Sozialversicherung - wären allerdings nur mit Hilfe der Versicherten oder gar nicht mehr zu rekonstruieren. Die Daten aller hier lebender Ausländer im Ausländerzentralregister, die Eintragungen von über 4 Millionen Bundesbürger im Bundeszentralregister[65] oder die 55 Millionen Datensätze des Kraftfahrtbundesamtes[66] könnten zwar weitgehend rekonstruiert werden, da alle Daten auch noch einmal jeweils vor Ort gespeichert sind. Doch würde eine solche - nie mehr vollständige - Rekonstruktion der Daten Monate dauern, Leistungen an die Bürger verzögern und durch die aufgestaute laufende Arbeit die Verwaltungstätigkeit noch für Jahre belasten.

Am meisten betroffen von einem Datenverlust wären letztendlich die Bürger.[67] Zum einen hätten sie die Nachteile zu tragen, wenn staatliche Bürokratien ihre Aufgabe nicht ausreichend erfüllen können. Zum anderen würde ihnen das Nachweisrisiko aufgebürdet. Immer wenn sie etwas von der Verwaltung wollen - Rentenbescheide, Versicherungs- und Unterstützungsleistungen, Aufenthaltsgenehmigungen, Führungszeugnisse, Führerscheine oder KfZ-Zulassungen -, müßten sie aufwendig und oft vergeblich versuchen, die verschwundenen Daten erneut zu beschaffen und zu belegen.

In der Folge eines solchen Schadensereignisses würde es daher nicht ohne Unruhen und Widerstand abgehen. Die Bürger wären verunsichert und könnten leicht ihr Vertrauen in die Sicherheit der Technik und die mit ihr identifizierte staatliche Verwaltung verlieren.[68] Zweifel an der Zuverlässigkeit der Bürokratie könnten dazu führen, daß Bürger ihre Mitwirkung an technikunterstütztem Verwaltungshandeln verweigern - sie füllen Formulare nicht mehr computerlesbar aus oder geben überhaupt keine Daten mehr über sich preis. Politiker würden versuchen, durch hektische Akte symbolischer Politik Handlungs-

64 S. hierzu Eidenmüller 224 ff.

65 S. hierzu Sawade/Schomburg NJW 1982, 551.

66 S. Roos KR 1987, 321.

67 S. hierzu auch SARK 118.

68 S. hierzu auch SARK 109, 118.

fähigkeit zu demonstrieren. Mißlingt dies, könnten sie sich am Ende verleitet sehen, der Unruhe mit repressiven Mitteln zu begegnen.

Telekommunikation

In einer 'Informationsgesellschaft' kann die gesellschaftskonstituierende Funktion der Telekommunikation gar nicht hoch genug veranschlagt werden. Jenseits der Rufweite wird nahezu jede Kommunikation auf das Funktionieren des ISDN/IBFN angewiesen sein. Da in ihnen alle Kommunikationsformen integriert sind, wäre jeder von einem Ausfall der Telekommunikation existenziell betroffen. Das Ausmaß möglicher Schäden ist dementsprechend extrem hoch. Es sind alle IuK-spezifischen Schäden möglich. Es können Kumulationsschäden (Typ I) entstehen - zum Beispiel durch massenhaftes Hacking - oder Multiplikationsschäden (Typ II) verursacht werden - etwa durch das computerunterstützte gleichzeitige Abhören[69] oder Stören vieler Kommunikationsverbindungen. Wir wollen jedoch im folgenden nicht die vielen Schadensdimensionen einzelner Telekommunikationsdienste[70] erörtern, sondern am Beispiel der Telekommunikation die Katastrophentauglichkeit der 'Informationsgesellschaft' testen. Dabei geht es - wie in dem ganzen Kapitel - nicht um die Wahrscheinlichkeit eines vollständigen oder regionalen Ausfalls der Telekommunikation. Er ist, um seine Folgen abschätzen zu können, vielmehr unterstellt. Möglich wäre er zum einen, wenn wichtige Vermittlungsstellen oder Leitungen koordiniert zerstört werden. Da das ISDN/IBFN nicht mehr mit elektromechanischer, sondern mit programmgesteuerter Vermittlung arbeitet, wäre er zum anderen auch denkbar durch eine Manipulation der Vermittlungssoftware oder durch eine flächendeckende elektromagnetische Beeinflussung.

Einen Vorgeschmack auf ein solches Ereignis haben 100.000 Frankfurter im Februar und im März 1988 erlebt, als jeweils für etwa einen Tag die Fernvermittlungsstelle für den Innenstadtbereich durch einen Softwarefehler ausfiel. "Banker mußten den Devisenhandel einschränken. Werber konnten ihre Grafiken nicht über Telefax wegschicken, der Handelsplatz Frankfurt war an seinem Nerv getroffen."[71] Sogar eine Million Telefonkunden waren betroffen, als 1981 das Netzzentrum Lyons, das alle Telekommunikationsverbindungen vermittelt, für wenige Tage ausfiel.[72]

Wir unterstellen also, daß durch einen Systemschaden (Typ III) nahezu alle Kommunikationsmöglichkeiten schlagartig ausfallen. Der dadurch verursachte Komplexschaden (Typ

69 S. hierzu z.B. den Bericht im Spiegel 7/1985, 134 ff. über die hochsensiblen Wirtschaftsinformationen ganzer Branchen, die zum Beispiel über 'Geisco' von General Electric, das größte kommerzielle Computernetz der Welt, "dickgebündelt" transportiert werden.

70 S. hiezu näher Pordesch Arbeitspapier Nr. 6.

71 FR v. 11.2.1988.

72 S. Kieler Nachrichten v. 11.12.1981.

V) würde sich in einer äußerst *dynamischen Schadensentwicklung* zu sehr vielen hohen Einzelschäden (Typ IV) verbreiten. Unmittelbar betroffen wären alle Nutzungen der Telekommunikation, die zu diesem Zeitpunkt stattfinden oder die zeitkritisch sind. Für Prozeßsteuerungen, Börsengeschäfte, Geldtransfers, Wirtschaftsinformationsdienste, Verkehrssteuerung, medizinische Informationssysteme, Notrufe oder Alarmbereitschaften könnte schon ein kurzfristiger Ausfall verheerend wirken. Alle aktuellen Arbeiten im online-Dialog mit einer entfernten Datensammlung würden zusammenbrechen. In allen Verwaltungsbehörden, Banken, Versicherungen, Handelsunternehmen, gewerblichen Büros oder Krankenhäusern, die über Telekommunikation an Rechenzentren angeschlossen sind oder sich im Datenaustausch mit anderen befinden, könnte nichts mehr bearbeitet werden. Darüber hinaus kann jedoch auch keine private oder geschäftliche Kommunikation mehr stattfinden. Einige der daraus entstehenden Folgen haben wir in unserem Eingangsbeispiel beschrieben. Bei einem flächendeckenden Ausfall käme nur alles noch viel schlimmer. Aufgrund der hohen *gesellschaftlichen Abhängigkeit* von der Telekommunikation entstünden nicht nur viele der Schäden, die wir gerade dargestellt haben. Betroffen wären vielmehr alle Bürger, alle Unternehmen und alle Institutionen und Organisationen. Und alle diese Schäden würden nahezu gleichzeitig eintreten und sich gegenseitig verstärken.

So können keine Waren mehr bestellt, keine Warenauslieferungen mehr disponiert, keine Zulieferungen mehr angefordert und keine Produktions-, Liefer- oder Lagerdaten mehr ausgetauscht werden. In der Folge kann bald nichts mehr produziert, nichts mehr geliefert und nichts mehr verkauft werden. Volle Lager könnten nicht ausliefern, leere Geschäfte nichts bestellen. Der elektronische Zahlungsverkehr fällt aus. Geld ist 'in Hülle und Fülle' vorhanden - es ist nur nicht zu haben. Die Gesellschaft ist noch immer reich und vermögend, und dennoch müssen viele bald Hunger leiden. Der Ausfall von Fernmeß- und Fernwirkdiensten verursacht kalte Räume, verschlossene Türen, unkontrollierte technische Prozesse, unbemerkte Notrufe und einen deutlichen Anstieg von Einbrüchen. Ohne Verkehrsleittechnik bricht in den Städten der Verkehr zusammen ... .

Viele dieser Schäden werden durch die Reaktion auf den Ausfall weiter verstärkt. Erfahrungen mit Katastrophen zeigen, daß in ihrem Verlauf die Informationen und der Kommunikationsbedarf explosionsartig zunehmen.[73] Jeder will sich informieren, was passiert ist, und anderen mitteilen, wie er sich verhalten will und sie sich verhalten sollen. Selbst wenn die Telekommunikation noch nicht völlig ausgefallen ist, wird ihr noch funktionierender Teil unter diesem Ansturm zusammenbrechen.

Während der Schneekatastrophen in Schleswig-Holstein zur Jahreswende 1978/79 und im Februar 1979 kam es zu einem sprunghaften Anstieg des Fernsprechverkehrs, der vielfach den Normalverkehr um das Zehnfache übertraf und zu einem Zusammenbruch des Fernsprechverkehrs führte. Die Behörden haben versucht, ihn zu verhindern, indem sie dessen Wirkungen teilweise vorwegnahmen.

73 S. hierzu z.B. Lagadec 207 ff.; Vester Universitas 1988, 748f.; Perry 115.

Sie haben durch eine 'Katastrophenschaltung' die Telefonnutzung in der Form eingeschränkt, daß zwar noch Telefonate empfangen, aber keine Verbindungen mehr hergestellt werden konnten.[74]

Informationen zu erhalten oder anderen etwas mitteilen, ist nur noch möglich im persönlichen Kontakt. Also werden alle, die ein Informations- oder Kommunikationsbedürfnis haben, sich in ihr Auto setzen und das Verkehrschaos noch weiter steigern. Fehlende Kommunikationsmöglichkeiten behindern aber vor allem das Katastrophenmanagement.[75] Sinnvolle Aktionen zur Behebung der Krise können nur initiiert werden, wenn über sie ausreichende Informationen eintreffen und viele koordinierte Instruktionen zu ihrer Bewältigung verteilt werden können. Beide Voraussetzungen aber fehlen.

Ebenso fehlen die *funktionalen Äquivalente* und die für sie *notwendige Infrastruktur*, um die ausgefallenen gesellschaftlichen Funktionen der Telekommunikation ersetzen zu können.[76] Es gibt zwar durch Vermaschung und Mehrwegeführung eine hohe Redundanz im Telekommunikationsnetz. Aber es gibt kaum Redundanz zu ihm. Die Briefpost ist durch elektronische Kommunikationsformen ausgedünnt worden. Sie kann weder die zeitkritischen Anwendungen ersetzen noch den nun anfallenden Andrang von Briefen bewältigen. Die relativ wenigen Funkverbindungen müssen für die allerwichtigsten Kommunikationsverbindungen reserviert werden. Mitteilungen können nur noch auf kurze Entfernung zu Fuß oder mit dem Fahrrad überbracht werden. Manche werden sich für eine ganz wichtige Botschaft mit einem Motorrad-Boten zu helfen wissen. Allgemeine Verhaltensanweisugnen zur Beruhigung der Bevölkerung werden über Rundfunk verbreitet, können aber nur noch von den Bürgern empfangen werden, die nicht 'voll verkabelt' sind oder die ein mobiles Radio - etwa im Auto - haben.

Auch zur Bewältigung der weiteren Folgen gibt es kaum äquivalenten Ersatz: Es wird sich kaum jemand finden, der die vielen ferngesteuerten und -überwachten Prozesse manuell steuern und persönlich kontrollieren könnte. Das noch vorhandene Papier- und Hartgeld ist völlig unzureichend. Die für die Produktion, den Vertrieb, den Handel und die Verwaltung notwendigen Informationen existieren nur in elektronischer Form. Papierakten werden nur noch selten geführt.

Selbst wenn es den Katastrophenschützern gelingt, relativ rasch eine notdürftige Kommunikations-Infrastruktur für die wichtigsten Bedürfnisse neu aufzubauen, wird diese für viele Zwecke unzulänglich sein. So können sie beispielsweise nicht die in die IuK-Technik inkorporierte Kontrolle mitproduzieren. So würden bestimmte Finanztransaktionen oder Geschäftsmitteilungen eher unterbleiben, auch wenn ein Notbetrieb über Richtfunk eingerichtet wäre. Denn dieser dürfte weder abhörsicher sein noch Verschlüsselungsmöglichkeiten bieten. Für viele Anwendungen fehlen auch die kompatiblen Ersatzgeräte. Insgesamt werden alle feststellen, daß sie sich zu sehr von einer einzigen

74 S. Innenminister des Landes Schleswig-Holstein, 63f.

75 S. Innenminister von Schleswig-Holstein 63.

76 S. hierzu auch SARK 41.

zentralen Infrastruktur abhängig gemacht haben, um diese auch nur notdürftig ersetzen zu können.

Auch besondere *Fähigkeiten und Kenntnisse* einzelner werden die ausgefallenen Strukturen nicht kompensieren können. Sie werden aber dafür entscheidend sein, wie jeder mit der Katastrophe umgeht. Die meisten werden von deren plötzlichem Eintreten überrascht und verwirrt sein. Sie haben sich an die IuK-Systeme gewöhnt. Ihre Kompetenzen sind weitgehend verkümmert zu der einen: den Arbeitsplatzrechner oder das Heimterminal zu bedienen. Keiner weiß sich mehr ohne IuK-Geräte zu helfen, weil die Lebensführung von ihnen abhängig geworden ist. Technik hat die Menschen von vielerlei Mühsal befreit. Sie konnten sich 'höheren Zielen' widmen als denen, mit denen sie nun konfrontiert sind. Der Rückschritt auf eine oder mehrere 'Zivilisationsstufen' vor ISDN fällt umso schwerer, als die meisten ihre Kenntnisse und das Wissen über diese Stufen als überflüssig vergessen oder sich als Jüngere nie angeeignet haben.[77]

Das große Bedürfnis nach Information und seine mangelnde Erfüllung ist der ideale Nährboden für Gerüchte aller Art.[78] Nach den Erfahrungen mit anderen katastrophenähnlichen Situationen, wie nach Tschernobyl, vertraut kaum noch jemand den amtlichen Durchsagen im Rundfunk. Statt sich nach diesen zu richten, versuchen viele, sich auf eigene Faust zu helfen - und durchkreuzen so die Planungen der Behörden.[79] Zuerst werden viele zu Hamsterkäufen losziehen[80] und die Geschäfte leerkaufen. Dann ist aber auch nicht mehr auszuschließen, daß viele, die hier zu kurz kommen, zu Plünderungen verleitet werden, um den Verteilungsproblemen von Waren und Geld auf ihre Weise abzuhelfen. Schon heute demonstrieren die Stromausfälle in amerikanischen Großstädten, daß Massenplünderungen, Vandalismus, Vergewaltigungen und Ausschweifungen keine seltenen Reaktionen auf Katastrophen sind.[81]

Gesellschaft wird durch sinnhafte Kommunikation konstituiert.[82] Je mehr gesellschaftliche Kommunikation auf technische Hilfsmittel angewiesen ist, desto stärkere gesellschaftsauflösende Entwicklungen wären bei einem fortdauernden Ausfall der Technik zu erwarten. Die hochspezialisierte Arbeitsteilung schlägt ohne ihre Infrastruktur um in hochgradige Hilflosigkeit. Die Menschen können einander kaum nützen. Sie werden im Gegenteil füreinander sozial unverläßlich, weil das gewohnte organisatorische Wechselspiel gegenseitiger Leistungen wegfällt.[83] Wird die Telekommunikation nicht bald wieder

77 S. hierzu auch Clausen 72.

78 S. Vester, Universitas 1988, 749.

79 S. hierzu auch Clausen/Dombrowski 299.; obwohl ihnen empfohlen worden war, zu Hause zu bleiben, sind etwa 350.000 Personen rund um Harrisburg nach dem Reaktorversagen in Three Mile Island geflohen; s. zur Gefahr einer Panik auch Roßnagel, Zivilverteidigung 4/1983, 26f.

80 In Harrisburg war nach kurzer Zeit an keiner Tankstelle mehr Treibstoff zu erhalten - s. Berger/Koch, 44 ff.

81 S. hierzu Dombrowski 34; s. auch Clausen 70f.

82 S. hierzu Luhmann 1986, 62 ff.; 1987, 191 ff. - dies gilt in unserem Zusammenhang unabhängig davon, ob eine Gesellschaftstheorie handlungs- oder kommunikationstheoretisch fundiert wird.

83 S. hierzu Clausen 70.

hergestellt, kann am Ende vielleicht nur noch das Militär als einzige eigenständig funktionierende Infrastruktur die gesellschaftsauflösenden Tendenzen aufhalten.[84]

84 S. hierzu Clausen 70.

9. Beherrschbarkeit komplexer Informations- und Kommunikationssysteme?

Wie kann dieses enorme Schadenspotential beherrscht werden? Individuen, Organisationen und die Gesellschaft insgesamt verlassen sich auf die Zuverlässigkeit der Technik. Kann künftig ausgeschlossen werden, daß die technischen Systeme versagen, von denen sie sich abhängig gemacht haben? Können sie sicher sein, daß keine unbeabsichtigten Fehler oder unglücklichen Zufälle eintreten, die bis dahin theoretische Schadensmöglichkeiten plötzlich real werden lassen? Für die Verletzlichkeit der Gesellschaft ist es daher sehr wichtig zu wissen, welche Schadensursachen möglich sind, mit welchem Aufwand sie vermieden oder beherrscht werden können und welches Restrisiko trotz allem bleibt.

Während in den folgenden Kapiteln untersucht werden soll, welche Risiken durch gezielten Mißbrauch der IuK-Techniken entstehen, wird in diesem Kapitel gefragt, aus welchen Gründen Informations- und Kommunikationssysteme *ungewollt* versagen können und in welchem Umfang es möglich ist, Fehler in der Anwendungsumgebung zu beherrschen. Unbeabsichtigte Störungen waren in der Vergangenheit weitaus häufiger als gezielte Aktionen. So verteilt sich das Schadensrisiko für Informationssysteme nach einer Auswertung von IBM[1] auf folgende Faktoren:

Fehler und Unterlassungen	54,0%
Unredliche Mitarbeiter	15,0%
Verstimmte Mitarbeiter	9,8%
Feuer	9,8%
Wasser	7,8%
externe Bedrohung	3,6%

Dennoch soll hier nur ein kurzer Überblick über ungewollte Schadensursachen erfolgen - in der Hauptsache gilt die Untersuchung den Mißbrauchsrisiken. Dies hat neben den bereits oben genannten methodischen[2] eine Reihe sachlicher Gründe. Zum einen ist für die Zukunft zu erwarten, daß die Chancen, die Zuverlässigkeit der IuK-Technik zu verbessern, größer sein werden als die, sie gegen Mißbrauch effektiver zu schützen. Quantitativ dürften auch künftig die unbeabsichtigten Fehler die beabsichtigten Schädigungen bei weitem übertreffen. Qualitativ befürchten wir aber, daß Carl Friedrich von Weizsäcker recht hat, wenn er meint, "man soll in bezug auf die Erzeugung von Gefahren

1 S. Winkler 2.1; ÖVD-Online 10/1986, 36 f.

2 S. Kap. 2.

vom menschlichen Willen viel mehr fürchten als von rein technischen Zufällen".[3] Zum anderen werden die Sicherungsmaßnahmen gegen Mißbrauch die sozialen und politischen Verhältnisse stärker beeinflussen als die Instrumente zur Verbesserung der technischen Zuverlässigkeit. Deshalb erfordern sie im Hinblick auf die technische Gestaltung besondere Aufmerksamkeit.

Zur Begrenzung der Verletzlichkeit durch das Auftreten unbeabsichtigter Ausfälle gibt es zwei unterschiedliche Konzepte: Es kann zum einen versucht werden, unabhängig von einer konkreten Fehlerursache von vornherein das Schadenspotential zu verringern oder in einem Schadensfall dessen Ausmaß zu begrenzen. Zum anderen kann das Ziel von Vorsorgemaßnahmen sein, eine konkrete Fehlerursache zu bekämpfen. Beide Konzepte werden in der Praxis oft kombiniert, hier aber zum besseren Verständnis getrennt dargestellt. Beginnen wir mit den Fehlerquellen und ihren Gegenstrategien.

Durch die Komplexität ihrer Komponenten und ihrer Einsatzumgebung weisen IuK-Systeme in der Praxis eine Fülle von Fehlerquellen auf. Sie sollen hier in vier Kategorien eingeteilt werden: Hardwarefehler sind Fehler in der Konstruktion, in der Herstellung oder beim Betrieb von elektronischen Bauelementen. Softwarefehler umfassen die Unzulänglichkeiten von Programmen. Unter Anwendungsfehlern verstehen wir die Fehlbedienung von IuK-Systemen oder die Fehlinterpretation ihrer Ergebnisse. Systemfehler schließlich fassen solche Ereignisse zusammen, die keiner der genannten Kategorien eindeutig zugeordnet werden können, sondern auf die Einbettung in andere technische Zusammenhänge und die Interaktionen zwischen Mensch, Maschinen und Anwendungsumgebung zurückzuführen sind.

Hardwarefehler

Fehler in der *Produktion* von Mikroprozessoren sind nur selten zu erwarten, da die Entwürfe und Produkte in der Regel sehr genau geprüft werden. Dennoch sind Fehlproduktionen nicht auszuschließen:

Die Firma Intel entdeckte 1987 einen Fehler in einigen ihrer 80388-Mikroprozessoren. Der Fehler führte dazu, daß Zahlen nicht richtig multipliziert wurden. Intel mußte bereits ausgelieferte Prozessoren zurückrufen.[4] Das Pentagon beschwerte sich 1984 über mangelnde Tests mehrerer Hersteller. Deren Chips waren in rund 50 Nachrichten- und Waffensysteme wie U-Boote, Flugzeuge und Raketen eingebaut worden. Ob durch die fehlerhaften Chips Schäden entstanden sind, ist nicht bekannt.[5]

3 V. Weizäcker 24.

4 S. CW v. 15.5.1987, 17.

5 S. CW v. 28.9.1984; 14.12.1984, 2.

In Zukunft ist durch Höchstintegration von Hundert Millionen Schaltungen auf einem fingernagelgroßen Chip und die zunehmende Übernahme von Softwarelösungen auf den Chips mit einer wachsenden Komplexität der Bauteile zu rechnen. Konzeptions- und Produktionsfehler könnten daher wahrscheinlicher werden. Andererseits reduziert die Integration andere Fehlerquellen, weil sie die Zahl der Einzelkomponenten und der notwendigen Verbindungen zwischen ihnen weiter verringert. Außerdem dürften die Testmethoden verbessert werden. Denn die Prüfung der Chips ist wegen der technischen Definitionen ihrer Funktion formalen Verfahren gut zugänglich.

Erheblich häufiger kommt es vor, daß Hardwarekomponenten *im Betrieb* ausfallen. Im Gegensatz zu mechanischen Teilen zeigen diese keine Verschleißerscheinungen, sondern ändern ihren Zustand zu einem zufälligen Zeitpunkt. Zwar kann statistisch ihre mittlere fehlerfreie Zeit (Mean Time Between Failure) abhängig vom Produktions- und Testaufwand berechnet werden. Dem einzelnen Chip ist aber nicht anzusehen, wann dies der Fall sein wird.[6] Bereits Fehler in einer einzigen Komponente eines Kommunikationssystems können sich gravierend auswirken.

Die Übertragungsstrecken des amerikanischen Raketenabwehrsystems NORAD werden durch die permanente Übermittlung von Meldungen geprüft. Im Normalfall teilen diese mit, daß auf der gegnerischen Seite 'Null' Raketenstarts erkannt wurden. Ein Multiplexer meldete allerdings 1980 zweimal durch fehlerhaft erzeugte Bits einen sowjetischen Massenangriff. Das fehlerhafte Funktionieren dieses Übertragungsbausteins hätte fast einen atomaren Gegenschlag ausgelöst.[7]

Die Zuverlässigkeit im Betrieb kann durch Fehlererkennung und Redundanz erhöht werden. Bereits heute werden Systeme angeboten, in denen alle Komponenten mindestens zweimal vorhanden sind. Arbeiten darüber hinaus beispielsweise statt nur einem drei Bauteile parallel, so kann ein vergleichendes System ihre Ergebnisse nach der Mehrheitsregel weiterverarbeiten. Der Ausfall eines Bausteins ist dann unschädlich. Er wird erkannt und der Baustein ersetzt (majority voting). Durch diese Methode können Fehler allerdings erst erkannt werden, wenn eine Komponente ausgefallen ist. Wird einem solchen System zusätzlich noch eine Überwachungs- und Anzeigeeinrichtung beigegeben, die alle Systemkomponenten ständig auf ihre Betriebstüchtigkeit überprüft und auch ihren eigenen Ausfall anzeigt, so können sogar 'schlafende Fehler' rechtzeitig erkannt werden.[8]

Eine weitere Steigerung der Zuverlässigkeit kann erreicht werden, wenn die redundanten Komponenten 'dissimilar' sind, also auf unterschiedliche Weise konstruiert und aus verschiedenen Materialien hergestellt wurden. Zum Beispiel sind in modernen Flugzeugen die Steuerungssysteme elektronisch und die Reservesysteme mechanisch. Im Airbus A320, der keine mechanische Steuerung mehr hat, sind die redundanten Steuer-

6 S. hierzu Gottschlich 44 ff.

7 S. Däubler u.a. FR-Dokumentation v. 13./14./15.2.1983; Bläsius/Siekmann, Informatik Spektrum 1987, 32 mwN.

8 S. hierzu Gottschlich 56; Gottschlich/Zerbst ELT 1983, 153 ff.

computer aus verschiedenen Mikroprozessoren aufgebaut, die einen inkompatiblen Maschinencode haben.[9]

In Übertragungsleitungen kann es aus unterschiedlichen Gründen zu Kurzzeitunterbrechungen in der Größe von Millisekunden kommen. Je höher künftig die Geschwindigkeit der Datenübertragung (z.B. 1 Million bit/s und mehr) sein werden, desto eher verfälschen oder 'verschlucken' selbst kürzeste Unterbrechungen gleich mehrere Bits. Durch Redundanz und Kodierung können auch Übertragungsfehler erkannt und korrigiert werden. Es werden zu jeder Nachricht eine gewisse Zahl von Zusatzbits beigefügt, aus deren Vergleich mit der empfangenen Nachricht erkannt werden kann, ob diese mit der abgesandten identisch ist. Im Fehlerfall wird die Übermittlung so oft wiederholt, bis die Nachricht korrekt angekommen ist (parity bit).[10]

Verfahren dieser Art können die Fehlerwahrscheinlichkeit erheblich reduzieren.[11] Sie sind allerdings mit einem hohen Kostenaufwand verbunden: Jedes Gerät muß mehrfach bereitgestellt werden. In dem gleichen Maß, in dem die Komponenten vervielfacht werden, müssen sie auch repariert oder ersetzt werden, da sie unabhängig voneinander ausfallen. Die Sicherheit steigt jedoch nicht im gleichen Verhältnis wie der Kostenaufwand. Durch Verdoppelung einer Komponente wird die Zuverlässigkeit nur um den Faktor 1,5 erhöht.[12] Mit entsprechendem Aufwand kann die Zuverlässigkeit also zwar sehr hoch getrieben werden. In den meisten Fällen düften jedoch finanzielle Erwägungen bescheidenere Sicherheitsansprüche erzwingen.

Für die Zuverlässigkeit von Prozeßsteuerungen sind neben den Steuerungsrechnern auch Anzeigen, Sensoren und Aktoren entscheidend. Ist ihre Funktionstüchtigkeit gestört, kann dies mitunter gravierende Folgen haben.

Für die Kernschmelze in dem Reaktor Three Mile Island 1979 war unter anderem das Versagen eines Sicherheitsventils verantwortlich. Dies wurde jedoch von der Betriebsmannschaft nicht erkannt, weil die (kurz zuvor aus Sicherheitsgründen neu eingebaute) zuständige Kontrollanzeige einen Fehler aufwies und die Stellung des Ventils nicht anzeigte. Die Mitarbeiter im Kontrollraum ergriffen daraufhin die falschen Maßnahmen.[13]

In einer Boeing 747 der Lufthansa führte 1974 in Nairobi eine Fehlanzeige auf dem Instrumentenpult des Bordingenieurs dazu, daß die Nasenklappen an den Flügeln während des Starts trotz gegenteiliger Meldung nicht ausgefahren waren. Dem Flugzeug fehlte beim Start der notwendige Auftrieb und es stürzte ab. Bei dem Unfall waren 50 Tote zu beklagen.[14]

9 S. Gottschlich 57.

10 S. hierzu Gottschlich 52 ff.; Weck 104 ff.

11 Durch Ausfallerkennung kann die mittlere Ausfallzeit um etwa den Faktor 18 erhöht werden - s. Gottschlich 59.

12 S. Gottschlich 48 ff.

13 S. Perrow 41 ff.

14 S. Gottschlich 69 ff.

Auch die Mikroperipherik kann wie die Prozessoren durch Redundanz und Fehlererkennung mit entsprechendem Aufwand erheblich sicherer gemacht werden. Allerdings zeigt das Beispiel aus Three Mile Island, daß zusätzliche Sicherungskomponenten nicht immer die Zuverlässigkeit des Systems erhöhen. Gerade bei großen Systemen können zusätzliche Kontrolleinrichtungen die Komplexität so sehr erhöhen, daß dadurch ihr partieller Zuverlässigkeitsbeitrag aufgehoben wird. Sie können nicht nur die Überschaubarkeit für die Bediener einschränken - sie sind vielmehr auch selbst immer wieder Fehlerquellen und führen besonders dann zu großen Risiken, wenn der Bediener einem falschen Signal vertraut.[15]

Computersysteme benötigen in der Regel spezifische Umgebungsbedingungen. Temperatur und Luftfeuchtigkeit dürfen nur gering schwanken. Die Räume müssen staubarm und die Stromversorgung muß stabil sein. Bereits Abweichungen von mehr als 10% der Netzspannung oder mehr als 1 Hz Frequenzänderung können in Computern zu Fehlern führen.[16] Alle diese Umgebungsbedingungen können in der Praxis nicht immer gewährleistet werden.

Nach einem starken Regen im August 1986 führte ein Wassereinbruch im Fernmeldehochhaus der Deutschen Bundespost in Frankfurt zu einem Ausfall der Klimaanlage. Da in der Folge der Vermittlungsknoten des Datennetzes ausfiel, konnten im Raum Frankfurt für mehrere Stunden keine Telexverbindungen mehr vermittelt werden.[17]

"Als die ersten Exemplare des neuen Airbus A320 ausgeliefert wurden, gab es u.a. in nordafrikanischen Ländern morgens beim Start Verzögerungen. Das Flugzeug hatte während der überaus kalten Nacht im Freien gestanden. Dann wurde es schlagartig der Hitze der aufsteigenden afrikanischen Sonne ausgesetzt. Ergebnis: Die Elektronik war den krassen Temperaturwechseln nicht gewachsen und ließ sich weder checken noch programmieren."[18]

Durch besser geplante Baumaßnahmen, durch Vervielfachung der erforderlichen Geräte und durch eine gut organisierte Wartung kann eine höhere Ausfallsicherheit erreicht werden.[19] Die Stromversorgung ist auch bei Ausfall eines Stromerzeugers oder einer Stromtrasse durch das Verbundnetz gesichert. Problematisch bleiben nur die Störung einer einfach ausgelegten Anschlußleitung oder Stromschwankungen.

Nachdem 1986 in der Nähe des Atomkraftwerks Krümmel ein Strommast zerstört worden war, fielen in Hamburg durch das kurzfristige Umschalten der Stromversorgung auf andere Kraftwerke in etlichen Unternehmen Tausende von Computersystemen aus.[20]

15 S. hierzu Perrow 42, 118 ff.

16 S. Wannow 708.

17 S. FR v. 23.8.1986.

18 S. Zeit v. 2.7.1988, 41.

19 S. hierzu näher Breuer 75 ff.

20 S. Spiegel 44/1986, 74.

Gegen solche Stromschwankungen kann eine unterbrechungsfreie Stromversorgung schützen, die ständig die Stromspannung mißt und Schwankungen durch Akkus oder Batterien ausgleicht. Wer sich dies nicht leisten kann, könnte zumindest dafür sorgen, daß die Schwankung der Stromversorgung solange gepuffert wird, bis eine Sicherungskopie des Arbeitsspeichers gezogen ist. Damit gehen wenigstens die Daten nicht verloren und es kann weitergearbeitet werden, sobald die Netzspannung wieder stabil ist. Ein Ausfall der Stromversorgung kann aufgefangen werden durch eine Notstromversorgung über Batterien oder Notstromdiesel.[21] Aber auch die können versagen.

Am 3.9.1987 brach das elektrische System des Frankfurter Flughafens zusammen und die Radarelektronik der Fluglotsen fiel schlagartig aus. Eine reibungslose Umschaltung auf die Notstromversorgung scheiterte, weil ein Notstromaggregat in Reparatur war und das zweite wegen Altersschwäche nicht ansprang. Erst nach zwei Minuten konnte die Stromversorgung wieder hergestellt werden.[22]

Die Notstromversorgung wird in der Regel nur einen eingeschränkten Notbetrieb ermöglichen und wegen ihrer hohen Kosten nur bei sehr wenigen besonders wichtigen Systemen vorgesehen werden können. Ist jedoch auch die gesamte Umgebung von dem Stromausfall betroffen, nützt die isolierte Stromversorgung für den Rechner möglicherweise auch nicht viel.

Als im Juli 1977 nach einem Blitzeinschlag in New York das Stromnetz zusammenbrach, konnten zwar viele Datenverarbeitungen durch Notstromaggregate gesichert werden. Da diese aber nur die Rechner mit Strom versorgen konnten, fuhr kein Lift, lief kein Wasser, ging keine Klimaanlage und funktionierte keine Ampel. Die meisten Computersysteme wurden deshalb erst nach der Reparatur der Stromversorgung zwei Tage später wieder in Betrieb genommen.[23]

Es können jedoch immer wieder neue Umweltbedingungen auftreten, die die Zuverlässigkeit von Computersystemen stören. So hat zum Beispiel die elektronische Umweltverschmutzung eine Reihe neuer Probleme verursacht.

Vermutlich sind mehrere Tornados der Luftwaffe 1984 abgestürzt, weil ihre Bordcomputer von der Sendestrahlung eines Rundfunksenders gestört wurden.[24] In den USA sind seit 1980 mindestens 5 'Black-Hawk'-Hubschrauber abgestürzt, weil sie von Funkwellen beeinträchtigt wurden.[25] In Japan soll das Radar des Flughafens von Osaka durch den benachbarten Fernsehsender gestört worden

21 S. hierzu näher Breuer 95 ff.

22 S. Spiegel 14/1988, 30.

23 S. Norman 170; s. zu einem ähnlichen Fall in New York 1981 Kieler Nachrichten v. 11.9.1981.

24 S. Kieler Nachrichten v. 19.7.1984.

25 S. EMC-Technology 1-2/1988, 3; The Chicago Tribune v. 11.11.1987 - nach Risk Digest v. 15.11.1987, Nr. 5.58, 1.

sein.[26] In den USA wurden in mehreren Fällen Herzschrittmacher durch Mikrowellen oder durch die Diebstahlsicherung in einem Kaufhaus umprogrammiert.[27] 1986 wurden 42 Personen verletzt, als wegen unbekannter elektromagnetischer Wellen zwei Wagen einer Berg- und Talbahn zusammenstießen. Ein Telespiel, dessen Störstrahlen die Kommunikation einer Eisenbahnschaltstelle beeinflußten, bewirkte, daß sich während der Fahrt die Türen eines Zuges öffneten.[28] Im Juli 1982 wurden in mehreren Rechenzentren in Sidney Daten falsch gespeichert und Magnetplatten falsch abgelesen, weil der Radarstrahl der Luftraumkontrolle in den Rechnern elektromagnetische Felder hoher Feldstärke erzeugt hatte.[29]

Auch andere nicht beachtete Umwelteinflüsse können IuK-Systeme stören: Kurzschlüsse in der Telefonverbindung zwischen Teneriffa und Gran Canaria wurden mehrfach von Haien verursacht, die ein unter Wasser verlegtes Glasfaserkabel mit ihren scharfen Zähnen traktierten.[30] Ein B-52-Bomber, der 1971 im Tiefflug direkt auf einen Atomreaktor am Michigansee zuflog, stürzte plötzlich ab, prallte von der Wasseroberfläche des Sees ab und explodierte in einem Feuerball. Vermutlich war er in eine radioaktive Gaswolke aus dem Schornstein der Anlage geraten, wodurch seine elektronische Steuerung gestört wurde. Zwei Sekunden später wäre die Maschine direkt auf die Reaktorkuppel geprallt.[31]

Ein Sachverständiger kommentiert diese Entwicklung so: "Die Probleme der elektromagnetischen Verträglichkeit nehmen trotz steter Bemühung laufend zu und es ist anzunehmen, daß sie in nicht allzu ferner Zukunft die Weiterentwicklung der Funktechnik bestimmen werden."[32]

Softwarefehler

Programme sind unzuverlässig. Dies ist eine der ersten Erfahrungen, die jeder Anwender von Softwaresystemen macht. Fehlerhafte Software kann verbessert werden. Es wäre daher zu erwarten, daß Systeme mit ihrem Alter reifen und zuverlässiger werden. Dies ist für komplexe Systeme jedoch nicht gewährleistet. Vielmehr führen die vielfältigen Abhängigkeiten einzelner Komponenten untereinander zu kontraproduktiven Effekten bei der Fehlerbeseitigung. Sneed geht von 1,5% bis 2,5% fehlerhafter Anweisungen in größeren Systemen aus. Dabei liegt der Anteil der Spezifikations- und Entwurfsfehler bei jeweils 30% und der von Kodierungsfehlern bei etwa 40%. Von den Entwicklungsfehlern sind nach Abschluß der Implementierungsphase ein Drittel noch nicht entdeckt.[33] In großen

26 S. The Guardian v. 26.5.1987 - nach Risk Digest v. 28.5.1987, Nr. 4.91, 2.

27 Software Engeneering Notes der ACM, 2/1985, 6.

28 S. The Guardian v. 26.5.1987- zit. nach Risk Digest Nr. 4.91 v. 28.5.197, 2.

29 S. Hennings/Müller ÖVD-Online 3/1985, 75f.

30 S. FR v. 23.8.1986.

31 S. Webb 194f.

32 Dvorak NTZ 1987, 432 ff.

33 S. Sneed 169.

Softwaresystemen muß daher mit einer entsprechenden Anzahl latenter Fehler gerechnet werden. Aus dem 40 Millionen Zeichen umfassenden Code des öffentlichen US-Telefonsystems wurden im Lauf der Zeit 40.000 Fehler eliminiert.[34] Schauen wir uns die einzelnen Fehlerkategorien und die Verbesserungsmöglichkeiten an.

Mit der *Spezifikation* wird festgelegt, was das künftige System können soll. Sie entscheidet über den Wirklichkeitsausschnitt, der in einem Programm abgebildet werden soll. Ist dieses Wirklichkeitsmodell unvollständig, erfüllt das Programm zwar seine Aufgabe, kann aber zu Katastrophen in seiner Anwendungsumgebung führen.

Im Falklandkrieg schoß Argentinien mit Exocet-Raketen auf den britischen Zerstörer 'Sheffield'. Da in der Spezifikation des Abwehrsystems nicht vorgesehen war, daß Raketen des eigenen Typs gegen eigene Schiffe anfliegen, hat das System funktionsgerecht nicht auf diesen Beschuß reagiert.[35] Weniger gravierend war der Spezifikationsfehler im System des Verbandes deutscher Rentenversicherungsträger. Da nicht berücksichtigt worden war, daß es Menschen mit gleichem Vor- und Zunamen geben kann, wurden bei Routineprüfungen die Konten gleicher Namensträger automatisch zu einem zusammengefaßt.[36] Mail-Dienste fielen in den USA aus, weil im elektronischen Kalender der 29. Februar im Schaltjahr 1988 vergessen worden war.[37] Weil Systementwickler nicht berücksichtigt haben, daß Kinder auf Klobrillen klettern können, kam in Frankreich ein Kind zu Tode. Nachdem keine Bodenbelastung mehr angezeigt wurde, setzte sich das vollautomatische Reinigungssystem des Toilettenhäuschens in Betrieb. Durch das Umdrehen der Toilettenschüssel wurde das Mädchen gewürgt und durch die Wasserspülung wurden ihre Lungen mit Wasser gefüllt.[38]

Formalere Methoden der Spezifikation können helfen, die erforderliche Vollständigkeit zu erreichen, sie aber nicht gewährleisten. Welche Modelle der Wirklichkeit einem Programm zugrundegelegt werden und welche Parameter in dieses eingehen, entscheidet der Auftraggeber oder sein beauftragter Entwickler. Ob die Anforderungen an ein Programm fehlerfrei sind, ist eine praktische, von den jeweiligen Interessen abhängige Frage. Selbst wenn von den Kosten ganz abgesehen werden könnte, löst eine voneinander unabhängige Mehrfachentwicklung (n-version-programming) die Probleme nicht. Verschiedene Entwickler machen signifikant häufig die gleichen Spezifikationsfehler.[39] Das Problem einer vollständigen Spezifikation ist prinzipiell nicht zu lösen.[40]

Im *Programmentwurf* werden anhand der Spezifikation eine Systemstruktur entwickelt und die Aufgaben von Teilsystemen bestimmt. Werden in dieser Phase Wechselwirkungen zwischen verschiedenen Komponenten übersehen oder falsch beschrieben, kann

34 S. Valk 19.

35 S. z.B. Zeit v. 18.3.1988. 37.

36 Bundesbeauftragter für den Datenschutz 1981, 58f.

37 S. Brunnstein CW v. 8.4.1988, 12f.

38 Zeitungsnotiz ohne Quellenangabe aus dem 'Katastrophenarchiv' der Universität Kiel.

39 Parnas et al. 4.

40 S. z.B. Bläsius/Siekmann, Informatik Spektrum 1987, 31.

dies im Betrieb zu einem Fehlverhalten des Systems führen. Für die Zukunft versprechen jedoch die automatische Unterstützung des Entwurfs auf der Basis der Spezifikation und moderne Strukturierungsverfahren für die Software deutliche Verbesserungen.[41] Ob diese den Komplexitätszuwachs künftiger Systeme auffangen werden, läßt sich nicht entscheiden.

Trotz größter subjektiver Sorgfalt sind Fehler in der *Implementierung* von Programmen nicht zu vermeiden.

Die USA verloren eine Venussonde, weil im Steuerungsprogramm ein Punkt statt eines Kommas stand. Eine Milliarde Mark war ins Universum verschwunden.[42] Umgekehrt, weil sich an der Stelle eines Kommas ein Punkt befand, entschwanden zwei Mariner-Sonden ins Weltall.[43]

Neue Programmierwerkzeuge und -umgebungen sowie begleitende Tests bereits auf den einzelnen Entwicklungsstufen versprechen künftig Qualitätssteigerungen. Durch Systematisierung des Implementationsprozesses sollen etwa zwei Drittel der Fehler vermieden werden.[44] Im Betrieb können Programmierfehler durch Redundanz aufgefangen werden. Arbeiten mehrere Anlagen simultan, kann bei abweichendem Verhalten eines Programms der Ablauf nach Mehrheitsentscheidung fortgeführt werden, ohne daß dieser Fehler irgendwelche Auswirkungen hätte. Spezifikations- und Entwurfsfehler schlagen sich jedoch in allen Programmen gleichermaßen nieder. Insgesamt ist unter Informatikern unumstritten, daß heute und in absehbarer Zukunft Programme nicht fehlerfrei oder innerhalb einer vorgegebenen Fehlerwahrscheinlichkeit erstellt werden können.[45]

Ein wichtiges Hilfsmittel zur Fehlersuche ist daher das *Testen*. Tests können allerdings nur das Vorhandensein von Fehlern, nicht die Fehlerlosigkeit zeigen.[46] Im Gegensatz zu analoger Steuerungslogik, für die zwischen zwei Testergebnissen interpoliert wird, kann für ein Programm nicht davon ausgegangen werden, daß eine Funktion den dazwischenliegenden Wertebereich korrekt abdeckt. Zeigt der analoge Zeiger einer Temperaturanzeige bei 15° auf den richtigen Wert und rutscht er bei 20° fünf Einheiten nach oben, kann der Tester davon ausgehen, daß die Anzeige auch 16, 17, 18 und 19° richtig anzeigt. Bei einer programmgesteuerten Anzeige kann er dies nicht. Denn für jeden dieser Werte könnte ein Fehler einprogrammiert sein. Deshalb gibt es für Programme eine unübersehbare Menge von Testfällen, die praktisch nicht erprobt werden können. Verschärft wird dieses Problem noch dadurch, daß Softwarefunktionen um ein Vielfaches komplexer

41 S. Sneed 170.

42 S. Zeit 44/1985, 25; WAZ v. 7.11.1987.

43 S. Valk 19.

44 S. Sneed 170.

45 S. hierzu Bläsius/Siekmann, Informatik Spektrum 1987, 31.

46 S. hierzu z.B. Parnas 4.

sein können als Analogsteuerungen.[47] Sogenannte statistische Testverfahren können deshalb zwar zur Korrektur von Fehlern führen, aber keineswegs die Korrektheit des Produkts garantieren.

Künftige Deduktionssysteme werden nach dem Jahr 2000 die Suche nach Fehlern in Entwurf und Implementierung weiter verbessern. Soweit die Anforderungen formal beschrieben werden können, sind sie in der Lage, für nicht allzu komplexe Programme die Übereinstimmung mit der Spezifikation automatisch zu überprüfen, ohne allerdings eine vollständige Korrektheit gewährleisten zu können. Da sie überdies kosten- und zeitintensiv sind, werden viele Systeme auch in Zukunft unvollständig geprüft sein.

Durch die *Wartung* können erkannte Softwarefehler verbessert werden. Wie mangelhaft Programme in der Regel sind, zeigt, daß heute 40 bis 80% der Gesamtkosten eines Systems auf die 'Wartung', also Fehlerbehebung nach Fertigstellung und Auslieferung an den Kunden entfallen. Die Fehlerrate ist so hoch, obwohl der Herstellungsprozeß eine intensive Testphase mit vielleicht 20% Entwicklungskosten enthält.[48] Oft führt jedoch die Suche nach Fehlern zu keinem Ergebnis. Dies wird insbesondere künftig ein Problem werden, wenn viele Programme eines Systems parallel arbeiten und miteinander kommunizieren. Fehler können dann oft nicht gezielt reproduziert werden. Eine systematische Suche der Fehlerquelle ist unmöglich.[49]

Sind Fehler erkannt, zeigt die Erfahrung, daß bei deren Korrektur oft neue Fehler entstehen. Die Struktur von Software-Systemen kann sich durch Erweiterungen und Anpassungen stark verändern. Die Zahl der Konstrukte für die Behandlung von Ausnahmen wächst und die Systematik sowie deren Verständnis nehmen ab.[50] Die Unübersichtlichkeit großer Programme führt dann zu 'fehlerhaften' Korrekturen. Nach Aussagen von Experten nimmt ab einem bestimmten Alter eines Softwareprodukts die Fehlerrate mit jeder neuen Korrektur oder Ergänzung zu.[51]

Ein Beispiel hierfür ist eine Korrektur einer speicherprogrammierten Vermittlungsstelle im Wiener Telefonnetz. Die Software wurde bei Wartungsarbeiten um ein Programmteil ergänzt. Wenig später konnten die Telefonkunden mit den Anfangsziffern 51, 52 und 53 nicht mehr telefonieren.[52]

In Utah/USA staunte ein 17 Jahre alter Schüler nicht schlecht, als er statt der erwarteten Steuerrückzahlung von 14,39 Dollar einen Scheck über 800.014,39 Dollar erhielt. Da er eine ehrliche Seele war, informierte er die Steuerverwaltung. Nachforschungen ergaben, daß bei Korrekturarbeiten von der Systemkonsole aus ein Teil der Postleitzahl in das Feld für die Auszahlungen gerutscht war. Die

47 S. Parnas et al. 3; Bilinski 23.

48 S. Valk 21; Bilinski 23.

49 S. Valk 20f.

50 S. Valk 22; Bilinski 23.

51 S. Bilinski 23; Brunnstein CW v. 8.4.1988, 12; Ebbinghaus 238. Übereinstimmende Aussagen auf dem Projekt-Workshop am 13./14.10.1987.

52 S. CW v. 27.6.1986, 40.

Ausgabekontrolle hatte den Fehler nicht entdeckt, weil diese durch den unmittelbaren Eingriff von der Systemkonsole aus umgangen worden war.[53]

Anwendungsfehler

Informations- und Kommunikationssysteme arbeiten nicht für sich. Sie sind letztlich immer in übergreifende Mensch-Maschine-Systeme eingebunden. Als zusätzliche Fehlerquelle sind daher menschliche Handlungen zu berücksichtigen. Sind Hard- und Softwaresysteme in Betrieb genommen, können sie fehlerhaft angewendet, also unsachgemäß behandelt, mit falschen Daten 'gefüttert' oder in ihren Ergebnissen fehlerhaft interpretiert werden. Menschen sind bisweilen müde, alkoholisiert, bekifft, abgelenkt, vergeßlich, leichtgläubig oder fahrlässig. Sie können daher in der Bedienung eines Geräts unnötige Schritte hinzufügen, notwendige Schritte auslassen oder eine Schrittfolge verändern. Bedienungsfehler, die auf solchen menschlichen Schwächen beruhen, sind nicht zu vermeiden, solange Menschen Maschinen bedienen. Um ihre Zuverlässigkeit und damit die des gesamten Mensch-Maschine- Systems zu erhöhen, kann jedoch versucht werden, sie noch stärker den Erfordernissen der Technik anzupassen. So können sie zum einen durch bessere Bezahlung, ein höheres Sozialprestige oder ein günstiges Arbeitsklima stärker motiviert werden. Zum anderen kann eine schärfere Überwachung der Arbeit die Zuverlässigkeit erhöhen. Und drittens können Menschen mit den geforderten Eigenschaften durch ausgefeilte psychologische und motorische Tests ausgewählt werden.[54]

Anwendungsfehler sind aber oft auch darauf zurückzuführen, daß die Bediener unzureichend informiert, schlecht ausgebildet, überfordert oder gestreßt sind.[55] Gerade die zunehmende Automatisierung von Arbeitsprozessen weist dem Menschen vor allem Kontroll- und Überwachungsaufgaben zu. Langen Phasen der Monotonie folgen plötzliche Alarmsituationen mit einer Fülle von Informationen, die unter hohem Zeitdruck zu einer Entscheidung verarbeitet werden müssen, von der hohe Sachwerte oder gar Menschenleben abhängen.[56] Unter solchen Streßbedingungen sind Fehlentscheidungen nicht zu vermeiden. Diese als 'menschliches Versagen, zu interpretieren, verkennt meist den richtigen Ausgangspunkt der Beurteilung. Nicht der Mensch muß sich technikgerecht verhalten: vielmehr muß die Technik menschengerecht sein. Verleitet die Ausgestaltung eines Systems zu Fehlern, so versagt die Technik, weil sie unzureichend den menschlichen Verhaltensbedingungen angepaßt ist. Anwendungsfehler dieser Art sind eigentlich auf ein Versagen der Organisation zurückzuführen. Arbeitsstreß, Hektik, Monotonie

53 S. Norman 101.

54 S. hierzu z.B. Husseiny/Zeinab Atomkernenergie/Kerntechnik 1980, 115 ff.; Roßnagel 1983, 224 ff.; ders. 1987, 137 ff. mwN.

55 S. z.B. Bilinski 24.

56 S. z.B. Wiener 165; Dhillon 184; Bilinski 24.

könnten in vielen Fällen durch eine andere Arbeitsorganisation reduziert oder beseitigt werden.

Falsch eingegebene oder interpretierte Werte können - wie andere Fehler in komplexen Systemen auch - verheerende Folgen haben. Sie können unmittelbar Schäden verursachen, etwa falsche Eingabedaten, die zu einer Fehlsteuerung einer Chemieanlage führen. Sie können aber auch in Systemen 'schlafen' und erst zu einem späteren Zeitpunkt eine Fehlentscheidung herbeiführen. Eine fehlerhafte Regel oder ein falsches Datum in der Wissensbasis eines Expertensystems wird selbst ein Experte oft nicht erkennen und sein Handeln auf die erhaltene Information gründen. Eingabefehler sind dann besonders gravierend, wenn der Anwender den Informationsverarbeitungsprozeß nicht nachvollziehen kann und daher seinem Ergebnis vertrauen muß.

Am 9.11.1979 wurden im amerikanischen Raketenabwehrsystem NORAD Anzeichen eines Massenangriffs sowjetischer Raketen dadurch verursacht, daß durch einen Bedienungsfehler Programmteile zum Testen des Systems in Angriffssimulationen in das Computersystem eingeführt wurden. Der Bedienermannschaft war dies nicht sofort erkennbar.[57]

Eine verbesserte Ergonomie der Systeme und eine Verbesserung der Arbeitsorganisation können Fehler verringern, aber nicht ausschließen. Den 'Störfaktor Mensch' durch vollständige Automation ausschließen zu wollen[58], wäre illusionär und würde in eine im wörtlichen Sinne unmenschliche Welt führen. Ihn durch mehr Automatisierung zu reduzieren, bringt zwar Sicherheitsvorteile bei Routinetätigkeiten, weil diese nur einmal mit großer Sorgfalt in einem Programm festgelegt und nicht jedes Mal mit neuer Versagensmöglichkeit von Menschen erbracht werden müssen. In bestimmten Systemen sind automatische Regulierungen notwendig, weil die Zeitspanne für Reaktionen des Bedienungspersonals zu kurz ist.

In den meisten Fällen dürfte eine weitergehende Automatisierung jedoch der falsche Weg sein. Da auch automatische Steuerungen im Rahmen eines komplexen Mensch-Maschine-Systems bleiben, beruht die Sicherheit des Gesamtsystems mit wachsender Zuverlässigkeit der Technik zunehmend auf dem Faktor Mensch - und nicht umgekehrt.[59] Denn der Mensch ist entweder für die Konstruktion des Systems, für dessen Kontrolle und Wartung, für die Bereitstellung der Primärdaten, für die Interpretation der Ergebnisse oder deren Umsetzung oder für alle diese Aufgaben zugleich verantwortlich. Alle nicht routinemäßigen Tätigkeiten, die automatisiert werden, unterliegen jedoch der besonderen Gefahr unvollständiger Spezifikationen. Im Ausnahmefall muß dann der Mensch einspringen und unter Zeitdruck handeln. Aufgrund der fortgeschrittenen Computerisierung fehlt ihm jedoch zunehmend das Gesamtverständnis für komplexe Systeme, und er muß auf

57 Däubler u.a. FR-Dokumentation v. 13./14./15.2.1983.

58 Davon träumt zumindest für das Rechenzentrum Bschorr 142 ff.

59 Nach Aussagen der NASA wäre bis heute noch kein Raumflug erfolgreich beendet worden, wenn nicht die Besatzung an irgendeinem Punkt eingegriffen hätte. Vgl. Wiener 164.

der Grundlage nicht nachvollziehbarer automatisch erzeugter Informationen agieren - zwei schlechte Voraussetzungen für Eingriffe in unvorhergesehenen Situationen.[60]

Aus unbekanntem Grund kam es bei einigen Kontrollanzeigen des Atomkraftwerks Crystal River in Florida 1980 zu einem Kurzschluß. Er verfälschte einige Meßdaten im Kontrollsystem, unter anderen die wichtige Anzeige für die Temperatur des Kühlmittels. Der Computer 'glaubte', das Kühlmittel würde zu kalt, und beschleunigte die Kernreaktionen im Reaktor. Es kam zu einer Überhitzung des Reaktorkerns und zu einer automatischen Schnellabschaltung. Der Computer war dadurch vermutlich 'verwirrt' und gab die richtige Anordnung, das Entlastungsventil zu öffnen, und die falsche, es offenzulassen. Dieser 'Fehler' des Computers führte zu einem Druckabfall im Reaktor, der die Hochdruckeinspeisung auslöste. Über das offene Ventil entleerten sich 200.000 Liter radioaktives Wasser in den Reaktor. Nach einigen Minuten bemerkte ein Operateur den Fehler und schloß das Ventil von Hand. Zum Glück hatte er sich nicht an die Vorschrift gehalten, dem Computer die Störfallreaktion zu überlassen.[61]

Systemfehler

An sich harmlose Komponenten-, Programm- oder Anwendungsfehler können in komplexen Systemen zu unerwarteten und während eines kritischen Zeitraums auch undurchschaubaren Wechselwirkungen führen. Ist dann das System auch noch eng gekoppelt, dann können solche Fehlerinteraktionen große Schäden verursachen.[62]

Als im Februar 1988 die Fernvermittlungsstelle für die Frankfurter Innenstadt ausfiel und über 100.000 Teilnehmer für etliche Stunden von der Außenwelt abgeschnitten waren, vermuteten die Fernmeldetechniker als Ursache einen Softwarefehler. Offenbar war eine Sicherung, die dafür sorgt, daß das System bei Überlastung nicht 'abstürzt', selbst überlastet. Wie es jedoch dazu kam, darüber konnten sie nur spekulieren: "Da ist möglicherweise gerade eine Werbeaktion oder ein Preisausschreiben gelaufen, bei dem tausende von Leuten zum Hörer griffen." Mindestens zwei weitere Störfaktoren, etwa ein Leitungsausfall, müssen aber dazugekommen sein. Dieser Störfall war im Sicherungsprogramm nicht vorgesehen. Vier Wochen nach diesem "einmaligen" Störfall führte die gleiche Panne zu einem erneuten Totalausfall der Vermittlungsstelle.[63]

Informations- und Kommunikationssysteme sind zum einen komplex, weil sie mit Hunderttausenden oder Millionen von Anweisungen arbeiten, die nicht linear angeordnet, sondern vielfältig vernetzt sind. Sie sind zum anderen komplex, weil sie durch ihre Pro-

60 S. hierzu Perrow 164; Wiener 164f.

61 S. Perrow 119.

62 S. hierzu näher Perrow 17 ff., 105 ff.; Bläsius/Siekmann, Informatik Spektrum 1987, 30; Bilinski 25f.

63 S. hierzu FR v. 11., 12., 13. 2. und v. 5.3.1988.

grammsteuerung wesentlich komplexere Steuerungsaufgaben übernehmen können als konventionelle Steuerungssysteme[64] und auf das vielfältigste Zusammenwirken technischer Geräte angewiesen sind. Sie erhöhen dadurch zugleich die Komplexität ihrer Anwendungsumgebung.

Die *innere Komplexität* großer Softwareprogramme ergibt sich aus den vielfältigen Funktionen, die einzelne Basisprogramme wie Betriebssysteme, Compiler oder Editoren haben. Auf diesen Basisprogrammen bauen weitere Anwendungsprogramme auf, etwa Datenbanken, die wiederum die Grundlage spezieller Auswertungsprogramme sein können.[65] Durch die Vernetzung all dieser Einzelprogramme entsteht ein neues "Ganzes", das in vielfältiger Weise Handlungen vollführt, die in komplexer Weise voneinander abhängen. Jeder Teil des Systems kann mit anderen Teilen in Interaktion treten. Deshalb können triviale Ereignisse in nicht-trivialen Systemen unvorhersehbare Ereignisketten auslösen. Für den einzelnen Fehler haben die Entwickler meist Vorsorge getroffen, auf ihn sind die Bediener in der Regel gefaßt. Daß jedoch mehrere Fehler gleichzeitig auftreten, hat niemand vorhergesehen und geplant. Ihre komplexen Interaktionen sind den Bedienern im kritischen Zeitraum meist undurchschaubar.[66]

Dies hat seinen Grund auch darin, daß in großen Softwareprojekten gleichzeitig mehrere hundert Entwickler an einem Produkt arbeiten. Dazu muß das Projekt in einzelne Programmteile aufgegliedert und eine oft schier unüberschaubare Zahl von Schnittstellen definiert und angepaßt werden. Gerade diese Schnittstellen sind sehr fehlerträchtig, weil viele Details für selbstverständlich gehalten und daher überlesen oder gar nicht erst dokumentiert werden. Schnittstellendefinitionen sind praktisch nie vollständig. Hinzu kommt, daß während der Projektdurchführung eine Fülle von Änderungen erforderlich wird, die immer wieder zu neuen Anpassungen der Arbeitsorganisation zwingen. Der Informationsfluß und die Koordination zwischen den Beteiligten können oft nicht den vielfältigen Wechselbeziehungen der einzelnen Programmteile gerecht werden und sind daher eine ständige Quelle für Fehler.[67] In der Folge kommt es dann im Zusammenspiel zwischen den einzelnen Programmteilen zu Schwierigkeiten:

So führte der Einsatz eines unzureichend abgestimmten Spezialprogramms, das von einem anderen Hersteller stammte als die Basisprogramme, bei der drittgrößten australischen Bank dazu, daß unautorisierte Benutzer auf Dateien zugreifen konnten, ohne daß sich der Vorgang später nachvollziehen ließ. Möglicherweise konnten sogar die Passwortlisten eingesehen werden.[68]

Zu finanziellen Verlusten in Millionenhöhe führe ein neues Computerprogramm zur Steuerung der Geldautomaten bei einer anderen australischen Bank (Westpac). Nach einer Woche stellte die Bank jede Auszahlung an ihren Automaten ein. Die neue Software hatte Geld in unbegrenzter Höhe

64 S. hierzu Parnas et al. 2.

65 S. näher Jahl 249 ff.

66 S. hierzu Perrow 21 ff., 42, 71, 105 ff.

67 S. hierzu Ebbinghaus 232 ff; Valk 21f.

68 S. CW v. 13.3.1987.

ausgezahlt - über die Tagesbegrenzung von 200$ hinaus, auch wenn das Konto ungedeckt war. Dies sprach sich herum und viele Kunden nutzten die 'neuen Kreditmöglichkeiten'.[69]

Durch ähnliche Koordinationsfehler war die Sicherheitslücke im VAX-Betriebssystem (VMS) der DEC-Rechner entstanden, die es 1987 Hackern ermöglichte, über das DEC-Net in das SPAN (Space Physics Analysis Network) zu gelangen und 136 weitere Großcomputer zu 'besuchen'.[70]

Programmsysteme werden in Zukunft aber nicht einfacher, sondern komplexer. Viele Unzulänglichkeiten heutiger Programme haben ihren Grund darin, daß deren Modelle die Komplexität der Wirklichkeit unzureichend abbilden. Zu viele Fälle, zu viele Zusammenhänge, zu viele Unwägbarkeiten erfordern Eingrenzungen des abzubildenden Wirklichkeitsbereichs.[71] Um die Modelle immer realitätsgerechter zu konzipieren, werden immer komplexere Programmsysteme entwickelt. Je komplexer Systeme jedoch sind, desto fehleranfälliger werden sie.[72]

Größe, Heterogenität und Komplexität eines Systems aus Computer-, Nachrichtentechnik und Mikroperipherik erlauben es grundsätzlich nicht, sehr kleine Fehlerraten zu erreichen. Die ständige Beteiligung von Menschen im Betrieb sowie laufende Anpassungen und Umstrukturierungen - bedingt durch neue Techniken und neue Spezifikationen - ergeben weiterhin grundsätzlich ein hohes Fehlerniveau.[73]

Es genügt daher in der Regel nicht, nur die Korrektheit eines Programms zu testen oder zu beweisen. Notwendig ist vielmehr, das gesamte System zu validieren. Doch dies ist um Potenzen schwieriger als die schon oben angesprochene Validierung einzelner Programme. Man kann also letztlich nie sicher sein, ob es funktioniert.

Die *äußere Komplexität* und Fehleranfälligkeit entsteht dadurch, daß parallel zur Wirklichkeit physischer Abläufe in den IuK- Systemen zusätzlich regelnde, mit der Umwelt vielfältigst interagierende Handlungssysteme aufgebaut werden. Versagt nur eine von Millionen Komponenten, können große Schäden entstehen, wenn dadurch die Umgebungsbedingungen im Systemmodell nicht mehr ausreichend repräsentiert sind, wenn dadurch die Umgebung in unvorhergesehener Weise auf das System einwirkt oder wenn dadurch komplexe Wechselwirkungen ausgelöst werden.

Der Einsatz von Informationstechnik verringert also die Linearität von Prozessen und erhöht deren Komplexität. Sie ergänzt bestehende Prozeßabläufe - etwa in einer Chemieanlage oder einer Fabrik - um eine parallele, regelnde und deshalb mit anderen Teilfunktionen interagierende Struktur. Sie verfügt über eine kaum überschaubare Anzahl von Schnittstellen mit der Wirklichkeit. Versagt eine von diesen, kann es zu automatischen oder menschlichen Fehlinterpretationen oder -reaktionen kommen. Ein defekter Sensor,

69 S. Sydney Morning Herald v. 5.6.1987 und The Canberra Times v. 16.6.1987 zit. nach Risk Digest Nr. 5.3 v. 16.6.1987, 2 und 4.

70 S. hierzu Wernery, Datenschutz-Berater 9/1987, 1 ff; Tempo 10/1987, 100 ff.

71 S. hierzu Gaede/ Hammer/Pordesch, 72 ff.

72 S. Perrow 107.

73 S. Däubler u.a. FR-Dokumentation v. 13./14./15.2.1983.

ein durchgebranntes Birnchen, ein verklemmtes Relais können genau die falsche Reaktion eines Systems oder eines Menschen auslösen. Der Bildschirm zeigt dann das Modell einer Wirklichkeit, die einer Kontrolle bereits entglitten ist. Da aber die unmittelbare Beobachtung durch die künstliche Wirklichkeit des Computermodells ersetzt wird[74], kann der Bediener leicht falsch handeln, gerade weil er diese 'korrekt' interpretiert. Perrow spricht in diesem Zusammenhang von "erzwungenen Fehlinterpretationen".[75] Gerade die gefährlichen unerwarteten Interaktionen von Fehlern müssen ihm verborgen bleiben, da sie in der künstlichen Welt des Modells nicht vorgesehen sind.

Ein gleiches gilt für die Reaktionen in einem Störfall. Zur Beherrschung komplexer Abläufe wird in der Modellierung von der Wirklichkeit abstrahiert oder Steuerungsmechanismen automatisiert. Der Operateur kann das Verhalten des Gesamtsystems nicht mehr direkt beobachten und oft nur noch auf komplexe Komponentensysteme, nicht mehr aber auf einzelne Teile steuernd zugreifen. Folgerichtig erhöht sich im Störfall das Risiko unerwarteter Interaktionen.[76]

Die Einbettung von Steuerungssystemen in ihre Arbeitsumgebung kann zu nicht vorhersehbaren Wechselwirkungen führen.

In Japan sind von 1980 bis 1987 zehn Menschen von Industrierobotern 'ermordet' worden. In vier Fällen war eine Fehlbedienung die Ursache. In den sechs anderen setzten sie sich jedoch aus ungeklärten Ursachen in Bewegung und begannen zu 'arbeiten'. In zahlreichen weiteren Fällen fügten sie Menschen zum Teil schwere Verletzungen zu. Weltweit wird die Zahl von Todesfällen durch Roboter auf zwanzig geschätzt. Es wird vermutet, daß signal-verfälschende elektromagnetische Wellen in den Fabrikhallen Steuerungsmechanismen der Roboter in Gang setzten. Diese Wellen könnten etwa von den Impulsen stammen, die beim Ein- und Ausschalten von Aufzügen oder schweren Maschinen auftreten können. Aber exakte Beweise gibt es nicht, weil die genau gleichen Bedingungen wie zum Zeitpunkt des Unfalls nicht wieder hergestellt werden können.[77]

Räumliche Nähe und eng gekoppelte Funktionszusammenhänge können selbst das Auswechseln einfacher Hardwareteile in hochentwickelten komplexen Systemen zu Risiken werden lassen.

Aufgrund enger räumlicher Nähe und unvorhergesehener Interaktionen verursachte zum Beispiel 1959 eine 300-Watt-Glühbirne im Pentagon einen Schwelbrand, der sich auf das gesamte Rechenzentrum ausbreitete und drei Zentraleinheiten zerstörte. Es entstand ein Schaden von über sechs Millionen Dollar.[78]

1978 fiel einem Arbeiter eine Glühbirne aus der Hand, die er an der Schalttafel des Atomkraftwerks Rancho Secco in Kalifornien auswechseln sollte. Sie verursachte bei einigen Meßfühlern und

74 S. hierzu näher Gaede/Hammer/Pordesch 41 ff.

75 Perrow 41 ff.

76 S. hierzu auch Perrow 165.

77 S. FR v. 22.5.1987; TAZ v. 22.5.1987.

78 S. Norman 68.

Schaltungen einen Kurzschluß. Zum Glück war die Steuerung der Schnellabschaltung nicht betroffen und der Reaktor schaltete automatisch ab. Aber durch den Ausfall der Meßfühler konnte die Bedienungsmannschaft den Zustand der Anlage nicht überprüfen. Es kam daher zu einer rapiden Abkühlung der Reaktorkerns, die bei anhaltend hohem Druck die Innenwände des Druckbehälters starken Schrumpfungsspannungen aussetzte. Hätte die Anlage nicht erst zwei, sondern bereits zehn und mehr Jahre unter Vollast gearbeitet, dann hätte dadurch der Druckbehälter platzen können.[79]

Selbst völlig korrektes Verhalten kann, wenn es in unvorhergesehener Form zusammenwirkt, zu Systemversagen führen:

45.000 Fernsehzuschauer griffen im Rahmen der Sendung "Wetten, daß..?" im September 1987 nahezu gleichzeitig zum Telefon, um über das Teledialog-System die beste Wette zu küren. Durch diese Überbelastung brach in der ganzen Bundesrepublik für sieben Minuten das Telefonnetz einschließlich Küstenfunk und Autotelefon zusammen.[80] Zum 'Börsen-Crash' am 'Schwarzen Montag', dem 19.10.1987, hat wesentlich beigetragen, daß die Makler durch moderne Telekommunikationssysteme weltweit 'real time' informiert waren und überwiegend ähnliche Börsenprogramme benutzten, die bei Unterschreiten bestimmter Börsenwerte automatisch ganze Aktienpakete auf dem elektronischen Markt zum Verkauf freigaben. Da alle das gleiche taten, kam es aufgrund sich selbst verstärkender Effekte zu dem rasanten Kurssturz.[81]

Nicht einzelne - möglicherweise mit großen Anstrengungen vermeidbare - Fehler, sondern hohe Komplexität und enge Kopplung führen als Eigenschaften großer Informations- und Kommunikationssysteme zwangsläufig zu Unfällen.[82] Es genügt daher für schadensträchtige Systeme nicht, einzelne Programme oder - soweit dies überhaupt möglich ist - das gesamte Softwaresystem zu testen. Erforderlich wäre vielmehr ein vollständiger Test des Zusammenspiels von Software, Hardware und Bedienungsmannschaften. Aber gerade die Steuerungs- und Alarmprogramme von Hochrisikosystemen können oft nicht unter Ernstfallbedingungen getestet werden. Denn die Kosten eines realistischen Versuchs wären unbezahlbar. So wäre es um keinen Preis zu verantworten, nur zu Testzwecken eine besonders hohe Überlastung des Luftverkehrs, eine Kernschmelze in einem Atomkraftwerk, einen Kühlausfall in einem hochgiftigen und energiereichen chemischen Prozeß oder einen 'Krieg der Sterne' herbeizuführen.

Die Gefahr von Systemfehlern kann dann reduziert werden, wenn es gelingt, all jene Ereignisse auszuschließen oder zu verringern, die unvorhergesehene Interaktionen auslösen können. Die vorrangige Sicherheitsstrategie besteht also darin, das System um zusätzliche Komponenten zu erweitern und es noch komplexer zu konstruieren. Zusätzliche Redundanz erhöht aber gleichzeitig erneut die Möglichkeit von Systemfehlern. Es ist

79 S. Perrow 72.

80 S. Weser-Kurier v. 28.9.1987.

81 S. hierzu z.B. Zeit v. 30.10.1987, 25.

82 S. zu solchen Systemfehlern näher Perrow 18, 107 ff.

daher fraglich, ob diese Sicherheitsstrategie tatsächlich zu einer Reduzierung von Systemfehlern führen kann.[83]

Maßnahmen zur Schadensbegrenzung

Wenn die Fehlermöglichkeiten von IuK-Systemen so groß und vielfältig sind, gewinnen Konzepte zur Schadensvermeidung oder -verminderung zunehmend an Bedeutung. Ein Beitrag zur Schadensbegrenzung kann von der *Systemgestaltung* ausgehen, die zu dezentralen, linearen und entkoppelten Prozessen führt.[84] In Zukunft werden Konzepte für 'verteilte Systeme' zur Verfügung stehen, die es erlauben, Rechnerkapazität sowie Daten und Programme auf mehrere Stellen zu verteilen. Führt dies lediglich zu einer Dekonzentration, durch die zwar der Zugriff auf Daten und Programme über ausgelagerte Terminals möglich ist, die Verarbeitung aber zentraler erfolgt, dann leistet die Verteilung keinen Beitrag zur Sicherheit, sondern erhöht nur die Komplexität des Systems. Anders bei einer Dezentralisierung[85]: Imdem sie die Steuerungsprozesse auf niedrigere und kleinere Einheiten überträgt und diese im Störfall voneinander entkoppelt, ermöglicht sie eine Reduzierung des Schadenspotentials.[86] Allerdings erschwert eine dezentrale und komplexe Organisation im Notfall das Umschalten auf Ersatzrechenzentren.

In der Prozeßsteuerung kann Dezentralisierung zu einem 'Line Replacable Unit-Konzept' umgesetzt werden, nach dem in modularem Systemaufbau räumlich verteilte Mikrorechner den Prozeß steuern. Das Ausfallrisiko wird dadurch auf die gesamte Regelanlage verteilt. Fällt ein Rechner aus, führt dies nicht mehr zum Ausfall des Gesamtsystems, sondern nur zu einer Minderung der Systemleistung. Gleichzeitig ist dieses verteilte System wartungsfreundlich und erhöht durch kurze Reparaturzeiten die Systemverfügbarkeit.[87]

Redundanz kann nicht nur helfen, den Ausfall eines Systems zu verhindern, sondern auch dazu beitragen, den Schaden nach einem Ausfall zu begrenzen. Bereits heute verfügen manche Großanwender über zwei oder mehr Anlagen, zwischen denen nach einem Ausfall die Software ausgetauscht werden kann. Häufig werden Unterstützungsverträge mit Partnerrechenzentren geschlossen, die eine gleiche Hardware benutzen. Spezialisierte Unternehmen bieten 'kalte' *Ausweichrechenzentren* an. Sie verpflichten sich, nach einem Ausfall innerhalb von Stunden Container-Rechenzentren zum Einsatzort zu bringen, die einen Notbetrieb ermöglichen. Die uneingeschränkte Wiederaufnahme des EDV-Betriebs soll mit Hilfe mobiler EDV-Gebäude bereits innerhalb von drei bis sechs Tagen

83 S. hierzu näher Perrow 108 mwN.

84 S. hierzu SARK 135 und Perrow 111, 125.

85 S. zum Unterschied zwischen Dezentralisierung und Dekonzentration Nora/Minc 65 ff.

86 S. hierzu auch SARK 132.

87 S. hierzu Gottschlich 27.

möglich sein. Ein anderes Konzept ist das der 'warmen' Ersatzrechenzentren. Nach diesem hält ein Back-up-Unternehmen an einem zentralen Ort ständig ein Rechenzentrum in Betrieb, in das Vertragspartner im Notfall innerhalb von Stunden ihre Datenverarbeitung hinverlagern können. Dort kann die Hardware des jeweiligen Anwenders simuliert werden, so daß keine Anpassungsprobleme entstehen.[88] Im Jahr 2000 dürften solche Ausweichreserven für die besonders sicherheitsempfindlichen und im Jahr 2020 wohl für die meisten Anwendungen zur Verfügung stehen. Voraussetzung für einen Weiterbetrieb ist in allen diesen Konzepten, daß noch eine gewisse Infrastruktur erhalten ist und die Daten und Programme noch zur Verfügung stehen.

Dies zu gewährleisten, ist die Aufgabe von *Sicherungskopien*. Auch wenn der Arbeitsspeicher oder Bänder und Platten zerstört werden, kann auf die Duplikate zurückgegriffen werden. Selbst wenn nur jeden Tag oder jede Woche eine Sicherungskopie erstellt wird, können die verlorenen aktuellen Daten weitgehend mit 'Recovery-Programmen' rekonstruiert werden. Und da es künftig möglich sein wird, auch große Datenmengen in kurzer Zeit ohne physischen Transport zu Partnerrechenzentren auszulagern und auf optischen Speichermedien abzulegen, könnten sich diese Intervalle noch verkürzen. Daten können dann nur noch durch ein unglückliches Zusammenwirken von mehreren Fehlern verlorengehen.

Bei 'Oldsmobile' fiel 1987 infolge eines technischen Fehlers die 70-Megabyte-Platte aus, auf der die Design-Daten des 1990 Olds-Modells gespeichert waren. Da jedoch die Daten routinemäßig auf Magnetbändern gesichert wurden, sah niemand einen Grund zur Panik. Dies änderte sich, als sich herausstellte, daß auch die Back-up-Bänder aufgrund eines technischen Versagens leer waren. Alle Design-Arbeiten mußten erneut ausgeführt werden.[89]

Im Telekommunikationssystem wird schadensmindernde Redundanz durch *Vermaschung* des Netzes erreicht. Beim Ausfall einer Übertragungsleitung oder einer Vermittlungsstelle kann die Kommunikation über Umwegschaltungen an den ausgefallenen Komponenten vorbei aufrecht erhalten werden. Möglicherweise führt die Überlastung der Ausweichstrecken oder -vermittlungsstellen zu Komforteinbußen. Außerdem ergeben sich weitere Sicherheitsreserven aus dem Grundsatz der *Zwei-Wege- und Zwei-Medienführung* im Fernnetz. Nach diesem sollen für alle wichtigen Fernstrecken sowohl Richtfunk- als auch Kabelverbindungen bestehen und für beide Medien jeweils zwei getrennte Trassen benutzt werden.[90]

Aus der Erkenntnis heraus, daß große Softwaresysteme nicht fehlerfrei sind, wurde das Konzept der *fehlertoleranten Systeme* entwickelt, die beim Auftreten eines Hardware-, Software- oder Anwendungsfehlers das umgebende Gesamtsystem in einem stabilen,

88 S. hierzu z.B. Breuer 256 ff.; Abel/Schmölz 50f.; Heidinger/Andrich 77 ff.; Steinbach DuD 1985, 159 ff.; Harmsen/Weiß 69 ff.

89 S. Car and Driver 6/7/1987, 34 - zit. nach Risk-Digest 5.11 v. 10.7.1987, 2.

90 S. hierzu ausführlich Pordesch, Arbeitspapier 6.

schadensarmen Zustand halten. Eine besondere Ausprägung dieses Konzepts ist das 'fail-safe'-Prinzip, nachdem eine Komponente oder ein System immer nur 'nach der sicheren Seite hin' ausfallen kann: Eine Ampel schaltet sich auf 'rot', ein Zug wird abgebremst, eine Maschine gestoppt. Bei Ausfall einer wichtigen Komponente wird das Gesamtsystem in einen energieminimalen, unschädlichen Zustand überführt oder zumindest in seiner Leistung auf das notwendige Minimum gedrosselt (Degradation).[91]

Schadensbegrenzende Konzepte dieser Art können, sofern sie konsequent verwirklicht werden, das Risiko eines Fehlers beträchtlich reduzieren. Wie der 'Oldsmobile'-Fall gezeigt hat, lassen sich allerdings nicht alle Risiken ausschließen: Ausweichrechenzentren nützen nichts, wenn die Daten verloren sind oder sie aufgrund eines anderen Notfalls schon belegt sind; Vermaschung und Mehrwegeführung helfen nicht weiter, wenn in den Vermittlungssystemen der gleiche Softwarefehler steckt; 'fail-safe' oder Degradation können keine Wirkung mehr entfalten, wenn die Steuerungssysteme eines Flugzeuges oder eines leistungsexkursiven chemischen oder radioaktiven Prozesses ausfallen - um nur einige Beispiele anzudeuten

Beherrschbarkeit durch IuK-Technik?

Für den Versuch einer zusammenfassenden Wertung empfiehlt es sich, bekannte und daher kalkulierbare Risiken und die Risiken der Unkenntnis und des unbe kanntenEreignisses ebenso zu unterscheiden wie das künftige Zuverlässigkeitspotential und das real zu erwartende Zuverlässigkeitsniveau.[92]

Das Risiko *bekannter Fehlermöglichkeiten* könnte in Zukunft deutlich vermindert werden. Mit dem entsprechenden finanziellen und organisatorischen Aufwand ließe sich die Fehlerwahrscheinlichkeit von Hardwaresystemen sehr und die von Softwaresystemen beträchtlich reduzieren. Trotzdem auftretende Ausfälle könnten durch schadensmindernde Konzepte in den meisten Fällen aufgefangen werden. Während also künftig unterschiedlich wirksame Instrumente zu erwarten sind, die die Verletzlichkeit der Gesellschaft verringern, wirken andere Entwicklungen erhöhend. Die IuK-Technik wird erheblich breiter und intensiver genutzt werden, so daß verbleibende Fehlermöglichkeiten sich öfter realisieren. Gleichzeitig werden die Systeme komplexer und dadurch fehleranfälliger.[93] Insbesondere komplexe Programme werden auch künftig Fehler aufweisen, die nicht zuverlässig unter bestimmte Grenzwerte gedrückt werden können. Wie wir gesehen haben, verbindet sich dieser Trend mit der Erzeugung höherer Schadenspotentiale im Einzelfall und einem 'Verbrauch' von Sicherheitsgewinnen durch risikofreudige Leistungssteigerun-

91 S. hierzu Gottschlich 57.

92 S. hierzu Roßnagel 1984b, 209 ff.

93 S. hierzu z.B. Abel/Schmölz 9.

gen. Ob durch diese Entwicklungstrends die möglichen Fortschritte in der Zuverlässigkeit aufgebraucht werden, ist nicht zu entscheiden.

In der Praxis wird jedoch die Frage entscheidend, für welche Anwendungen welcher Sicherheitsstandard als angemessen und finanziell vertretbar erachtet wird. Zu vermuten ist, daß die 'unproduktiven' Sicherheitsaufwendungen vorrangig dann getroffen werden, wenn der Zugewinn an Sicherheit zugleich die Verfügbarkeit des eigenen Systems und damit die Produktivität erhöht und wenn die sicherheitstechnischen Eingriffe ohne nennenswerte Kosten möglich sind.[94] Die Sicherheit von Anwendungen zu erhöhen, die bei einem Ausfall nicht den Anwender selbst, sondern vorwiegend Dritte schädigen, entspricht nicht dessen Eigeninteresse. Ohne bindende Sicherheitsvorschriften wird er auf die Schwerfälligkeit des Beweis- und Haftungsrechts vertrauen und eine gute Versicherung vorziehen. Je mehr Risikoerzeugung und Risikobetroffenheit auseinanderfallen, desto risikobereiter dürfte der IuK-Anwender werden. Ebenso dürften die Sicherheitskosten für die Kommunikationsinfrastruktur nur in dem Maße aufgebracht werden, wie dies zur Akzeptanz bei den Kunden erforderlich ist. Jede darüber hinausgehende Maßnahme zur Erhöhung der Zuverlässigkeit schlägt sich in den Gebühren nieder und wirkt sich auf die Wettbewerbsfähigkeit der kommunizierenden Unternehmen aus. In der Praxis werden daher wenigen sehr zuverlässigen Systemen, die für die Anwender besonders sicherheitsrelevant sind, viele Systeme gegenüberstehen, deren Zuverlässigkeit ungenügend ist.

Die Risiken der *Unkenntnis* und der *unbekannten Ereignisse* werden mit der ansteigenden Komplexität der Systeme zunehmen. Wie die Beispiele aus der Vergangenheit erwarten lassen, werden auch künftig unvorhergesehene Umwelteinflüsse, unvollständige Modelle, unzureichende Spezifikationen und Möglichkeiten unvorhersehbarer Interaktionen von Fehlern in hochkomplexen Systemen unkalkulierbare Risiken hervorrufen. Da diese Risiken unbekannt sind, ist auch nicht abschätzbar, welche Bedeutung sie insbesondere für Hochrisikosysteme erlangen können. Jedenfalls kann niemand ausschließen, daß die Steuerungscomputer von Hochgeschwindigkeitszügen oder Verkehrsflugzeugen durch 'elektronische Emissionen' gestört werden, daß die Modelle oder die Wissensbasen medizinischer Expertensysteme unvollständig sind, daß die Spezifikation einer Prozeßsteuerung eine neu entstandene Umweltbedingung nicht erfaßt oder daß in einer vernetzten Produktionsanlage oder einem Telekommunikationssystem mehrere Fehler in unvorhersehbarer Weise zusammenwirken.

Zusammenfassend kann festgehalten werden: Die Verletzlichkeit der Gesellschaft durch unbeabsichtigtes Versagen der IuK-Technik wird nicht durch die Informatisierung und Automatisierung als solche verstärkt. Für viele einfache Routinearbeiten erhöhen sie den Grad der Sicherheit beträchtlich. Zu einem Problem der Verletzlichkeit werden sie dagegen unter zwei Bedingungen: Wenn sie in hochkomplexen, eng gekoppelten Syste-

94 S. Perrow 204f.

men mit großen Schadenspotentialen eingesetzt werden, und wenn die Gesellschaft sich von ihnen abhängig macht. Unter diesen Umständen muß es jedenfalls als unverantwortlich bezeichnet werden, mit Systemen zu arbeiten, von denen man weiß, daß sie unzuverlässig sind, aber nicht wissen *kann*, an welchen Stellen und in welchem Maß.

Von dieser Sorge bewegt hat auch die bedeutendste Berufsorganisation der US-Informatiker, die "Association for Computing Machinery" (ACM), 1984 ihre traditionelle gesellschaftspolitische Zurückhaltung aufgegeben und eine Resolution beschlossen. Dort heißt es:

"Entgegen dem Mythos der Unfehlbarkeit von Rechensystemen können diese sehr wohl versagen und tun dies auch. Folglich kann die Zuverlässigkeit von rechnergestützten Systemen nicht als gesichert gelten. Diese Tatsache gilt für alle solche Systeme, aber sie ist besonders wichtig für Systeme, deren Fehlverhalten ein besonderes öffentliches Risiko darstellt."[95]

95 Goldberg, CACM 1985, 131.

10. Missbrauchsmotive

Das hohe Schadenspotential der IuK-Technik kann nicht nur durch Fehler freigesetzt werden. Schäden können auch bewußt angedroht und herbeigeführt werden, um spezifische Interessen durchzusetzen. Wer aber könnte ein Motiv haben, diese Technik zu mißbrauchen? Wer hätte Vorteile, wenn er sie gegen ihre gesellschaftlich akzeptierte Bestimmung verwendet? Ist damit zu rechnen, daß die Gesellschaft mit diesem Schadenspotential erpreßt wird oder daß es zum Nachteil aller oder einzelner verwirklicht wird. Um zu erkennen, mit welchen Motivschwerpunkten künftig zu rechnen ist, werden die für IuK-Sicherheit Verantwortlichen die Motive bisheriger Mißbrauchsaktionen zusammenstellen. Auf der Grundlage dieser Erfahrungen werden sie dann versuchen, künftige Motive, deren Umsetzung sie ja verhindern sollen, abzuschätzen.[1] Dabei wollen wir ihnen über die Schulter schauen.[2]

Sicherheitsverantwortliche müssen sich ein Bedrohungsmodell konstruieren, an dem sie die Erforderlichkeit ihrer Sicherungsmaßnahmen messen. Hierfür versuchen sie, sich möglichst detaillierte Kenntnisse über Motive und Aktionsformen ihrer Gegner zu beschaffen. Öffentliche Fallsammlungen und Statistiken über Verurteilungen oder Anzeigen zur Computerkriminalität helfen ihnen wenig weiter, da diese nur das 'Hellfeld' abdecken und nur den zum jeweiligen Zeitpunkt strafbaren Mißbrauch erfassen.[3] Aber nur wenige Prozent aller Computer-Vergehen werden entdeckt und nur eine kleine Zahl der geschädigten Unternehmen zeigen erkannten Computer-Mißbrauch auch an. Sie wollen zum Schaden nicht auch noch den Spott der Konkurrenz und den Vertrauensverlust der Geschäftspartner haben.[4]

Der Chef des amerikanischen National Center for Computer Crime Data meint unter Berufung auf Quellen des FBI, daß nur 1% aller Computerdelikte entdeckt wird und daß von diesen entdeckten Delikten nur ca 14% zur Kenntnis der Ermittlungsbehörden gebracht würden, und daß hiervon wiederum nur in 3% der Fälle eine Verurteilung zu einer Freiheitsstrafe erfolgen würde. Das hieße, daß von 22.000 Tätern nur einer eine Freiheitsstrafe verbüßen müßte.[5]

Wegen des hohen 'Dunkelfelds' müssen die Sicherheitsmanager also versuchen, sich über bekannt gewordene Fälle ein eigenes Bild über Motive und Angriffsmöglichkeiten zu

---

1 Zur Vorgehensweise s. z.B. die Szenariomethoden von SBA - Security by Analysis - Computer Security Service GmbH; Eriksson 113 ff.

2 Zu den bisherigen Vorfällen und zum folgenden s. ausführlich Wedde, Die künftige Bedrohung der Informationsgesellschaft, Arbeitspapier Nr. 7.

3 S. hierzu näher Poerting KR 1986, 595 ff.

4 Wagner ÖVD-Online 5/1985, 39 schätzt die Entdeckungsrate auf 5% und die Chance, 'ungeschoren davonzukommen' auf über 99%. Nach Weck 28 werden etwa nur 1% solcher Manipulationen entdeckt und von diesen nur etwa 7% gemeldet. S. hierzu auch Sieg 313 mwN.; Bequai 5f.

5 Zit. nach Egli 146.

machen - nur so können sie Schwachstellen ihres Sicherungssystems erkennen. Sie werden bei ihrem Bemühen auf eine Fülle von Mißbrauchsfällen stoßen. Nach einer Diebold-Studie von 1984 über Computerkriminalität in Europa teilen sie sich in[6]

Brandstiftung und Bombenanschläge	20%
Sabotage	20%
Diebstahl von Geräten	20%
Diebstahl von Datenträgern und Informationen	15%
Betrugsfälle	10%
Sonstige	15%

Für unsere Studie wurden in der zweijährigen Bearbeitungszeit aus allen erreichbaren Quellen 1038 Mißbrauchsfälle zusammengetragen, von denen wir im folgenden einige darstellen werden. Zu diesem Zweck nutzten wir auch die neue Technik: Wir haben zweimal Recherchen in Datenbanken in der Bundesrepublik und den USA durchgeführt und den Mailbox-Dienst der 'Association for Computing Machinery' (ACM) 'Forum on Risks to the Public in Computer Systems' ausgewertet.[7] Unsere Fallsammlung enthält nur Vorfälle, die nach der oben gegebenen Definition[8] einen Mißbrauch der IuK-Technik darstellen, und dokumentiert die Breite und Vielfalt bisheriger Aktionen. Dabei variieren der Umfang, die Genauigkeit und vor allem die Glaubwürdigkeit der berichteten Ereignisse sehr und sind abhängig von der Quelle, aus der die Information stammt. Die überwiegende Mehrzahl der präsentierten Vorfälle scheint jedoch gesichert zu sein. Um eine Basis für die Abschätzung künftiger Motive und Aktionsformen zu finden, war es ausreichend, die zugänglichen Informationen zusammenzutragen und mit Quellenangaben zu präsentieren.[9] Eine Verifizierung jedes einzelnen Vorfalls ist nicht möglich und für den Untersuchungszweck auch nicht erforderlich. Die Mißbrauchsfälle verteilen sich nach folgender Struktur:

6 Diebold Parisini GmbH zit. nach CW 18/1984 v. 27.4.1984; Abel/Schmölz 42f.

7 Im folgenden zit. als Risk Digest.

8 S. Kap. 1.

9 Eine Vielzahl von Vorfällen aus eher zweifelhaften Quellen wurde nicht berücksichtigt.

Fallgruppe	Gesamt		BRD	Europa	USA	Sonstige
1. Bereicherung/Betrug	439	(24,3%)	125	130	178	13
2. Kreditkartenmanipulation	41	(4,0%)	26	10	2	3
3. Datendiebstahl	134	(13,0%)	61	43	27	3
4. Zeitdiebstahl	7	(0,7%)	4	0	3	0
5. Daten- oder Programmanipulation	45	(4,3%)	21	6	18	0
6. Inputmanipulation	40	(3,9%)	14	12	14	0
7. Unberechtigte Datenabfrage	17	(1,6%)	9	4	4	0
8. Hacking	62	(6,0%)	34	12	16	0
9. Spionage/Illegaler IuK-Technik-Transfer	22	(2,2%)	14	6	2	0
10. Sabotage	174	(16,8%)	89	29	54	2
11. Logische Angriffe (Viren, trojanische Pferde, logische Bomben)	57	(5,5%)	11	8	24	14
Gesamt	**1038**					

Bisherige Motive

Die Motive für solche Handlungen sind sehr breit gestreut. Einige Schwerpunkte lassen sich feststellen[10]:

Persönliche Motive

Viele Anschläge, Manipulationen, Spionage- und Sabotageaktionen erfolgten bisher aus persönlichen Motiven. So führten gerade die neuen, technikspezifischen Belastungen am Arbeitsplatz zu bisweilen kuriosen Versuchen, den *Streß* listig oder gewaltsam abzubauen.

Sachbearbeiter umgingen lieber die Prüfroutinen, indem sie die Prüfziffern änderten, als nach den Fehlern zu suchen, die nach unplausiblen oder unrichtigen Dateneingaben angezeigt wurden.[11] Um

10 S. hierzu auch Norman, Bequai, Weck 23 ff., Soyka, Heine, Schnarrenberg, Breuer 151 ff; Liebl 34 ff.; Sieber.

11 S. DSB 3/1979.

sich von ihrem Arbeitsstreß zu befreien, 'erschossen' Programmierer 1986 in North Carolina[12] und 1987 in New York ihren Computer[13], 'zertrümmerte' ein Mitarbeiter in Frankreich sein Terminal[14] und schmetterte ein Datenfachmann in einem Hamburger Illustrierten-Konzern 1979 eine volle Bierflasche in sein Gerät.[15] Ein Programmierer, der beim letzten Test eines größeren Programmprojekts einen Fehler entdeckte, übergoß Terminal und Unterlagen mit Spiritus und zündete sie an.[16] Streß war vermutlich auch der Grund, warum in einem Rechenzentrum in Süddeutschland die Stecker an der Zentraleinheit vertauscht wurden. Der Schaden betrug 40 000 Mark.[17]

Wirkliche oder vermeintliche Ungerechtigkeiten am Arbeitsplatz verleiteten Beschäftigte dazu, aus *Rache* an Vorgesetzten oder Kollegen, Geräte oder Programme zu zerstören.

Um seinen Betriebsleiter zu ärgern, mit dem er wegen eines überzogenen Urlaubs im Streit war, entwendete ein Mitarbeiter in einem Schiffsbaubetrieb die Lochstreifen für eine NC-Maschine und verursachte durch deren tagelangen Stillstand einen Schaden von mehreren 100.000 Mark.[18] Um sich an ihrem Chef zu rächen, gab eine Mitarbeiterin der Polizeizentrale in Los Angeles 1985 dessen Wagen in die Datei gestohlener Fahrzeuge ein und fügte den Hinweis hinzu, daß der vermeintliche Dieb bewaffnet sei.[19]

Gekündigte Mitarbeiter haben ihren *Ärger über die Entlassung* durch schädigende Manipulationen abreagiert und in der Zeit bis zu ihrem Ausscheiden ihr Fachwissen und ihre Systemkenntnisse destruktiv genutzt.

Ein entlassener Mitarbeiter löschte zum Beispiel Programme, die nur selten benötigt wurden, sorgte jedoch dafür, daß ihr Verlust erst dann bemerkt wurde, wenn sie gebraucht wurden, indem er sie in den Inhaltslisten beließ und ihren Speicherplatz weiterhin besetzte.[20] Ein anderer verursachte einen Schaden von 30 Millionen Dollar, indem er die Informationen auf allen Magnetbändern seines Arbeitgebers zerstörte.[21] Der entlassene Programmierer eines deutschen Unternehmens hat, um der Firmenleitung "eine Lektion zu erteilen", über die Datenfernverarbeitung noch lange nach seinem Ausscheiden Dateien seines früheren Arbeitgebers verändert.[22] Mit Blick auf seine baldige Kündigung hat ein Mitarbeiter den Firmenrechner so programmiert, daß durch Löschung seines Namens aus der Gehaltsliste alle Speicher zerstört wurden.[23] In einem parallelen Fall sorgte 1968 in Frank-

12 S. Bremer Nachrichten v. 10.10.1986.

13 S. Risk Digest 5.38, 2.

14 S. Zimmerli/Liebl 97.

15 S. Spiegel 4/1979, 38.

16 S. Zimmerli/Liebl 111f.

17 S. Sieber 2/122.

18 S. SBR 8/1982.

19 S. KES 5/1985, 189.

20 S. Zimmerli/Liebl 73.

21 S. SARK 162.

22 S. Sieber 2/100.

23 S. SARK 162; Volesky/Scholten iur 1987, 287, ähnliche Fälle berichten Lewens 19 und Zimmerli/Liebl 72.

reich ein Programmierer dafür, daß zwei Jahre nach seiner Entlassung alle Bänder gelöscht wurden.[24]

Neugier führte zum Ausspionieren personenbezogener Daten. Gerade bei Systemen, in denen zum einen hochsensible Informationen gespeichert sind und zum anderen leichte Abfragemöglichkeiten bestehen, sinkt offenbar die Hemmschwelle, auf diesem Weg Interessantes über Freunde oder Feinde in Erfahrung zu bringen.

So hat zum Beispiel ein Datenerfasser in der Polizeidirektion Pforzheim 1985 zwei Ausdrucke mit persönlichen Daten an Bekannte weitergegeben[25], und in Berlin rief ein Polizeiobermeister 1986 die Daten einer verfeindeten Nachbarin und ihrer zwei Kinder aus dem Polizeicomputer ab.[26]

Allgemeiner *Unmut* über das Eindringen der Datenverarbeitung in viele Lebensbereiche oder konkreter *Ärger* über eine Anlage führten zu einer Reihe von Sabotageanschlägen.

In Johannesburg versuchte ein Mann, den kommunalen Rechner von der Straße aus mit Gewehrschüssen außer Betrieb zu setzen. In den USA wurden Geldautomaten, die nicht funktionierten, 'erschossen' oder angezündet und auf Computer wurden 'Zielschießen' veranstaltet.[27] In Bremen gossen drei Jugendliche, die in einen metallverarbeitenden Betrieb eingedrungen waren, Granulat in die Tastaturen der DV-Anlage, bis diese ihren Betrieb einstellte.[28]

Spielerische *Lust am Probieren* und das Beweisen von Überlegenheit sind wesentliche Motive für 'Hacker'. Wenn sie in vernetzte Computersysteme eindringen und dort vorhandene Datenbestände inspizieren, verstehen sie sich meist als Anwälte des Datenschutzes, die Schwachstellen von Programmen aufdecken, oder als Vorkämpfer einer Informationsfreiheit, die ein solches Recht bereits praktizieren. Im Gegensatz zu ihnen arbeiten 'Cracker' zwar mit den gleichen Mitteln, aber mit destruktiven Motiven.

'Hacks' gelangen zum Beispiel 1981 in das 'Arpanet' des US-Verteidigungsministeriums[29], 1984 in das NASA-Netzwerk[30] und in das System der 'Companie International de Service en Informatique' in Frankreich[31], 1986 in die "nicht knackbaren" französischen Großrechner vom Typ Cray One und VAX und dort in Datenspeicher der Atombehörde CEA[32] und in 30 amerikanische Rechner mit

24 S. Spiegel 4/1979, 49; Norman 99; Sieber 93.

25 S. Taz v. 2.9.1985.

26 S. FR v. 17.9.1986.

27 S. Soyka 83 und 85.

28 S. Weser-Kurier v. 4.6.1988.

29 S. Spiegel 21/1983, 185.

30 S. Weser-Kurier v. 18.7.1984.

31 S. FR v. 29.11.1984.

32 S. FR v. 22.7.1986.

militärischen Daten[33], 1987 in das britische PRESTEL-System[34], in das Rechenzentrum der Freien Universität Berlin[35], in das DEC-Net und von da über das Space Physics Analysis Network in Rechner des NASA-Hauptquartiers[36] und 1988 in die Jet Propulsion Laboratories der NASA.[37] Mitglieder des Chaos Computer Clubs demonstrierten 1984 die Unsicherheit des Btx-Systems, indem sie mit der Codenummer und dem ausgespähten Passwort der Hamburger Sparkasse 13.000 mal eine von ihnen erstellte Bildschirmseite aufriefen. Dafür stellten sie der Sparkasse rund 130.000 Mark in Rechnung.[38]

Bereicherungsmotive

Bereicherungsabsicht führte zu Aktionen, die den Tätern materielle Vorteile sichern sollten. Dazu ist eine Fülle von Vorfällen dokumentiert, in denen Insider sich durch Manipulation von Daten- oder Programmen jeweils hohe Beträge auf ihre Konten überwiesen. Überall, wo mit Informationen über Geld zugleich geldwerte Verfügungen erfolgen, gab es auch schon Vorfälle, in denen diese Möglichkeiten zur Bereicherung mißbraucht wurden.

So haben sich Sachbearbeiter durch Computermanipulationen ungerechtfertigt regelmäßige "Sonderzahlungen"[39] oder Renten[40] gewährt, Kindergeld[41], Gehälter für Phantasiepersonen[42] oder bereits pensionierter Mitarbeiter[43], Zahlungen für fiktive Tätigkeiten[44] und Renten für bereits verstorbene Personen[45] überweisen lassen. Andere ließen die Zehntel-Pfennigs- bzw. -Cents-Beträge von Zinsberechnungen[46], die Pfennigsbeträge von auf volle DM-Beträge abgerundeten Zahlungen[47] oder Teilbeträge jeder Überweisung[48] auf ihr Konto gutschreiben oder sicherten sich eine Einlösung ihrer Schecks auch ohne die nötige Deckung.[49] Die Devisenmanipulationen, die Mitte der siebziger

33 S. New York Times v. 18.4.1988, 1f.

34 S. Zimmerli KR 1987, 339.

35 S. Spiegel 21/1987, 246 ff.; FR v. 19.5.1987.

36 S. Zeit v. 23.10.1987, 15f.

37 S. New York Times v. 18.6.1988, 45; FR v. 18.6.1988.

38 S. z.B. Zimmerli KR 6/1987, 338.

39 S. Spiegel 4/1975, 44.

40 S. Sieber 137f.; Sieg 321.

41 S. Sieber 47 ff.; ders. BB 1982, 1434; Sieg 316f.

42 S. Heine 171, Norman 217; Zimmerli/Liebl 38.

43 S. Norman 105f.; Heine 184.

44 S. Norman 78.

45 S. Zimmerli/Liebl 34; Zeit v. 26.10.1984, 35.

46 S. z.B. Heine 181f.; Lenckner 23; von zur Mühlen 47; Sieg 319f.; Söldner KR 1973, 1f.

47 S. Sieg 320; Söldner KR 1973, 1f.

48 S. Norman 83 mwN.

49 S. von zur Mühlen 57f.; Zimmerli/Liebl 43.

Jahre zum Zusammenbruch der Herstatt-Bank führten[50], sowie der Devisenbetrug bei VW 1987[51] zeigen, daß durch Mißbrauch der EDV zu betrügerischen Zwecken sogar mehrstellige Millionenbeträge erschwindelt werden können.

Habgier war auch das Motiv für Betrügereien und Unterschlagungen, die nicht unmittelbar auf Geld(informationen), sondern auf geldwerte Informationen über Güter und Leistungen zielten.

So erzielten mehrere Täter in den 70er Jahren in Florida bei Hundewetten einen Gewinn von mehr als einer Million Dollar, weil sie noch nach Abschluß des Rennens Wetten in den manipulierten Computer eingeben konnten.[52] An der University of Southern California hat 1984 eine Verwaltungsbeamtin gegen Bezahlung die Noten von fünf Studenten korrigiert.[53] In den USA konnten Insider Fernseher[54] und in Deutschland Kabeltrommeln[55] zu einem Bruchteil des realen Preises kaufen, weil sie Programme manipuliert hatten, die die Preise errechneten. 1987 wurden in den USA neun Studenten verhaftet, weil sie über die Telefonleitungen verschiedener Geschäfte Kreditkartennummern abgehört und damit Waren im Millionenwert elektronisch eingekauft hatten.[56] Durch Manipulation von Programmen gelang es einer Gruppe 1971 sogar, 200 Eisenbahnwaggons aus dem vollautomatischen Fahrplanablauf einer amerikanischen Eisenbahngesellschaft auszuklinken, zu entladen und wieder in den normalen Fahrplan einzufügen.[57]

Um materielle Vorteile zu erlangen, wurden in der Vergangenheit auch vielfach Daten und Datenträger gestohlen oder wertvolle Programme kopiert und Dritten zum Kauf angeboten.

1970 verkauften drei Programmierer der "Encyclopedia Britannica" die Anschriften von zwei Millionen Kunden, deren Wert auf drei Millionen Dollar taxiert wurde, an ein Versandhaus.[58] 1979 boten ein Angestellter der Firma 'Quelle' 327.000 Adressen zum Preis von 50 Pfennig pro Stück und ein Angestellter eines Versandgroßhandels 767.696 Adressen auf zwei Magnetbänder für 35.000 Mark an.[59] Mitarbeiter der britischen Fluggesellschaft BOAC verkauften Ende der 60er Jahre das gerade für etwa 2,5 Millionen Pfund neu entwickelte Abrechnungsprogramm an die Konkurrenz.[60] Und einem 17jährigen Schüler gelang es 1987, über das Datennetz in Computer des Nato-Hauptquartiers in

50 S. hierzu Sieber BB 1982, 1435; Sieg 320; Egli 155.

51 S. hierzu z.B. Spiegel 24/1987, 27 ff.

52 S. Zimmerli/Liebl 56; Norman 176; Sieber 2/127.

53 KES 5/1985, 189; Gleichzeitig hielt sich an der Universität das Gerücht, es wäre möglich, auf ähnliche Weise einen Doktortitel für 25.000 Dollar zu kaufen.

54 S. Norman 140f.

55 S. Zimmerli/Liebl 46.

56 S. Risk Digest 5.16 v. 24.7.1987.

57 S. Norman 96 f.

58 S. Heine 182.

59 S. Spiegel 4/1979, 41; Sieg 327.

60 S. Norman 74; s. ähnliche Fälle in Zimmerli/Liebl 66 und 76.

Burlington/North Carolina und des Luftwaffenstützpunkts in Robins einzudringen und hochentwickelte Programme zu kopieren, die er dann über ein Computernetz in Texas zum Verkauf anbot.[61]

Mit entwendeten Daten- oder Programmträgern wurden auch hohe Lösegelder erpreßt:

Zwei Angestellte der britischen Firma ICI versuchten, 275.000 Pfund damit zu erpressen, daß sie 540 Magnetbänder und 48 Plattensätze in der holländischen Niederlassung entwendeten.[62] In den USA soll ein Operator für die Rückgabe von Magnetbändern 200.000 Dollar erhalten haben.[63] In der Bundesrepublik entwendete ein ehemaliger Mitarbeiter mit einem Nachschlüssel alle Daten eines ausländischen Großprojekts, um noch offene Lohnforderungen gegen seinen konkursgefährdeten Arbeitgeber abzusichern.[64] In Belgien wurde 1986 einem Informatikunternehmen Software im Wert von 20 Millionen Francs gestohlen und für 3,5 Millionen Francs zum Rückkauf angeboten.[65]

Um Konkurrenzvorteile zu erlangen, griffen einige Unternehmen sogar zum Mittel der Wirtschaftsspionage und nutzten dabei Schwachstellen in Computernetzen oder -anlagen.

In den USA wurde die Datenleitung eines Ölkonzerns angezapft und so die Wirtschaftlichkeitsberechnung eines neuen Fördervorhabens abgefangen. Mit diesen Kenntnissen konnte die Konkurrenz den Konzern bei der Vergabe der Bohrrechte überbieten.[66] 1987 wurde bekannt, daß mehrere Personen über Datenleitungen längere Zeit Programme einer "international bekannten Firma im Schwarzwald" an eine "renommierte Firma in Saarland" überspielt und über eine dritte Firma weiterverkauft hatten.[67] Ein westdeutscher Elektrokonzern mußte feststellen, daß sein US-Konkurrent bestens über seinen Forschungsstand informiert war. Nachforschungen ergaben, daß im Rechenzentrum drei einschlägige Magnetbänder kopiert worden waren. Der Täter konnte nicht ermittelt werden.[68]

Da Rechenzeit eine kostspielige 'Ware' ist, wurde auch sie in der Vergangenheit des öfteren 'gestohlen'.

Entweder nutzten die 'Diebe' die Rechenanlage des Arbeitgebers, um eigene Programme zu entwickeln, zu testen und zu produzieren[69], oder sie bedienten sich der angeschlossenen Service-[70] bzw. Tochterrechenzentren.[71]

---

61 S. Weser Kurier v. 18.9.1987 und ausführlicher Washington Post v. 18.9.1987.

62 S. SARK 58.

63 S. SARK 67.

64 S. Sieg 315; Steinke NStZ 1984, 296.

65 S. Bremer Nachrichten v. 10.10.1986.

66 S. SARK 67.

67 S. FR 25.2.1987.

68 S. von zur Mühlen 87f.

69 S. Sieg 332f.; Wiesel, date report 3/1973, 26; Zimmerli/Liebl 69.

Politische Motive

Auch politische Motive waren Anlaß zu Aktionen gegen die IuK-Technik, und betriebliche Auseinandersetzungen Grund für Manipulationen an Daten und Programmen.

In den USA haben 1971 streikende Ingenieure einer Lebensversicherung die zentrale Datenverarbeitungsanlage dadurch lahmgelegt, daß sie Nacht für Nacht, bevor die Filialen ihre Daten vom Vortag überspielten, von einem externen Terminal aus den Befehl zum Durchlauf der Magnetbänder gaben. Auf die nicht zurückgespulten Bänder konnten dann keine Daten übermittelt werden.[72]

Politisch motiviert waren offensichtlich auch viele Fälle der Wirtschaftsspionage und des Schmuggels modernster IuK-Geräte.

So hat sich ein Angestellter eines westdeutschen Dienstleistungsunternehmens 1978 mit Wirtschaftsinformationen über 8000 Unternehmen in die DDR abgesetzt[73], haben Unbekannte 1987 aus der Universität Uppsala zwei als strategisch nutzbar klassifizierte Computer gestohlen und vermutlich in den Ostblock verkauft[74] und zwei norddeutsche Händler bis 1986 immer wieder Computer illegal nach Ost-Berlin exportiert.[75]

Protest gegen die Geschäftspolitik von Unternehmen führte des öfteren zu Brand- und Bombenanschlägen gegen deren Rechenzentren.

Ein Brandanschlag der "Action Directe" zerstörte 1980 die Räume von CII Honeywell Bull in Toulouse[76], ein Brandanschlag verursachte 1985 bei einem Datenverarbeitungsunternehmen in Karlsruhe einen Schaden von knapp einer halben Million Mark[77], und ein weiterer vernichtete 1987 elektronische Geräte der Computerfirma TST in Tutzing.[78] 1986 beschädigte ein Bombenanschlag das IBM-Forschungszentrum in Heidelberg.[79] In der Nacht nach dem Anschlag in Karlsruhe kam eine Person bei einem Sprengstoffanschlag auf ein Stuttgarter Rechenzentrum ums Leben.[80] "Kämpfende Einheiten" aus dem Umfeld der RAF verübten 1986 einen Anschlag auf eine Sendeanlage des Bundesgrenzschutzes bei Bonn.[81] Wegen seiner Unterstützung für das Apartheid-Regime in Südaf-

70 S. von zur Mühlen 105f.

71 S. Coughran 92.

72 S. Heine 158 ff.

73 S. SARK 67 mwN.

74 S. Toronto Sun v. 27.9.1987.

75 S. Weser Kurier v. 28.1.1987.

76 S. Wechselwirkung 16/1983, 27.

77 S. Sieg 314.

78 S. SZ v. 15.4.1987.

79 S. FR v. 17.11.1986.

80 S. hierzu den Verfassungsschutzbericht 1985, 124.

81 S. FR v 22.8.1986.

rika brachen 1986 in der Schweiz Unbekannte in die Räume eines multinationalen Konzerns ein, rissen alle Stecker aus den Geräten des Rechenzentrums und übergossen diese mit Cola.[82] In Frankreich hat die Gruppe CLODO[83] seit 1980 zahlreiche Brandanschläge auf Datenverarbeitungssysteme durchgeführt. Ihr erklärtes Ziel ist "der Kampf gegen jede Herrschaft".[84]

Im Vergleich zu anderen Motivgruppen und zu anderen Techniken war die Zahl politisch motivierter Anschläge gegen die IuK-Technik relativ gering. Sie richteten sich weniger gegen die Technik als solche, sondern vorwiegend gegen den Anwender. Als Angriffsobjekt war sie eher Mittel, um ihn zu schädigen, als primäres Ziel der Aktion. Die Vorläufer der künftigen Telekommunikation, die Briefpost und das Telefonnetz, waren keinen politisch motivierten Angriffen ausgesetzt. Sie boten bisher keine ideologische Angriffsfläche.

Künftige Mißbrauchsmotive

Künftige Handlungsmotive einzuschätzen, ist äußerst schwierig. Sie entwickeln sich nicht linear, sondern dynamisch. Je nach politischer und sozialer Situation, je nach konkretem Anwendungskontext der Technik, nach der spezifischen technischen Gestaltung oder praktizierten Sicherungsmaßnahmen und deren Abschreckungseffekt werden sich Anreize und Hemmnisse, die Technik zu mißbrauchen, unterschiedlich entwickeln. Selbst wenn im Sinne unseres Gedankenexperiments unterstellt wird, daß sich die 'Informationsgesellschaft' entsprechend unserem Zukunftsbild entwickelt, ist es nicht möglich, für einzelne Anwendungsbereiche die künftige Bedrohungssituation präzise einzuschätzen. Im folgenden können daher lediglich einige plausible Trendentwicklungen angedeutet werden. Wir werden jedoch sehen, daß dies zur Durchführung unserer Verletzlichkeitsanalyse ausreichend ist.

Auf eine problemfreie Einpassung von Individuen in die Verkehrsformen und Arbeitsverhältnisse der 'Informationsgesellschaft' kann niemand hoffen. Vielmehr dürften die künftigen gesellschaftlichen Strukturveränderungen noch stärker als die vergangenen die Aufgaben der Sozialisationsinstanzen erschweren und gesellschafliche Bindungen auflösen. Die abnehmende gesellschaftliche Integration wird zu weiteren Orientierungsverlusten, zu einer weiteren Steigerung der Kriminalität und zu einer weiteren Radikalisierung von Minderheiten führen.

Künftig wird keines der gegenwärtigen Motive wegfallen. Sie dürften sich zumindest in dem Umfang verbreiten, in dem die Nutzung von IuK-Systemen zunimmt. In dem Maße, wie die IuK-Technik Funktionen in Bereichen übernimmt, in denen Informationsverarbei-

82 S. KES 4/1986, 159f.

83 Clodo steht im Französichen eigentlich für Clochard. Als Name für diese Gruppe ist es eine Abkürzung für "Comite liquidant et detournant les ordinateurs" = Komitee zur Beseitigung und Entwendung von Computern.

84 S. Wechselwirkung 16 (1983), 27.

tung oder Kommunikation bisher noch konventionell erfolgt, werden Mißbrauchsmotive aus diesen Bereichen auf die IuK-Technik verlagert.[85] Über diese hinaus werden allerdings noch Mißbrauchsmotive hinzukommen, die durch die gesellschaftlichen Bedingungen einer 'Informationsgesellschaft' erzeugt werden.

Haß, Rache, Neid und Neugier wird es auch künftig geben. Zusätzliche *persönliche Motive* sind vor allem im Arbeitsleben und im Alltag zu erwarten. Die IuK-Technik wird in den kommenden Jahrzehnten die gesamte Arbeitswelt prägen und das private Leben des einzelnen sehr stark beeinflussen. Für nicht wenige Beschäftigte bringt dann die IuK-Technik mit ihren betrieblichen Folgewirkungen eine Erhöhung der Arbeitsintensität und damit eine Verschärfung des Arbeitsstresses mit sich. Gleichzeitig erwartet sie eine immer effektivere Kontrolle der Arbeitsleistung und des Verhaltens. Nicht jeder wird von der zunehmenden Automatisierung profitieren. Vielmehr werden viele die Entwertung ihrer Arbeitsqualifikation oder gar den Verlust ihres Arbeitsplatzes erleben. Je mehr die 'intelligente Gesellschaft' den intelligenten Individuen erlaubt, ihre Leistungen zu entfalten, um so schneller veralten Qualifikationen, die vordem etwas gegolten haben. Der Erfolg der einen bedeutet so für die anderen die Vernichtung ihrer Existenzgrundlagen, für viele Familien verbunden mit einer Minderung des Einkommens. Im gesellschaftlichen Bereich wird zugleich die Möglichkeit der Überwachung zunehmen. Auch im Privatbereich dürfte nicht jeder die Informatisierung als Bereicherung empfinden: Sie wird für viele mit Isolierung, verminderter Kommunikationsfähigkeit, Orientierungslosigkeit und ähnlichem einhergehen. Einige dieser 'Verlierer' der Informatisierung werden die IuK-Technik als Identifikationsobjekt ihrer Benachteiligung ausmachen. Für andere könnte die wachsende gesellschaftliche Bedeutung der Informationstechniken Anlaß sein, sie zum Gegenstand auch irrationaler Angriffe zu machen.

Aus diesen sozialen Veränderungen könnten also leicht Mißbrauchsmotive resultieren. Zwar dürfte die Mehrheit sich am Arbeitsplatz den Anforderungen der neuen Technik anpassen; und nicht wenige werden die durch sie ermöglichten Arbeitserleichterungen begrüßen. Für einen - stetig steigenden - Teil der Betroffenen jedoch dürfte der zunehmende Arbeitsstreß, das Gefühl, der unerbittlich kontrollierenden, aber undurchschaubaren Technik ausgeliefert zu sein, sich unmittelbar in Anreize zu Manipulations- oder Sabotagehandlungen umsetzen. Die Befürchtung, den Arbeitsplatz zu verlieren, könnte gerade bei den Computer-Spezialisten zu 'vorsorglichen Racheaktionen' führen, indem sie Programme so manipulieren, daß sie im Fall ihrer Entlassung einen Schaden verursachen. Angesichts der künftigen 'Computersozialisation' ist es nicht auszuschließen, sondern eher anzunehmen, daß sowohl vom Arbeitsplatz als auch vom heimischen Terminal aus Versuche unternommen werden, aus Neugier und Lust am Computer-Abenteuer elektronische Sicherungen zu überwinden, in Datennetzen herumzureisen und

85 So z.B. Bschorr 7.

neue Computerwelten zu entdecken.[86] Die 'Hackerbewegung' könnte leicht zu einer Subkultur der 'Informationsgesellschaft' werden.

Zusätzliche *kriminelle Motive* dürften sich aus dem steigenden Wert von Informationen ergeben. Konkurrenzvorteile beruhen zunehmend auf der Verfügung über Informationen und die Methoden ihrer Verarbeitung. Dementsprechend dürfte auch das Interesse Dritter in Wirtschaft, Wissenschaft oder Militär steigen, über diese ebenfalls zu verfügen oder sie der Konkurrenz abzunehmen. Damit erhöht sich aber auch der Anreiz für Bestechung, Spionage, Erpressung, Daten- und Datenträgerdiebstahl sowie Manipulation und Vernichtung von Daten und Programmen oder Sabotage.

Der Anteil der Software an den Kosten von IuK-Systemen wird bis auf 80 und 90% ansteigen. Viele Anwender werden bestimmte Programme nicht entwickeln oder bezahlen können. Dies dürfte insbesondere für Software von Expertensystemen oder Anwendungen 'künstlicher Intelligenz' gelten. Sie werden daher zunehmend einen Ausweg auf einem grauen oder schwarzen Markt suchen. Die dort zu erzielenden Gewinne lassen einen steigenden Anreiz zu Softwarediebstählen erwarten.

Im Konkurrenzkampf werden spezifische Informationen über potentielle Kunden immer wichtiger. Die Nachfrage nach solchen Daten trifft zusammen mit einer erheblich umfangreicheren Speicherung personenbezogener Daten. Nicht nur im Verwaltungs-, Gesundheits- und Sozialbereich werden solche Daten gesammelt und ausgewertet, sondern auch in den Personalinformationssystemen der Unternehmen, in den Kundendateien der Versicherungen, Banken und Handelshäuser oder bei den Anbietern von Telekommunikationsdiensten. Der steigende Wert spezifischer Kundeninformationen dürfte einen großen Anreiz auf die Betreiber solcher Datensammlungen oder auf ihre Mitarbeiter ausüben, Profile der bei ihnen gespeicherten Personen auch kommerziell zu verwerten.

Die Geldwirtschaft wird weitgehend elektronisiert. Milliardenwerte werden täglich in Form von Bits und Bytes verschoben. Die Automatisierung und Beschleunigung des Zahlungsverkehrs macht diesen immer weniger durchschaubar. Während früher, als die Buchhaltung noch manuell erledigt wurde, ein Beleg durch viele Hände ging, bis eine Zahlungsanweisung ausgeschrieben wurde, werden künftig die Kontrollen in der Regel Automaten übertragen. Wem es gelingt, diese Kontrollen zu unterlaufen, der geht nur noch ein sehr geringes Entdeckungsrisiko ein.[87] In einer Welt ohne Kassen und Papiergeld wird zwar Bankraub seltener, dafür aber elektronischer Raub häufiger.[88] Für alle, die am Geldtransfer beteiligt sind und die die Kontrollen kennen, wächst der Anreiz, durch kleine gezielte Manipulationen zu großen Gewinnen zu gelangen. Vor allem in Klein- und Mittelbetrieben hängt dann die wirtschaftliche Existenz von der Ehrlichkeit einer kleinen Anzahl Spezialisten ab, die allein in der Lage sind, die automatischen Zahlungsabwicklungen zu kontrollieren. Ähnliches gilt für die Zukunft der Warenwirtschaft. Lagerverwal-

86 S. z.B. Heidinger/Andrich 168; Schönberg 96; Solarz 20f.

87 S. Abel/Schmölz 126; Abel RDV 1988, 74; Solarz 16 ff.; Egli 147.

88 S. z.B. Bequai 181; Egli 147.

tung und Warenflüsse werden automatisch verwaltet und gesteuert. Wer Möglichkeiten hat, die entsprechenden Programme oder Daten zu beeinflussen, kann sich leicht Vermögensvorteile verschaffen, ohne daß dies bemerkt wird.

Wenn nahezu alle Geld- und Warenströme von Computern gesteuert und kontrolliert werden, dann sind im Bereich der Computer-Kriminalität auch Formen organisierten Verbrechens zu erwarten.[89] Solche Organisationen dürften versuchen, Computer-Spezialisten in Rechenzentren einzuschleusen oder die dort Beschäftigten zu erpressen, zu bestechen oder zu verführen. Sie könnten aufgrund ihrer Struktur ein Zusammenspiel vieler Stellen innerhalb eines Computernetzwerks organisieren, und dadurch sowohl den Effekt von Manipulationen erhöhen, als auch ihre Aufdeckung erschweren.

So soll eine 90köpfige Organisation von 1985 bis 1987 mit gestohlenen oder manipulierten Euroscheck-Karten größere Geldbeträge automatisch abgehoben haben - mit einer einzigen Karte bis zu 26.000 Mark an einem Tag.[90] Südamerikanische Drogensyndikate nutzen bereits heute Computer, um den Drogenversand zu überwachen, ihre Geldströme zu lenken und die Mitarbeiter zu beaufsichtigen. Sie beschäftigen Computer-Spezialisten, die sogar in Computer der US-Drogenfahnder in El Paso eingedrungen sein sollen.[91] Wong berichtet, die Mafia habe einen Software-Entwickler beauftragt, für die arabische Bankenwelt ein Datennetz zu entwickeln und in dieses eine 'Falltür' einzubauen, durch die sie später in das Netz eindringen könnten.[92]

Politische Motive entstehen zusätzlich und verstärkt vor allem durch die gesellschaftlichen Folgewirkungen der Informatisierung. Die IuK-Technik wird zukünftig *das* Rationalisierungsmittel und *das* Überwachungsinstrument sein oder als solches angesehen werden. Sie wird als die Technik gelten, die das gesamte gesellschaftliche und politische Leben verändert und in jedem Gesellschaftsbereich soziale und individuelle Anpassungsleistungen erzwingt. Sie entwickelt sich daher auch zu einem Kristallisationspunkt für kulturelle, soziale und politische Unzufriedenheit. Alle, die unter den neuen Verhältnissen leiden, alle, die die 'Dynamik der Technik' aufhalten wollen, werden ihre Aggressionen gegen diese Technik und ihre Protagonisten richten. Als Symbol für den verhaßten gesellschaftlichen und technischen 'Fortschritt' wird sie nicht nur - wie bisher - Mittel, sondern auch primäres Ziel militanter Aktionen sein.[93] Gegner des Gesellschaftssystems könnten folglich versuchen, dessen 'Nervenzentren und -bahnen' auszuschalten.

Sie werden zunehmend erkennen, welches Schadenspotential mit IuK-Technik-Anwendungen verbunden ist und welchen Stellenwert die IuK-Technik für die 'Informationsgesellschaft' oder einzelne Unternehmen und staatliche Institutionen hat. Ihnen wird noch deutlicher werden, welche Bedeutung die weltweiten Computernetze für die Macht

89 S. z.B. Bequai 188; Steiner IO-Management-Zeitschrift 1988, 119.

90 S. Weser Kurier v. 29.7.1987.

91 S. FR v. 6.8.1988.

92 S. Wong DuD 1987, 135.

93 S. z.B. Nora/Minc 73.

multinationaler Konzerne, die neuen Medien für die Beeinflussung der politischen Verhältnisse oder die Telekommunikation für betriebliche Rationalisierungen und gesellschaftliche Kontrolle haben. Dadurch wird die *Infrastruktur* der 'Informationsgesellschaft' zum Angriffsobjekt. Insgesamt ist also zu erwarten, daß militanter Widerstand sich vermehrt direkt gegen diese Techniken richtet - gewalttätig oder listig, durch Bomben oder durch Manipulation von Programmen.

Ebenso wie heute neue Formen des sozialen Widerstandes durch Blockaden, Mahnwachen, Boykottmaßnahmen und ähnliche Aktionen erprobt und durchgeführt werden, könnten sich in der 'Informationsgesellschaft' entsprechende Aktionsformen herausbilden - vom Überfüllen elektronischer Briefkästen über die gezielte Überlastung von Telekommunikationsdiensten bis hin zur Blockade elektronischer 'Zufahrtswege'.[94]

Die durch IuK-Technik ermöglichte neue Flexibilität der Unternehmen wird zu einem Machtzuwachs gegenüber den Arbeitnehmern und deren Interessenvertretungen führen. Diese werden Gegenmacht weitgehend nur noch entfalten können, wenn sie ihre Schlüsselstellungen in der Herstellung und Nutzung von IuK-Technik als Druckmittel einsetzen. Geringe Manipulationen an Daten oder Programmen könnten dieselben Auswirkungen haben wie herkömmliche Streiks. Und durch Eingriffe in IuK-Systeme ließe sich auch die Arbeit von Streikbrechern verhindern.

Zusammenfassend ist festzuhalten: Der Anreiz zu Mißbrauch von IuK-Systemen wird nicht nur proportional mit dem Ausbau dieser Systeme steigen. Vielmehr werden gerade einige spezifische soziale Folgen dieser Technik dazu führen, daß sowohl die Zahl als auch die Varianten von Mißbrauchsmotiven künftig zunehmen werden.

Kollektive Mißbrauchsmotive

Aber nicht nur Motive für einzelne Personen oder kleine Gruppen sind in Betracht zu ziehen, sondern auch soziale Prozesse, die die 'Informationsgesellschaft' in unvorhergesehener Weise gefährden könnten. Die Bundesrepublik wird in den kommenden Jahrzehnten ihren Reichtum nicht wie bisher still und unangefochten genießen können. Sie wird stärker in den Weltmarkt und in die Weltpolitik integriert werden und daher politischen Turbulenzen in anderen Weltgegenden stärker ausgesetzt sein. In dem Maße, wie die Bundesrepublik als eine der führenden Industrienationen die wirtschaftlichen, politischen, sozialen und ökologischen Verhältnisse in anderen Teilen der Welt beeinflußt und damit mehr oder weniger stark Unterdrückung, Diskriminierung, Hunger, Elend und Krankheit in der Dritten Welt verursacht oder unterstützt, werden sich die dadurch hervorgerufenen Konflikte und Krisen, Widerstands- und Befreiungskämpfe auch hier im Land auswirken. Wer kann annehmen, daß etwa die politische Unterstützung Israels oder die Lieferung von Waffen an Südafrika oder Saudiarabien folgenlos bleiben würde?

94 S. hierzu auch SARK 79f.; Wechselwirkung 16 (1983), 21.

In den letzten 20 Jahren haben sich die Formen, Konflikte bewaffnet auszutragen, gewandelt.[95] Statt 'regulärer' Kriege sind viele Staaten immer mehr zu Formen indirekter Kriegsführung übergegangen. Sie unterstützen Gruppen, die mit terroristischer Gewalt ihre Ziele verfolgen, oder lassen eigene Agenten Anschläge ausführen. Sie nutzen Terrorismus als ein weiteres 'Waffensystem', als eine billige , risikolose Möglichkeit, Krieg zu führen. Was als Taktik der Schwachen und Verzweifelten begonnen hatte und in Zukunft weiterhin Bedeutung haben wird, dürfte künftig zur bevorzugten Form werden, Konflikte mit anderen Staaten auszutragen.

So wie im August 1986 in der Bretagne aufgebrachte Bauern zwei Finanzämter gestürmt haben[96], könnten auch Entwicklungen in der Bundesrepublik kollektive Aktionen gegen technische Anlagen möglich erscheinen lassen. Die zu erwartenden wirtschaftlichen Modernisierungs- und sozialen Anpassungsprozesse werden stärkere soziale Konflikte hervorrufen, als in den letzten Jahren auszuhalten waren. Wie lange werden es die vielen Dauerarbeitslosen noch tatenlos hinnehmen, an dem wachsenden Reichtum der Volkswirtschaft nicht beteiligt zu werden? Wann werden die drohenden ökologischen Katastrophen zu ersten kollektiven Verzweiflungsaktionen führen, die eine wirkliche Wende in der Politik herbeizwingen wollen?

Gesellschaftliche Unruhen, härtere Arbeitskämpfe, die Zuspitzung innenpolitischer Konflikte bis hin zu bürgerkriegsähnlichen Situationen, äußere Spannungslagen, stärkere Auswirkungen des internationalen Terrorismus oder Agentenaktionen in größerem Ausmaß - wer wollte dies alles für die nächsten 20 bis 30 Jahre ausschließen? In einer solchen Welt voller Konflikte wird künftig auch versucht werden, durch Mißbrauch der IuK-Technik politische Vorteile zu erzielen. Dann kann nicht mehr nur mit vereinzelten Angriffen gerechnet werden. Im Rahmen eskalierender Konflikte sind vielmehr auch koordinierte Aktionen in Rechnung zu stellen, durch die gezielt versucht wird, den maximalen Schaden anzurichten.[97]

95 S. hierzu Jenkins 1 ff.; SARK 46.

96 S. FR v. 22.8.1986.

97 S. hierzu auch Roßnagel 1987a, 56 ff. für das Beispiel der Atomtechnik.

11. Angriffsformen

Um den Sicherungsbedarf und das Sicherungsniveau bestimmen zu können, werden die Verantwortlichen für das jeweilige IuK-System eine Bedrohungseinschätzung erstellen müssen. Neben dem Schadenspotential und dem Mißbrauchsmotiv müssen zu diesem Zweck die künftig möglichen Angriffsformen abgeschätzt werden - und zwar zunächst ohne Berücksichtigung zusätzlich möglicher Sicherungsmaßnahmen. Denn in welchem Umfang diese erforderlich sind, wird nur deutlich, wenn untersucht wird, was ohne sie möglich wäre. Die Sicherheitsbeauftragten werden versuchen, für ihre Bedrohungseinschätzung aus den Vorfällen der Vergangenheit zu lernen. Angriffe können gewaltsam oder listig sein. Je nachdem, ob sie von Insidern oder von Externen vorgetragen werden, haben sie unterschiedliche Voraussetzungen und Erfolgsaussichten.

Es mag gefährlich sein, über Mißbrauchsaktionen und -möglichkeiten zu informieren. Aber noch gefährlicher ist es, diese Gefahren nicht öffentlich zu diskutieren. Jeder, der IuK-Technik mißbrauchen will, kennt ohnehin die ihm gegebenen Möglichkeiten. Die Öffentlichkeit aber muß informiert sein, welche Risiken sie durch die Nutzung von IuK-Technik eingeht, wie diese begrenzt werden können und welche Restrisiken verbleiben. Um keine neuen zusätzlichen Vorbilder für kriminelle Aktionen zu liefern, beschränken wir uns jedoch soweit wie möglich darauf, künftig zu erwartende Aktionen an bereits veröffentlichten Fällen zu illustrieren.[1]

Insider

Interne Angreifer, die aufgrund ihres Arbeitszusammenhangs mit dem IuK-System Zugang oder Zugriff zu technischen Anlagen oder Informationen haben, können in der Regel erheblich größere Schäden anrichten als Externe. Sie kennen die Schwachstellen, wissen, wo sie ansetzen müssen, und können den richtigen Zeitpunkt für ihren Anschlag abwarten.

Ein böswilliger interner Angreifer könnte versuchen, ein Informationsverarbeitungssystem, ein Lager mit Datenträgern oder Leitungen und Vermittlungsstellen des Telekommunikationsnetzes zu *zerstören* oder zu *beschädigen*. Als Mittel hierfür kommen Brand- und Bombenanschläge in Frage.

Der Hausmeister legte 1969 in Zürich in der Quartierzentrale Hottingen der schweizerischen Post ein Feuer, das den gesamten Hauptverteiler für Telefon und Telex zerstörte.[2]

---

1 Ebenso SARK 56.

2 Laut Schreiben der Generaldirektion der PTT Bern vom 1.4.1987.

Aber auch indirekte Aktionen, wie die Zerstörung der Klimasysteme oder der Stromversorgung, Überflutung, Verschmutzung oder Feuchtigkeitszufuhr können zum Ausfall der Systeme führen.

In den USA legte ein Systemoperator mit Hilfe eines einfachen kleinen Metallstücks innerhalb von zwei Jahren 56 mal den Großrechner der National Farmers Union Corporation durch Kurzschlüsse lahm.[3]

Für Insider gibt es darüber hinaus noch eine Fülle kleinerer verdeckter Sabotagemöglichkeiten, die die besondere Empfindlichkeit von IuK-Systemen ausnutzen - etwa das 'versehentliche' Verschütten von Flüssigkeiten, das Einführen von Büroklammern oder Nadeln in die Lüftungsschlitze der Geräte[4] oder das Überstreichen von Datenträgern mit einem kleinen Magneten. Die Mittel für solche kleinen Anschläge befinden sich am Arbeitsplatz oder können unauffällig dorthin gebracht werden. Das Entdeckungsrisiko ist relativ gering.[5]

Insider können aufgrund ihres Zugangs zu Geräten und Datenträgern versuchen, diese zu *entwenden*. Wenn auf den Datenträgern wertvolle Informationen oder Programme gespeichert sind, können die Täter diese weitergeben oder den Eigentümer damit erpressen. Durch ihr Fehlen kann auch der Betrieb der EDV für eine gewisse Zeit gestört oder verhindert werden.

1968 stahlen z.B. zwei Mitarbeiter das neu entwickelte Buchungsprogramm von BOAC und verkauften es an die Konkurrenz.[6]

Insider könnten die Programme und Daten, zu denen sie Zugang haben, Dritten dadurch *zugänglich machen*, daß sie diese kopieren, über Datenleitungen übermitteln, in allgemein zugängliche Informationssysteme überspielen oder sie einfach nur zur Kenntnis nehmen und wichtige Details weitergeben.

Der spektakulärste Datenträgerdiebstahl fand in Holland statt: Wie bereits erwähnt, wurden der Firma ICI 540 Bänder und 48 Magnetplattenstapel entwendet.[7]

Die in Zukunft zu erwartenden drastischen Verkleinerungen der Massenspeicher wird den Diebstahl von Datenträgern erheblich erleichtern. Wenn der "Inhalt der Sozialdatenbank in vielleicht zehn Jahren in einen 'Zuckerwürfel' paßt, .. wird es sehr schwer sein, alle

3 S. Heine 185.

4 S. hierzu z.B. Breuer 206.

5 S. hierzu näher Wechselwirkung 16 (1983), 20.

6 S. Norman 74.

7 S. Norman 176 ff.; SARK 68; Sieber 2/123.

Personen, die damit irgendwie zu tun haben, davon abzuhalten, diesen Zuckerwürfel eines Tages zu schlucken und aus dem Rechenzentrum herauszutragen."[8]

Betriebspersonal der TELEKOM, anderer Betreiber von Telekommunikationsdiensten oder von ISDN-Nebenstellenanlagen könnte durch Manipulation der Vermittlungssoftware die Aufnahme aller Verbindungsleitungen veranlassen, ohne daß der Teilnehmer dies bemerkt. Mit Hilfe einer 'Konferenzschaltung' könnten 'interessante' Gespräche sowie Text-, Bild- und Datenübermittlungen an einen dritten Anschluß übermittelt, automatisch aufgezeichnet und ausgewertet werden. Ebenso könnten die Inhalte von Mailboxen ausgekundschaftet oder Dritten zugänglich gemacht werden. Informationsanbieter oder deren Personal hätten die Möglichkeit, aus den anfallenden Benutzungsdaten Personenprofile zu erstellen und für Marketingzwecke weiterzuverkaufen.[9]

Einen besonderen Verwendungszweck für ausspionierte Daten hatte ein amerikanischer Kokainhändler. Er soll regelmäßig die Computerdatei des California Department of Justice angezapft haben, um die 'Bonität' seiner Kunden zu überprüfen. Sie waren ihm nur dann vertrauenswürdig, wenn sie einschlägig vorbestraft waren.[10]

Durch *Programm-* und *Datenmanipulationen* können Insider im Vergleich zu herkömmlichen Verfahren der Informationsverarbeitung mit einem minimalen Aufwand etwa durch die Eingabe weniger Programmzeilen oder falscher Daten einen sehr großen Schaden anrichten. Kurze Anweisungen lassen sich zwischen Millionen von Programmzeilen mit einem geringen Entdeckungsrisiko 'verstecken'. Gelingt es einem Beschäftigten, Programmfehler auszunutzen, die im Test unentdeckt blieben, von ihm aber in der praktischen Anwendung erkannt wurden, so ist sein Entdeckungsrisiko gering. Er muß dann nämlich keine Manipulationen mehr durchführen, durch die er auffallen könnte.

Die größten Risiken gehen von Programmentwicklern, Wartungstechnikern oder Systemverwaltern aus. Denn sie haben am ehesten die Möglichkeit, unentdeckt Programme und Daten zu manipulieren. Dadurch könnten sich Insider materielle Vorteile, kostenlosen Zugang zu Rechnern und Netzen, Rechenzeit oder Einblick in Dateien verschaffen und für weitergehende Zwecke nutzen. Die Manipulation einer Datensammlung kann auch gleichbedeutend sein mit ihrer Vernichtung. Das im Rechner zu bearbeitende Modell der Wirklichkeit kann durch die so erzeugte Differenz zur Wirklichkeit wertlos werden.

Als besonders gefährliche Angriffsformen der Zukunft dürften neue, durch die IuK-Technik erst ermöglichte '*logische Angriffe*' gelten: Folgende Funktionen können neben anderen durch Manipulation in Programme eingeführt werden:

8 Haefner 1989.

9 S. hierzu auch Bundesbeauftragter für den Datenschutz, 5. Tätigkeitsbericht, 37.

10 S. KES 3/1986, 121; Zeit v. 15.4.1988, 23.

Trojanische Pferde sind Programmteile, die Funktionen ausführen, die dem normalen Benutzer verborgen bleiben - wie etwa die bei der Rundung von Zinsberechnungen wegfallenden Zehntelpfennige auf ein bestimmtes Konto zu überweisen. Sie könnten auch die Aufgabe haben, bestimmte Daten oder Programme zu kopieren, bei Gelegenheit an einen Empfänger zu übertragen und sich danach selbst zu löschen. Eine eher spaßige Spielart ist das Keks-Monster.

Auf dem Bildschirm erscheint in bestimmten Abständen die Aufforderung "Ich möchte einen Keks". Wird das Wort "Keks" eingegeben, verschwindet das Monster wieder. Wird die Aufforderung ignoriert, erscheint es nach einiger Zeit wieder mit der Aufforderung "Ich habe Hunger und will einen Keks". Diese wiederholt sich immer häufiger, bis das Monster ernst macht und androht: "Wenn Du mir keinen Keks gibst, fresse ich eine Deiner Dateien". Spätestens dann sollte jeder Nutzer diesen "Keks"-Hunger stillen.[11]

Eine spezielle, besonders bösartige Form der Trojanischen Pferde sind *logische Bomben*: Versteckte Befehle, die zu einem bestimmten Zeitpunkt oder bei einem bestimmten Befehl das Programm oder die Datei löschen.

Ein Computerexperte an der Bundeswehrhochschule in München drohte, sein von ihm erstelltes Programm GURUGS werde sich in der Silvesternacht 1984 selbständig zerstören, wenn seine Gehaltsforderungen nicht erfüllt würden. Da sein Arbeitgeber auf diese Forderung nicht einging, löschte sich das Programm zum vorhergesagten Zeitpunkt selbst.[12] In Minneapolis (USA) legte 1985 ein Programmierer eine "Zeitbombe" in das System seines Arbeitgebers, die im Fall seiner Kündigung alle Dateien löschen sollte. Als dies bekannt wurde, weil er es stolz einem Kollegen erzählt hatte, versuchte er, seinen Arbeitgeber zu erpressen. Der ließ ihn jedoch verhaften und die 'Zeitbombe' durch besonders beauftragte Spezialisten entfernen.[13]

Eine spezielle Form der Trojanischen Pferde sind *Falltüren*: Funktionen, die ein unbemerktes Eindringen in ein System unter Umgehung von Zugangs- und Zugriffskontrollen ermöglichen. Sie können so angebracht werden, daß sie die Rechte eines Systemmanagers gewähren. Wer sie kennt kann, dann Rechenzeit, Speicherplatz oder Programme verfügen, neue Programme einschleusen und die Rechte anderer einräumen, erweitern, begrenzen oder aufheben.

Solche Falltüren zu installieren ist in einigen Fällen sogar Externen gelungen. Im September 1987 gelang es deutschen Hackern, über Datennetze Großrechner der NASA zu erreichen. Durch einen Fehler im Betriebssystem konnten sie die Tabelle der Zugriffsberechtigungen manipulieren und sich so den Status des Systemverwalters verschaffen. Als solcher schufen sie über ein nur ihnen bekanntes Kennwort einen 'Generalschlüssel', der ihnen jederzeit den Zugriff auf das System mit allen

11 S. zum Cookie-Monster Witten, Abacus Nr. 4/1987, 13; Darmstädter Echo v. 24.3.1988.

12 S. Spiegel 2/1985, 79.; Volesky/Scholten iur 1987, 287; Sieg Jura 1986, 359.

13 S. Software Engeneering Notes 3/Juli 1975, 15 f.; s. hierzu auch den in SARK 162 genannten Fall.

Privilegien und unter Umgehung aller Zugangsbeschränkungen und Kontrollmechanismen sicherte. Über die beiden NASA-Rechner hatten die Hacker Zugang zum SPAN-Netz (Space Physics Analysis Network). Sie konnten in weitere 136 Rechner eindringen und dort ebenfalls 'Generalschlüssel' hinterlegen. Betroffen waren Rechenzentren in der ganzen Welt, die Daten sowohl aus militärischen wie auch zivilen Projekten verarbeiten.[14] Ähnliche Falltüren konnten sich Hacker 1986 im Rechenzentrum der Universität Linz[15] und 1987 im Rechenzentrum der Universität Berlin einrichten.[16]

Trojanische Pferde und Falltüren sind Manipulationen, die jedesmal in 'Handarbeit' eingebracht werden müssen. Direkte Manipulationen können leicht auffallen. Eleganter ist es da, Manipulationen automatisch ausführen zu lassen.

Während des 'NASA-Hacks' gelang es den Hackern nach monatelangen Versuchen, die letzten Versionen ihres Generalschlüssels ohne 'Anwesenheit' des Hackers im Rechner automatisch unbemerkt einzugeben - während dort die normalen Rechenprozesse abliefen.[17]

Es gibt aber auch besondere Programmarten, die schädliche Programmbefehle automatisch verbreiten können. Am bekanntesten sind hier 'Würmer' und 'Viren'. *Würmer* sind Programme, die sich durch Kopieren ihrer selbst in den Programmen eines Systems bewegen. Sie wurden entwickelt, um von einem Ausgangsrechner nach einem festgelegten Protokoll Kopien auf andere Knoten eines Rechnernetzes zu übertragen und dort dann Funktionstests durchzuführen.[18] Sie könnten aber auch andere Aufgaben haben und dann großen Schaden anrichten.

Ein *Virus* ist ein Programmstück, das sich von einem 'Wirtsprogramm' aus, in das es eingepflanzt ist, in andere Programme kopieren kann und das in seinen 'Wirtsprogrammen' Manipulationsaufgaben erfüllen kann. Wie bei biologischen Viren gibt es auch bei Computerviren viele verschiedene Arten und Varianten. Das Standardvirus besteht aus drei Teilen: einem Infektionsverfahren, das eine Kopie des Virus in andere Programme (nicht Dateien) pflanzt, einem Erkennungsverfahren, das verhindert, daß ein infiziertes Programm erneut infiziert wird, und dem 'Krankheitskeim', einem Manipulationsverfahren, mit dem eine gewünschte Wirkung erzielt werden kann. Gelingt es, ein infiziertes Programm in eine Anlage einzuschleusen und wird dieses aufgerufen, so wird vor dessen Ausführung zuerst das Virus aktiv. Es sucht nach einem anderen Programm, das noch nicht infiziert ist. Enthält dieses noch keine Viruskennung und hat das Virus schreibenden Zugriff auf dieses Programm, kopiert es sich vor dieses Programm und kennzeichnet es

14 S. hierzu ausführlich Wernery, Datenschutz-Berater 9/1987, 1 ff. sowie den Bericht in Tempo 10/1987, 100 ff.; s. auch Marshall, Science 240 (1988), 134; DSB 10/1987, 1 ff.; FR v. 16.9.1987

15 S. Volesky/Scholten iur 1987, 289.

16 S. z.B. Spiegel 21/1987, 247.

17 S. Wernery, DSB 9/1987, 2.

18 S. hierzu Shoch/Hupp, Communications of the ACM, 25 (März 1982), 172 ff.; Dewdney, Scientific America 252 (März 1985), 16f.; Brunnstein AI 1987, 399; Burger 34.

als infiziert. Entweder besetzt das Virus zu diesem Zweck zusätzlichen Speicherplatz oder es überschreibt, um nicht aufzufallen, dessen Anfang. Wird nun dieses neue 'Wirtsprogramm' aufgerufen, verbreitet sich das Virus erneut. Auf diese Weise kann es in kurzer Zeit eine gesamte Anlage verseuchen und über Computernetze in andere Systeme verbreiten. Das Fatale an virulenten Programmen ist, daß die Viren ein Eigenleben entwickeln und sich auch von ihrem Erzeuger unkontrolliert und unbeeinflußbar vermehren können.[19]

Wie schnell eine weltweite 'Epidemie' möglich ist, zeigt folgendes Beispiel: Zur Weihnachtszeit 1987 sandte ein Student der Technischen Universität Clausthal über das hausinterne Datennetz seinen Kollegen einen elektronischen Weihnachtsgruß. Sie fanden in ihren Mailboxen ein neues Programm mit Namen 'Christmas' vor. Riefen sie es auf, erschien auf ihren Bildschirmen ein Weihnachtsbaum - und gleichzeitig durchsuchte das Programm (für die Anwender nicht sichtbar) alle vorhandenen Dateien des Kollegen nach Namens- und Adressenlisten ab und sandte an diese ebenfalls Kopien der Weihnachtsgrüße. Jeder, der das Programm in seiner Mailbox vorfand und es aufrief, verstärkte den Schneeballeffekt. Nachdem 'Christmas' über diesen Verbreitungsmechanismus das Universitätsnetz verlassen hatte, wurde es an verschiedene Rechenzentren in allen Kontinenten versandt. Die vielen Datenübertragungen führten zu einer spürbaren Belastung des EARN (European Academic Research Network). Da das Programm eine einfache und stabile Struktur hatte, gelang es schließlich 'Killer-Programmen', es wieder zu löschen.[20]

Die Manipulationsaufgabe eines solchen Programms hätte auch weniger harmlos sein können - eine logische Bombe etwa, die alle betroffenen Programme zu einem bestimmten Stichtag löscht, ein Befehl zum Ausspähen von Passwörtern oder ein Trojanisches Pferd, das in einem Rechenprogramm etwa zu einer Umkehrung aller Vorzeichen oder zur Vertauschung von Zahlen führt. Eine ständige Selbstmutation und der Befehl: "Schicke unter immer anderem Programmnamen eine Kopie an alle Adressen", könnte in dem Weihnachtsbaumbeispiel zu einer gezielten Überlastung des Datennetzes führen. Denkbar ist auch, daß die Manipulation erst dann ausgeführt wird, wenn alle Programme auf einem Datenträger oder in einem bestimmten System infiziert sind.[21]

Werden dadurch auf einen Schlag alle Programme zerstört, vermag dies in der zentralen Anlage eines Finanzamtes, einer Bank, eines Großunternehmens oder eines Krankenhauses einen verheerend hohen Einzelschaden (Typ IV) anzurichten. Doch schon allein der Verdacht einer Verseuchung kann eine Anlage wertlos machen. Ein sensitives System, von dessen Zuverlässigkeit Menschenleben abhängen oder in dem Staats- oder

19 S. hierzu näher Burger 15 ff., 63 ff., 191 ff.; Cohen 240 ff.; Dewdney, Scientific America 252 (März 1985), 14 ff.; Dierstein 87 ff.; Marshall, Science 240 (1988), 133; Witten, Abacus Nr. 4/1987, 7 ff.; Brunnstein AI 1987, 399 ff.; Schöneburg, Dornier Post 1/1987, 69 ff.; Müller DuD 1987, 482 ff.; Abel/Schmölz 76 ff.

20 S. hierzu DSB 1/1988, 1 ff.; FR v. 17.12.1987; Weser-Kurier v. 24.2. 1988; Burger 141f.; das Listing dieses Programms ist abgedruckt in Burger 287 ff.

21 Zu weiteren Viren-Manipulationen s. Burger 148 ff.

Geschäftsgeheimnisse gespeichert sind, muß dann abgeschaltet werden, weil die Folgen einer tatsächlichen Verseuchung unabsehbar wären.[22]

Viren gibt es erst relativ kurze Zeit. Sie sollen zuerst von Software-Herstellern entwickelt worden sein, um den Weg von Raubkopien verfolgen zu können.[23] Wissenschaftlich untersucht werden sie erst seit 1981 bzw. 1984.[24] Da eine Virenverseuchung Zweifel an der Datensicherheit in einem Unternehmen weckt, gibt es bisher nur wenige Hinweise auf realexistierende Viren.

In den USA, Großbritannien und Australien wurde gleichzeitig die Verseuchung von etwa 2000 Amiga-PCs gemeldet.[25] In den USA sollen außerdem der Rechner einer IBM-Niederlassung, das Computernetzwerk eines kalifornischen Unternehmens und Computerbanken mehrerer Regierungsstellen befallen worden sein.[26] In der Universität von Bethlehem (USA) wurde 1987 ein PC-Virus entdeckt, der erst in der "fünften Generation" damit begann, alle auf den Datenträgern vorhandenen Dateien zu vernichten.[27] Im Herbst 1987 wurden an einer Universität in Jerusalem PC-Programme von Viren gefallen, die den Befehl hatten, am nächsten Freitag dem 13. (einen Tag vor dem Jahrestag der israelischen Unabhängigkeitserklärung am 14. Mai 1988) alle infizierten Programme zu löschen.[28] Im Juli 1988 gab das FBI bekannt, daß ein Virusprogramm die Datenbanken mehrerer amerikanischer Regierungsstellen zerstört hat.[29]

Am 2. November 1988 brachen Großcomputer-Systeme an US-amerikanischen Universitäten wie Harvard, MIT und Stanford, aber auch in einer Kommandozentrale der US-Marine in San Diego zusammen, da sie die steigende Zahl der zu leistenden Rechenoperationen nicht mehr bewältigen konnten. Ursache war ein Viren-Programm, das über das sog. ARPA-Net und über das Science Internet verbreitet worden war. Betroffen waren in der Folge auch die NASA in Kalifornien und das Verteigigungsministerium in Washington.[30]

Nur mit massiven Anstrengungen gelang es Fachleuten, das Virusprogramm, das zu einer Bedrohung für bis zu 250.000 Computer hätte werden können[31], innerhalb von 24 Stunden unter Kontrolle zu bringen.

Geschrieben hat das Programm vermutlich der 23 jährige Sohn eines amerikanischen Computer-Sicherheitsexperten. Als Folge der Attacke kam es in den USA zu einer "Geheimkonferenz" im hermetisch abgeriegelten NSA-Hauptquartier in Fort Meade (Maryland). Hier sollen von Fachleuten aller Sparten Alarmpläne für mögliche weitere Virenfälle entwickelt worden sein.[32]

---

22 S. hierzu Burger 86f., 95, 145.

23 S. hierzu Marshall, Science 240 (1988), 133; Beier in FR v. 2.7.1988.

24 S. Kraus und Cohen.

25 Marshall, Science 240 (1988), 134; FR v. 2.7.1988; AP-Meldung vom 11.1.1988.

26 S. FR v. 2.7. und 5.7.1988; AP-Meldung vom 11.1.1988.

27 New York Times v. 31.1.1988.

28 S. New York Times v. 31.1.1988; zu weiteren Viren-Beispielen s. Burger 141 ff.

29 S. FR v. 5.7.1988.

30 S. Spiegel 45/1988, S. 294; The Detroit News v. 5.11.1988, S. 1; USA Today v. 7.11.1988, S. 1; CW v. 11.11.1988, S. 4.

31 S. CW v. 11.11.1988, S. 4.

32 S. Spiegel 47/1988, S. 252 ff.

Die Gefährlichkeit dieser Softwaremanipulationen resultiert daraus, daß die Aktion lange Zeit verborgen bleibt, der konkrete Angriff mit großer zeitlicher Verzögerung zur Manipulation ausgelöst wird und der Schaden sehr groß sein kann. Als 'Molotowcocktails der Zukunft'[33] könnten sie aus politischen Gründen eingesetzt werden und zum Handwerkszeug staatlicher Agenten gehören. Sie wären geeignete Mittel für Sabotageaktionen bei Konkurrenten und für Erpressungen. Einen anderen kriminellen Verwendungszweck zeigt das folgende Beispiel:

"Die Fakturierungsprogramme sollen in Unterschlagungsabsicht einen ganz bestimmten Kunden begünstigen, zum Beispiel Mengen oder Preise einer Lieferung reduzieren. ... Der Täter gibt die Manipulationsaufgabe an ein Virus, das er in einem unauffälligen Bereich des Systems absetzt und das sich aus infizierten Programmen wieder herauslöscht, es sei denn, es wäre im gewünschten Fakturierungsprogramm angekommen. Die Kundennummer ist dann das Stichwort für die Manipulationsaufgabe."[34]

Der Aufwand, ein schädigendes Programm zu schreiben, ist nicht sehr groß. Viren zum Beispiel können innerhalb weniger Stunden erzeugt werden. Das Virusprogramm selbst läuft in Sekundenbruchteilen ab und verseucht alle Programme eines unter Vollast im 'Time-Sharing-Betrieb' arbeitenden Systems innerhalb von Minuten.[35] Außerdem dürfte das geringe Entdeckungsrisiko die Hemmschwelle senken, solche logischen Angriffe durchzuführen. In großen Netzwerken wird schwer nachzuweisen sein, von welchem Terminal aus etwa ein Virus gestartet wurde - schon gar nicht, wenn das 'Wirtsprogramm' nach einem einmaligen Start wieder aus dem System entfernt wird oder sich selbst vernichtet.[36] Noch radikaler beseitigt die 'Explosion' einer logischen Bombe alle Spuren der Manipulation.[37]

Katastrophal wäre der Kopplungs- (Typ III) und der sich anschließende Komplexschaden (Typ V), wenn es einem oder mehreren Insidern gelänge, die künftig programmgesteuerten Telekommunikationsnetze durch Manipulation der Vermittlungssoftware auszuschalten - beispielsweise eine logische Bombe, die alle Systeme mit gleichen Programmen zur gleichen Zeit zum Absturz bringt. In einem Unternehmen oder einer Behörde würde ein solcher Anschlag auf die ISDN-Nebenstellenanlage zu einem kompletten Ausfall aller Telekommunikationsdienste führen - und damit jede vernetzte Produktion oder Bürokommunikation verhindern. Da TELEKOM im ISDN Anlagen zweier verschiedener

33 Burger 73.

34 Gliss in: Burger 96f.

35 Cohen benötigte z.B. für ein 200 Zeilen langes Virus für ein UNIX-Betriebssystem acht Stunden. Im Durchschnitt benötigte das Virus 30 Minuten, um das System vollständig zu verseuchen. - s. hierzu auch Dierstein 92 ff.

36 S. Burger 70f.

37 S. hierzu Paul CR 1985, 52; Volesky/Scholten iur 1987, 287.

Hersteller verwendet, könnte ein Anschlag die Verbindung für mindestens die Hälfte aller Anschlüsse zerstören. Und weil die noch funktionierenden Vermittlungsstellen dann durch ein schlagartig steigendes Kommunikationsbedürfnis überlastet werden, können die Folgen eines Anschlags noch erheblich gravierender sein, als in unserem Eingangsbeispiel beschrieben.

Wir können jetzt auch vermuten, was die Gründe für den Ausfall der drei Vermittlungsstellen in Düsselberg in unserem Eingngsbeispiel gewesen sein könnten. Nehmen wir an, alle drei Anlagen stammen vom gleichen Hersteller, so könnte die Software zum einen über den Zugang der Fernbetriebsführung manipuliert worden sein. In diesem Fall hätte der Angreifer auch erheblich mehr Systeme zerstören können. Die andere Möglichkeit wäre, daß ein Techniker während einer Wartungstätigkeit logische Bomben in die Vermittlungssystem-Software eingebaut hat. Dies wäre auch möglich, wenn die Anlagen von verschiedenen Herstellern stammen.

Externe Angreifer

Das Spektrum der Aktionsmöglichkeiten von externen Angreifern wird dadurch begrenzt, daß sie keinen unmittelbaren Zugang zu den IuK-Systemen haben und in der Regel auch nicht über Insider-Wissen verfügen. Allerdings ist in Betracht zu ziehen, daß sie sich beides durch freiwillige oder erzwungene Zusammenarbeit mit Insidern beschaffen können. Durch Erpressung oder Bestechung könnten sie Insider auch als ihre 'Werkzeuge' arbeiten lassen.

So hatten zwei Angestellte der First National Bank in Chicago ihren Komplizen den Geheimcode verraten, mit dem elektronische Banküberweisungen durchgeführt werden. Dadurch gelang es diesen, mittels Telebanking 70 Millionen Dollar auf ihre Konten zu überweisen. Entdeckt wurde der Vorfall, als die Bank einem der geschädigten Unternehmen mitteilte, daß dessen Konto um 20 Millionen überzogen war.[38] Ein weiteres Beispiel ist der DDR-Spion Prager, der von 1965 bis 1968 als Abteilungsleiter bei IBM in Sindelfingen arbeitete. Er kopierte dort im Rechenzentrum Bänder, die Daten über Planung, Produktion und Personal von rund 3000 Unternehmen enthielten.[39]

Von den verdeckten Sabotageakten abgesehen können externe Täter sämtliche physischen Angriffe durchführen, die als Aktionsmöglichkeiten von Insidern genannt wurden. Dies könnte sowohl von außen als auch nach einem erfolgreichen Eindringen geschehen.

So ist im November 1987 ein ehemaliger Angestellter von Australian Telecom, mit besten Kenntnissen über das unterirdische Kabelnetzwerk in die Untergrundschächte in Sydney eingedrungen und

38 S. Weser Kurier v. 20.5.1988.

39 S. Schlomann, Datenschutz-Berater 5/1987, 8f., s. dort auch 10 die Spionagetätigkeit für die DDR von G. Arnold bei IBM; s. weitere Fälle in Liebl u.a. 1987, 26 ff., 190 ff.

hat dort 24 der 600 schweren Kabelstränge an zehn sorgfältig ausgesuchten Stellen durchtrennt. 35.000 Telefonverbindungen in 40 Stadtteilen Sidneys fielen aus, Hunderte von Computersystemen brachen zusammen und die Banken, Versicherungen und Geschäfte in der Innenstadt waren ohne Verbindung zur Außenwelt. Vierhundert Mitarbeiter von Telecom waren 48 Stunden damit beschäftigt, den Schaden zu beheben. Da die Schnittstellen nur ein Zentimeter breit waren, mußten alle Kabel in den 27 Kilometer langen Tunnels mit der Hand abgetastet werden, um sie zu entdecken. Der Anschlag selbst hatte dagegen wohl weniger als eine Stunde Zeit gekostet.[40]

Die fehlende Nähe zum Anschlagsziel kann in vielen Fällen durch eine ausreichende Menge Sprengstoff ausgeglichen werden.

1983 zerstörte eine 'Feuerlöscherbombe' das Rechenzentrum von MAN in Gustavsburg.[41] Rund 4 Millionen Mark Schaden haben zwei Bomben angerichtet, die in einer Septembernacht 1985 fast gleichzeitig vor den Gebäuden der Firmen SCS in Hamburg und MBP in Dortmund explodierten und deren Rechenzentren verwüsteten.[42] Weitere Brand- und Bombenanschläge wurden im vorigen Kapitel dargestellt.[43]

Erheblich einfacher dürfte es für externe Angreifer sein, die Umgebungsbedingungen von IuK-Anlagen negativ zu beeinflussen. Sie könnten die Systeme indirekt schädigen, indem sie etwa die oben[44] beschriebenen elektromagnetischen Störungen absichtlich herbeiführen[45],das Klimasystem zerstören, die Stromversorgung unterbrechen oder das Gebäude beschädigen, in dem sie untergebracht sind.

Mit Hilfe einer Warensendung schmuggelten 1972 politische Extremisten eine Bombe in das Lagerhaus der Cooperative Society Ltd. in Belfast. Ihre Explosion im zweiten Stock des Lagerkomplexes führte zu einem Brand, der am Ende auch das Rechenzentrum im vierten Stock zerstörte.[46]

Insbesondere von der Stromversorgung geht ein hohes Verletzlichkeitsrisiko aus. Zum einen können nicht alle Strommasten auf freier Fläche gegen Anschläge geschützt werden. Allein von Januar bis November 1986 wurden 103 Anschläge auf Strommasten registriert.[47] Zum anderen zeigt ein Blick auf die Trassenführung im Verbundnetz, daß die Stromversorgung ganzer Regionen durch die koordinierte Zerstörung nur weniger Masten unterbrochen werden kann.

40 S. The Australian v. 23.11.1987 - zit nach Risk-Digest 5, 73 v. 13.12.1987, 1.

41 S. Zimmerli KR 1987, 341.

42 S. FR v. 3.9.1985; ÖVD-Online 8/1985, 9.

43 S. zu weiteren Anschlägen auch Dahmen ÖVD-Online 5/1985, 50.

44 S. Kap. 9.

45 S. hierzu ECM-Technology 1-2/1988, 3.

46 S. Norman 113 ff.

47 S. Innere Sicherheit Nr. 6 v. 29.12.1986, 18.

Angreifer könnten auch daran interessiert sein, eine Kommunikationsverbindung zu stören oder die übermittelten Daten zu manipulieren und damit insbesondere bei sehr zeitkritischen Übertragungen große Schäden anzurichten.

Spionage ist externen Angreifern zum einen möglich durch das Abhören von Leitungen. Am einfachsten gelingt dies an der Anschlußleitung des interessierenden Endgeräts. Aber auch Leitungen, auf denen gleichzeitig viele verschiedene Übertragungen stattfinden, können mit geeigneten Geräten abgehört werden. Dies gilt auch für den künftigen digitalen Mobilfunk.[48] Allerdings besteht bei ihm die Möglichkeit, Gespräche zu verschlüsseln.

Beispiele hierfür sind die bereits vorgestellten Fälle, in denen durch Abhören der Telekommunikationsverbindung Wirtschaftlichkeitsberechnungen eines Ölkonzerns und Nummern fremder Kreditkarten abgefangen wurden.[49] Im März 1988 wurde ein politisch sehr brisantes Autotelefongespräch zwischen dem Vorstandsvorsitzenden von Krupp-Stahl Crome und seinem Thyssen-Kollegen Kriwet abgehört und bekannt gemacht.[50]

Zum anderen lassen sich Militärinformationen, Bankgeheimnisse oder industrielle Forschungsergebnisse mit relativ einfachen Mitteln ausspähen, indem die - im Extremfall Hunderte von Metern weit reichende - kompromittierende Strahlung von Bildschirmen aufgefangen wird. Entsprechende Antennen in Plexiglasdächern von PKWs gelten bereits als Standard der Spionagetechnik. Deutschen Diensten soll eine Liste östlicher Geheimdienste in die Hände gefallen sein, in der mehrere hundert 'gute Aufnahmeplätze' verzeichnet waren.[51]

Soweit Telekommunikationsnetze den Zugang zu Datenverarbeitungsanlagen ermöglichen oder externe Angreifer sich den ihnen eigentlich versperrten Zugang eröffnen können, sind sie grundsätzlich in der Lage, alle logischen Angriffe durchzuführen, die auch Insidern möglich sind.

Daß dies möglich ist, zeigen nicht nur die bereits erwähnten erfolgreichen 'Hacks'. Neben dem 'NASA-Hack' mit Zugang zu 136 Rechnern ist es Externen auch in weiteren Fällen gelungen, bis in die höchsten 'Prioritäten' vorzudringen. In Berlin gelangten 1987 zwei Schüler "mit viel Fleiß und ein wenig Glück" in den Besitz des Zugangscodes für den 'Super User' des Rechenzentrums der Freien Universität. Sie konnten dadurch immer wieder in dieses System eindringen, die Passworte aller Benutzer auskundschaften und diese sogar verändern.[52] Auch bei dem 'Einbruch' in das PRESTEL-

48 S. Abel/Schmölz 279; für den digitalen Taxifunk s. z.B. Spiegel 34/1987, 56.

49 S. SARK 67; Risk Digest 5.16 v. 24.7.1987.

50 S. Spiegel 14/1988, 73.

51 S. hierzu Abel/Schmölz ; Schmidt DuD 1987, 276 ff.; Koenen KES 2/1985, 60f.; Sicherheitsberater 1986, 173f.; Schlomann, Datenschutz-Berater 5/1987, 9.

52 S. Spiegel 21/1987, 247.

System (das britische Btx) entdeckten die Hacker die Passwörter des System-Managers und des System-Editors und konnten dadurch zum Beispiel Bildschirmseiten ändern oder löschen.[53]

Noch lange nach seinem Ausscheiden aus einem deutschen Unternehmen nahm ein Programmierer über die Datenfernverarbeitung Manipulationen in den Dateien seines ehemaligen Arbeitgebers vor. In Baltimore/USA hat 1976 ebenfalls ein ehemaliger Angestellter innerhalb von vier Monaten über 40 mal auf das System seines früheren Arbeitgebers zugegriffen und sich Programme überspielt.[54] 1986 überwies der Volvo-Konzern 53 Millionen Kronen Aktienausschüttung elektronisch auf ein Bankkonto der Pensionsversicherungskassen Schwedens. Dort kam es jedoch nicht an. Hackern war es gelungen, die Überweisung abzufangen und auf ein Privatkonto bei der gleichen Bank umzuleiten. Die Polizei konnte zwar den Inhaber des Kontos verhaften, bevor er das gesamte Geld in Aktien umgetauscht hatte, nicht jedoch dessen Hintermänner.[55]

Aber auch ohne umfassende Zugriffskompetenz ist es nicht ausgeschlossen, von außen Viren in ein System einzubringen. Ein Virus kann nämlich auf alle Zugriffsebenen verschleppt werden, wenn Nutzer mit hoher Zugriffskompetenz Programme aufrufen, die bereits infiziert sind.[56] Auch bei Programmaustausch mit anderen datenverarbeitenden Stellen besteht die Gefahr, daß sich im benutzten Fremdprogramm ein Virus verbirgt.

Kollektive Aktionen

Daß Angriffsaktionen gegen die IuK-Technik nur von Einzelpersonen oder kleinen Gruppen ausgehen, darf keineswegs immer unterstellt werden. Wie bereits in der Vergangenheit könnten auch künftig unterschiedlichste Aktionen durchgeführt werden, an denen viele Angreifer mitwirken.

Organisierte Bereicherungsaktionen könnten nach dem Vorbild jener 90 Mitglieder starken Gruppe erfolgen, die in koordinierter Weise Bankautomaten leerte.[57] Mehr als vierzig Hacker tummelten sich letztlich in dem Rechenzentrum der Freien Universität Berlin, nachdem Passwörter in der Hackerszene die Runde gemacht hatten.[58]

Nach der Reaktorkatastrophe in Tschernobyl wurden zahlreiche Anschläge gegen Strommasten durchgeführt. Ebenso wäre es künftig auch denkbar, daß es etwa nach dem Bekanntwerden eines Überwachungsskandals zu vielen spontanen Zerstörungsaktionen von Telekommunikationseinrichtungen kommt. Wie das Beispiel der Strommasten

53 S. Zimmerli KR 1987, 339.

54 S. zu beiden Fällen Sieber 2/100.

55 S. FR v. 1.7.1986.

56 S. hierzu z.B. die Szenarien von Fix in Burger 305 ff.

57 S. Weser-Kurier v. 29.7.1987.

58 S. Spiegel 21/1987, 247.

zeigt, sind flächendeckende technische Versorgungssysteme leicht verwundbar. Millionen von Kabelkilometern und Tausende von Verteilstationen können nicht geschützt werden.

Automatisierte Verfahren der Informationsverarbeitung sind oft auf formalisiertes Verhalten der Benutzer angewiesen. Als besondere Form sozialen Protestes könnte sich daher herausbilden, das standardisierte Verhalten leicht abzuwandeln.[59] Vom 'versehentlichen' Ausfüllen falscher Felder in maschinenlesbaren Formularen über das Abschneiden von Formularen, Überweisen von Teilbeträgen, Geltendmachen von Rückforderungen und Auskunftsansprüchen bis hin zur automatischen 'Erzeugung' von Phantasiepersonen, hat der Widerstand gegen die Volkszählung 1987 bereits einen Vorgeschmack möglicher Behinderungsstrategien gegeben.[60]

Da die Sicherheitsmanager nicht ausschließen können, daß auch Agenten oder größere Terrorgruppen Angriffe auf die Nervenzentren und Nervenbahnen der 'Informationsgesellschaft' unternehmen, müssen sie mit der Möglichkeit rechnen, daß durch koordinierte Angriffe auch gezielte Schadensakkumulationen verursacht werden.

Vorbilder sind in anderen Bereichen leicht zu finden: So verübte die "Rote Zora" in einer Augustnacht 1987 gleichzeitig Anschläge auf acht Betriebe des Bekleidungsunternehmens Adler.[61] Um den Bau des Atomkraftwerks Lemoniz zu verhindern, hat die ETA mehrere überfälle und Sabotageanschläge auf das Kraftwerk unternommen, Hunderte von Anschlägen gegen Eigentum des Bauherrn verübt, mehrere leitende Angestellte entführt und ermordet, den Ingenieuren in Lemoniz gleiches angedroht und dadurch bis heute die Fertigstellung der Anlage verhindert.[62] Im Juni 1985 führten Guerillas eine Sabotage-Kampagne gegen das erste Atomkraftwerk auf den Philippinen durch und sprengten binnen zwei Wochen 26 Stromleitungsmasten, um das Stromnetz um den Reaktor zu zerstören.[63]

Durch ähnlich koordinierte Aktionen könnten beispielsweise sowohl eine Rechenzentrale als auch das dazugehörige Ersatz-Rechenzentrum zerstört oder die Originaldatenbestände ebenso wie die Sicherheitskopien vernichtet oder entwendet werden. Die Beschädigung einiger wichtiger Stromleitungen würde - von wenigen Notstromreserven abgesehen - alle Formen der Informationsverarbeitung in großen Regionen ausschließen. Um jede Telekommunikation in einem größeren Gebiet zu verhindern, könnten koordinierte Gruppen mehrere Leitungen, Vermittlungsstellen, Richtfunkeinrichtungen und Satellitensteuerungsanlagen systematisch zerstören. Auch unterschiedliche Kommunikationswege oder -medien könnten sich dann nicht mehr gegenseitig ersetzen.[64] Einen verheerenden Schaden würden sie - wie unser Eingangsbeispiel zeigt - auch schon erzielen, wenn es ihnen gelänge, in einigen Ballungszentren die Telekommunikationsknoten auszuschalten.

59 Ebenso SARK 79f.

60 S. zu solchen Aktionsformen auch Wechselwirkung 16 (1983), 21.

61 S. Spiegel 35/1987, 82 ff.

62 S. hierzu die Nachweise in Roßnagel 1987a, 19, 23, 27f. 37 und 47 mwN.

63 S. Roßnagel 1987a, 24 mwN.

64 S. hierzu auch SARK 72.

- Und alle diese Aktionen erfordern künftig nicht mehr unbedingt Feuer, Bomben und MGs. Sie könnten unter Umständen auch als 'elektronischer Guerrilla-Krieg'[65] - zeit- und ortsunabhängig, aus dem sicheren Versteck und ohne persönliches Risiko - durchgeführt werden.

Informationstechnische Abhängigkeit

Als letzter Aspekt möglicher Schadensverursachungen soll die Erpreßbarkeit von Anwendern der IuK-Technik betrachtet werden, die dadurch entstehen kann, daß sie vom Material oder Wissen anderer abhängig sind.

In vielen - insbesondere kleineren - Betrieben und Behörden sind die Informationsverarbeitungssysteme so kompliziert, daß nur noch einer oder wenige Spezialisten sie beherrschen. Ständige - mehr oder weniger 'handgestrickte' - Verbesserungen haben das System so unübersichtlich gemacht, daß der Behördenchef oder der Unternehmer, selbst wenn sie etwas von EDV verstehen, es nicht selbst überprüfen oder betreuen könnten. Fehlt für die ständigen 'Verbesserungen' auch noch die Dokumentation oder ist sie mangelhaft, so können sich auch neue Spezialisten kaum in das System einarbeiten.[66]

Die Mitgliedsländer der EG müssen derzeit etwa zwei Drittel aller mikroelektronischen Bauelemente aus den USA und Japan[67] und den überwiegenden Teil ihrer Computer aus den USA importieren. IBM allein hat bei Großrechnern einen Weltmarktanteil von 72%, die amerikanische Computerindustrie insgesamt einen Anteil von 93%.[68] Sie verkauft weltweit 80% aller Informationsverarbeitungssysteme.[69] Diese hohe Abhängigkeit hat bereits einzelne deutscher Anwender benachteiligt und die Politik der Bundesrepublik beeinflußt.

Nachdem IBM zehn Jahre lang die deutsch-russische Schiffahrtsagentur Transnautic in Hamburg mit Informationssystemen versorgt hatte, verweigerte die deutsche IBM-Niederlassung 1987 auf Weisung der US-Regierung plötzlich die Lieferung der neuesten Ausbaustufe, schloß alle Mitarbeiter der Agentur von Fortbildungskursen aus und kündigte an, auch gebraucht gekaufte IBM-Geräte weder zu installieren noch zu warten oder mit Software zu versorgen. Dem Unternehmen, das sich komplett auf ein neues System umstellen mußte, entstanden Verluste in Millionenhöhe.[70] Das Max-Planck-Institut für Meteorologie erhielt 1986 einen amerikanischen Höchstleistungsrechner erst nach massiven Vorstößen der Bundesregierung und "unter fast unzumutbaren Bedienungs- und Verwendungs-

65 Marshall, Science 240 (1988), 133.

66 S. hierzu z.B. SARK 161.

67 S. Informationstechnik 2000, Arbeitskreis Mikroelektronik 2.3.

68 S. Spiegel 5/1986, 127; bei Kleinrechnern hat IBM einen Weltmarktanteil von etwa 50%.

69 S. Informationstechnik 2000, Arbeitskreis Informationsverarbeitung 9.

70 S. Spiegel 9/1987, 76 ff.

auflagen" geliefert.[71] Auch den Universitäts-Rechenzentren in Stuttgart und Heidelberg schrieben die USA vor, wer und unter welchen Bedingungen mit den neu gelieferten Superrechnern sollte arbeiten dürfen.[72] Insbesondere über das 'Coordinating Committee for East-West-Trade Policy' (CoCom) in Paris haben die USA ihre starke Stellung ausgenutzt, um mit sicherheitspolitischen Argumenten den deutschen Ost-West-Handel und den von der Bundesrepublik gewünschten weiteren Ausbau der Handelsbeziehungen zu seinen östlichen Nachbarn zu behindern.[73]

Ähnliche Abhängigkeiten könnten sich durch die Monopolisierung von Wissen in den USA ergeben. 80% aller direkt abrufbaren wissenschaftlich-technischen Informationen sind in Datenbanken in den USA konzentriert, auf die 78% des Weltumsatzes entfallen.[74] Auch hier mehren sich die Fälle, in denen die USA sogar Nutzern aus dem verbündeten Europa den Zugang zu ihren Datenbanken, und zwar zu 'unclassified informations', verwehren.[75] Der amerikanische Präsident hat beispielsweise bei der Vorstellung eines nationalen Supraleitungs-Programms zugleich angekündigt, die Zugriffsmöglichkeiten auf amerikanische Datenbanken mit gespeichertem Supraleitungs-Wissen für Ausländer zu reglementieren.[76]

Bleibt auch künftig diese hohe Abhängigkeit bestehen, ist es in keiner Weise auszuschließen, daß die USA und andere Staaten den Zugang zu elektronisch gespeichertem Wissen oder die Lieferung von IuK-Technik als strategisch zu behandelnde Ressource nicht nur im militärischen Wettrüsten, sondern auch im internationalen ökonomischen Wettlauf einsetzen und damit ihre Vormachtstellung gegenüber Europa und der Bundesrepublik weiter ausbauen. Ein Lieferstopp für Hardware, Software, Ersatzteile und Informationen würde zwar auch die amerikanische Exportindustrie schädigen, aber in dem betroffenen Land erheblich bedeutendere Schäden verursachen. Aufgrund ihres ökonomischen Drohpotentials könnten die Vereinigten Staaten auch leicht die Politik der Bundesrepublik beeinflussen: Versucht die Bundesrepublik, insbesondere in ihren Beziehungen zu ihren östlichen Nachbarn, politisch eigene Wege zu gehen, läuft sie Gefahr, von US-Technologien und -informationen abgeschnitten zu werden.[77] Sie wäre durch eine weitere Kette an die Politik der USA gebunden.[78]

71 Häussler CM 9/1986, 1.

72 S. Charlier CM 7/8/1987, 19; Communale v. 11.2.1988.

73 S. hierzu z.B. Jacobsen, Nötzold und Vogel, Blätter für deutsche und internationale Politik 3/1988, 359 ff.; Becker NfD 1988, 26.

74 S. Ulrich, Zeit 44/1987, 13; Becker 1984, 19.

75 S. Becker NfD 1988, 21 ff.

76 S. Ulrich, Zeit 44/1987, 13.

77 So auch Schulte-Hillen/v. Weitersheim in ihrer 'geheimen' EG-Studie "Analyse von Beschränkungen des Zugangs zu außergemeinschaftlichen Informationsquellen" wie sie Becker in NfD 1988, 21 ff., 25 referiert hat.

78 S. zur internationalen Abhängigkeit ähnlich auch SARK 177 ff., 206f.

Angriffsformen des 21. Jahrhunderts

Gab es alle diese Mißbrauchsmöglichkeiten aber nicht auch schon in der Vergangenheit? Werden nicht einfach bisherige Tatformen auf den Computer übertragen? Oder besitzt die künftige Bedrohung vielleicht doch eine besondere, eigene Qualität?

Auch in der Vergangenheit haben untreue Kassierer Gelder unterschlagen, verschuldete Buchhalter Finanzen veruntreut, verführte Sekretärinnen Akten kopiert oder gefilmt, bestochene Ingenieure Forschungsergebnisse verraten, verschuldete Sachbearbeiter Urkunden gefälscht und verärgerte Mitarbeiter Sabotage verübt. Auch bisher wurden Telefone abgehört, Postsendungen absichtlich fehlgeleitet[79] oder unterschlagen.[80] Terroristen haben Brand- und Bombenanschläge unternommen. Kriminelle haben Banken beraubt, Unternehmen bestohlen und reiche Opfer erpreßt. Und auch der hohe Energie- und Rohstoffbedarf machte die Bundesrepublik vom Ausland abhängig.

Diese Bedrohungsformen des 19. und 20. Jahrhunderts werden weiterbestehen und mit der Verschiebung sozialer Funktionen auf die IuK-Technik auch auf diese übertragen. Insofern ersetzen die geschilderten Mißbrauchsformen veraltete Aktionsmöglichkeiten oder vermehren - wie das Beispiel der informationstechnischen Abhängigkeit zeigt - die bisherigen Probleme. In sehr vielen Fällen verändert sich durch die Übertragung auf die IuK-Technik aber auch ihr Charakter - die Angreifer können künftig die spezifischen Vorteile dieser Technik nutzen. So wird es ihnen möglich sein, in der hohlen Hand den Informationsgehalt zu entwenden, für den sie früher ganze Güterzüge voll Akten hätten wegschaffen müssen. Künftig können sie in Sekundenschnelle Daten kopieren, für deren Ablichtung sie früher Jahre gebraucht hätten. Sie können diese Daten in einem Augenblick an viele Adressaten gleichzeitig verschicken - was früher schon bei einen Empfänger Tage gedauert hätte. Während bisher eine einzige Urkundenfälschung mühsame Handarbeit war, werden sich künftig solche Manipulationen automatisch tausendfach durchführen lassen. Ein Spion, der in der Vergangenheit immer nur einige wenige Telefongespräche abhören konnte, läßt sich künftig Tausende von Gesprächen, Text-, Daten- und Bildübertragungen automatisch auswerten.[81]

Völlig neu und mit bisherigen Angriffsformen nicht zu vergleichen sind die 'logischen Angriffe' in Form von Viren, Würmern, Zeitbomben, Falltüren und Trojanischen Pferden. Viren und Würmer ermöglichen, in vernetzten Systemen Angriffe in kurzer Zeit automatisch zu vervielfältigen und zu verbreiten. Logische Bomben in weitverbreiteten Betriebssystemen könnten sogar völlig entkoppelte Prozesse zeitgleich ausfallen lassen (Kopp-

79 In einem Hamburger Paketpostamt wurde ein halbtags beschäftigter Student dabei ertappt, wie er auf ein Paket an den Militärischen Abschirmdienst vor die Postleitzahl das Staatenkürzel "DDR" schrieb - s. Spiegel 38/1987, 18.

80 S. hierzu Spiegel 38/1987, 18. Aus der Postverteilerstelle des römischen Flughafens wurde im September 1987 ein Paket mit einer Milliarde Lire (etwa 1,4 Mio. DM) in Banknoten unterschlagen, das eine Züricher Bank an die italienische Zentralbank geschickt hatte - s. FR v. 14.9.1987.

81 Der Schaden ist im Einzelfall daher auch zwanzig- bis vierzigmal höher als bei konventionellen Delikten - s. Abel/Schmölz 11.

lungsschaden - Typ III). 'Explodieren' sie in der Vermittlungssoftware eines Telekommunikationssystems, zerstören sie mit einem Schlag Tausende oder Millionen von Kommunikationsverbindungen.

Diese Angriffsformen des 21. Jahrhunderts nutzen die Offenheit der 'Informationsgesellschaft'. Wir können daher als ein weiteres Zwischenergebnis festhalten: Je freier und je breiter die Informationszugänge und Kommunikationsmöglichkeiten sind, desto verletzlicher scheint die Gesellschaft zu sein. Ob es eine offene 'Informationsgesellschaft' überhaupt geben kann, scheint somit sehr fraglich und hängt von ihren Möglichkeiten ab, Informationen und Kommunikationen zu sichern, ohne sie einzuschränken.

12. Möglichkeiten der Sicherung

Bereits in der Vergangenheit wurden gegen Angriffe auf IuK-Systeme Sicherungsmaßnahmen ergriffen. Diese werden künftig von den Sicherungsbeauftragten verbessert, effektiviert und ergänzt werden. Ebenso wie IuK-Technik neue oder qualitativ andere Angriffsformen ermöglicht, werden die Verantwortlichen mit ihrer Hilfe auch technische Sicherungen aufbauen, die mit klassischen Mitteln nicht möglich waren. Um ihren Vorgesetzten und Auftraggebern ein praktikables und finanzierbares Sicherungssystem vorschlagen zu können, müssen sie zwischen vielen Sicherungsmöglichkeiten eine objektgerechte Auswahl treffen. Zunächst interessieren sie sich für die Palette der Sicherungsmaßnahmen, die für sie theoretisch in Frage kommen, den Grad der Sicherheit, den sie bieten, und das Mindestrisiko, das sie nicht abdecken können. Die tauglich erscheinenden Bausteine versuchen sie, zu einem integrierten Sicherungssystem zusammenzufügen.

Das *theoretisch mögliche Sicherungsniveau* wird in diesem Kapitel durch die Sicherungsmaßnahmen beschrieben, die zwischen den Jahren 2000 und 2020 Stand der Technik sein dürften.[1] Die Einschränkungen, die in der Praxis zu erwarten sind, werden dann in den nächsten drei Kapiteln dargestellt.

Sicherungssysteme beruhen auf zwei sich ergänzenden Konzepten. Das erste sieht vor, durch technische oder organisatorische Maßnahmen das Schadenspotential eines Angriffs möglichst weit zu reduzieren. Das zweite Konzept versucht, den Erfolg von Angriffen dadurch zu verhindern, daß es gegen jede Aktionsform soweit möglich mehrere Schutzebenen vorsieht. Sie sollen die Erfolgsschwelle eines Angriffs soweit erhöhen, daß die erforderlichen Mittel, um das Ziel zu erreichen, die Möglichkeiten des Angreifers übersteigen oder die möglichen Vorteile des Angriffs aufwiegen.

Um dem jeweiligen Risiko gemäß differenzierte Schutzstrategien verfolgen zu können, werden die zu schützenden Objekte je nach Sensitivität der Daten und Systeme in verschiedene Sicherheitszonen und Schutzklassen eingeteilt. Vorbildhaft könnten insoweit die Schutzkategorien werden, die das US-Verteidigungsministerium in seinen "Trusted Computer System Evaluation Criteria" 1983 eingeführt und 1985 revidiert hat und die 1987 das National Computer Security Center in seinen "Trusted Network Interpretation of the Trusted Computer Evaluation Criteria" auf ganze Rechnernetze ausgeweitet hat.[2] Die dargestellten künftigen Sicherungsmaßnahmen dürften in ihrer Gesamtheit wohl nur für die allerhöchste Sicherheitskategorie zu erwarten sein.

---

1 Zum folgenden s. ausführlicher Hammer, Arbeitspapier Nr. 8; Pordesch, Arbeitspapier Nr. 6; Wedde, Arbeitspapier Nr. 9.

2 S. hierzu US-Department of Defense; National Computer Security Center; Cerny 1985(a), 255 ff.; ders. 1985(b), 171 ff.; DSB 2/1988, 1 ff.; zu Sicherheitsklassifizierungen s. auch Abel/Schmölz 29 ff.; Weck 68 ff.; Breuer 211 ff.

Maßnahmen zur Schadensbegrenzung

Die künftigen Möglichkeiten zur Schadensbegrenzung haben wir schon weitgehend kennengelernt, als wir das Problem der Beherrschbarkeit unbeabsichtigter Fehler erörterten. Da sie unabhängig von konkreten Fehlerursachen konzipiert werden, schützen sie auch gegen beabsichtigte Schädigungen. Es genügt hier, sie noch einmal kurz in Erinnerung zu rufen und nach dem verbleibenden Mindestrisiko zu befragen - also nach dem Risiko, das bleibt, wenn sie ihrer Bestimmung gemäß funktionieren.

Schadensbegrenzende Schutzmechanismen können Angreifern bekannt sein und so gezielt ausgeschaltet werden. Grundsätzlich wird ihre Effektivität gegen Angriffe daher geringer sein als die gegen unbeabsichtigte Fehler.

Künftige Konzepte für verteilte Systeme erlauben eine Dezentralisierung von Anlagen und Anwendungen unter Sicherheitsgesichtspunkten. Die Verlagerung von 'Intelligenz' innerhalb eines Netzes von Zentralrechnern in die Endgeräte der Teilnehmer läßt viele zentrale Angriffsobjekte entfallen. Der mögliche Schaden eines isolierten Angriffs kann dann meist auf die dezentrale Einheit begrenzt werden. Sind sensitive Daten auf dezentrale Speicher verteilt, sinkt auch die Wahrscheinlichkeit ihrer Ausspähung[3]. Dezentralisierung kann den Aufwand beträchtlich erhöhen, um einen großen Schaden zu verursachen. Er ist bei einer koordinierten Aktion mehrerer dennoch nicht auszuschließen. Je verteilter das System ist, desto schwieriger ist es aber auch, für alle Teile den gleichen Sicherheitsstandard zu gewährleisten. Angreifer jedenfalls suchen sich immer die schwächste Stelle heraus.

Fehlertolerante Systeme, die sicherstellen, daß beim Auftreten eines Fehlers das umgebende Gesamtsystem in einen stabilen, schadensarmen Zustand versetzt wird, können auch gezielte Angriffe in ihrer Schadenswirkung begrenzen.

Redundante Systeme mit Parallelverarbeitung verhindern die Unterbrechung des Betriebs, wenn nur eine Anlage ausfällt. Keinen Schutz können sie allerdings bieten, wenn beide zugleich angegriffen werden oder die nur einmal vorhandene Infrastruktur zerstört wird. Gleiches gilt für Ersatzrechenzentren. Sie können den Schaden auf kurzfristige Ausfälle begrenzen, setzen jedoch voraus, daß der Daten- und Programmbestand sowie ein Minimum an Infrastruktur erhalten geblieben sind. Fehlt es an diesen oder werden die 'warmen' Rechenzentren gleichzeitig oder die 'kalten' nach ihrer Errichtung angegriffen, fällt auch ihr Sicherungsbeitrag aus. Vereinbarungen zwischen Ersatzrechenzentren, sich im Notfall gegenseitig zu ersetzen, helfen bei vereinzelten Ausfällen, versagen jedoch bei mehreren koordinierten Angriffen.

Sicherungskopien von Daten und Programmen zu erstellen und an einen geschützten Ort auszulagern, ermöglicht auch nach einem Angriff auf die Originale, den Betrieb mit den Kopien fortzusetzen. Ein physischer Angriff kann aber auch die Sicherungskopien mit einbeziehen. Seine Erfolgschancen werden jedoch mit jedem gut gesicherten Duplikat

3 S. Abel RDV 1988, 75.

geringer. Bleiben Manipulationen längere Zeit unbemerkt, sind sie ebenfalls in allen Sicherungsgenerationen zu finden.

Eine in dieser Hinsicht besonders heimtückische Virenart stellt Burger vor[4]: Ein Virus, das in kürzester Zeit alle Programme eines Systems befallen hat, schleust als Manipulationsverfahren eine Funktion ein, mit deren Hilfe alle Datensätze verschlüsselt werden. Da alle verseuchten Programme jedoch diesen Verschlüsselungsalgorithmus beherrschen, bringen sie die Daten vor der Verarbeitung immer wieder in lesbare Form. Alle Arbeiten werden weiterhin zur Zufriedenheit erledigt, bis die gesamten Datensicherungen durch verschlüsselte ersetzt sind. Werden nun, beispielsweise datumsabhängig, die infizierten Programme durch die Viren gelöscht, sind auch die Datensicherungen wertlos, weil keine Programme mehr existieren, die sie entschlüsseln können.

Sicherungskopien schützen gegen das Verlustrisiko von Daten, wenn Datenträger entwendet werden, um zu schädigen oder zu erpressen. Andererseits erhöht jedoch jede Kopie das Risiko der Spionage. Diesem Risiko kann nur durch verschlüsselte Speicherung begegnet werden. Aber auch diese ist nicht ohne Probleme.[5]

Physische Angriffe auf das Telekommunikationsnetz werden in ihrem Schadensausmaß durch die 'Kreuz-und Quervermaschung' des Fernnetzes stark reduziert und auf den Ortsbereich beschränkt. Der Grundsatz der Zwei-Wege- und Zwei-Medienführung im Fernnetz, nach dem für alle wichtigen Fernstrecken sowohl Richtfunk- als auch Kabelverbindungen bestehen und für beide Medien jeweils zwei getrennte Trassen benutzt werden sollen, macht den Ausfall von Kommunikationsmöglichkeiten auf der Fernebene durch einen oder auch zwei Anschläge unmöglich. Zu berücksichtigen ist allerdings, daß an bestimmten Vermittlungsstellen die Trassen und Medien zusammengeführt werden. Ausfälle, die über den Bereich einer Ortsvermittlungsstelle hinausgehen, durch physische Angriffe zu verursachen, ist im künftigen ISDN-Netz zwar nicht ausgeschlossen, aber nur mit erheblichem Aufwand zu erreichen. Gegen Manipulationen der Vermittlungssoftware hilft die Redundanz der Hardware allerdings wenig. Der einzige schadensmindernde Effekt geht bei einem solchen Angriff davon aus, daß die Software von zwei verschiedenen Herstellern (Siemens und SEL) stammt: Durch denselben Softwareangriff kann deshalb maximal die Hälfte der Vermittlungsstellen betroffen werden. Wegen der hierarchischen Struktur des Vermittlungsnetzes würden dadurch aber erheblich mehr als die Hälfte aller Kommunikationswünsche unbefriedigt bleiben.

Schadensbegrenzende Schutzmechanismen verringern die Verletzlichkeit gegenüber absichtlichen Schädigungen, können sie allein aber nicht auf ein erträgliches Niveau reduzieren. Sie sind daher um Sicherungsmaßnahmen zu ergänzen, die Mißbrauchsaktionen gezielt zu verhindern suchen.

4 Burger 64.

5 S. hierzu unten unter 'Verschlüsselung'.

Verhinderung von Angriffsfolgen

Die spezifische Folge tiefgestaffelter Schutzmaßnahmen gegen jede denkbare Angriffsform darzustellen, würde den Rahmen dieser Untersuchung bei weitem sprengen. Da viele Schutzvorkehrungen gleichzeitig unterschiedliche Angriffsformen verhindern und sie alle sich zu einem integrierten Sicherungssystem verbinden sollen, genügt es für unsere Zwecke, exemplarisch das Sicherungssystem eines verteilten Computernetzwerks zu betrachten.

Physische Schutzmaßnahmen

Als Schutzmaßnahme gegen physische Angriffe wie Zerstörung oder Entwendung von Geräten oder Datenträgern können Gebäude so angeordnet werden, daß die sensitiven Räume der Netzzentrale mit dem Großrechner und seiner Infrastruktur möglichst geschützt liegen und dem Stand der Technik entsprechend gegen Feuer, Wasser und mechanische Gewalt ausgelegt werden.[6] Ergänzt wird dieser Schutz durch Zutritts- und Außenhautsicherung sowie Ein- und Ausgangskontrollen.[7] Letztere sollen verhindern, daß unberechtigte Personen die Anlagen betreten und Zugangsberechtigte Sabotagemittel hinein- oder entwendete Gegenstände herausbringen. Die Kontrollen werden durch IuK-Technik unterstützt. Mit Hilfe von Chipkarten werden zeitlich und räumlich differenzierte Zutrittsberechtigungen vergeben. Ob auch die richtige Person die Chipkarte verwendet, wird durch eine automatische Kontrolle unveränderlicher Kennzeichen geprüft. Hier können die Verantwortlichen wählen zwischen dem Abgleich von Fingerabdrücken, Netzhautbildern, Stimmen, Unterschriften oder Gesichtern.[8] Die Kontrolle besonders zu schützender Räume erfolgt durch Bewegungsmelder und Videokameras. Bildverarbeitende Systeme vergleichen ständig das gespeicherte Bild eines Raumes mit dem aufgenommenen und geben bei Veränderungen Alarm. Die baulichen und technischen Schutzmaßnahmen sollen Angreifer so lange aufhalten (Widerstandszeitwert), bis Werkschutz oder Polizei eingreifen können.

Der Schutz gegen Spionage in Telekommunikationsnetzen kann durch neue Materialien verbessert werden. Zwar können auch Glasfaserkabel angezapft und abgehört werden, doch ist das Aufschalten technisch nicht einfach. Es kann zudem sofort automatisch angezeigt werden, wenn das Kabel mit einem überwachten Gasmantel umkleidet ist und

6 S. z.B. Breuer 19 ff.; Weese/Lessing KES 3/1987, 143 ff.; Weck 77 ff.; Abel/Schmölz 33 ff.; Droux 248 ff.

7 S. zu diesen z.B. Abel/Schmölz 33 ff., 47 ff.; Weese/Lessing, KES 3/1987, 143 ff.; Dahmen ÖVD-Online 5/1985, 46 ff.; Breuer 161 ff.

8 S. z.B. Weck 88 ff.; Hennings/Müller ÖVD-Online 3/1985, 77; Wirtschaftswoche 37/1986, 69f.

dessen Druckabsenkung registriert wird.[9] Derzeit ist allerdings kein Verfahren bekannt, auch den Funkverkehr vor unzulässigem Abhören zu schützen.[10]

Die Auswertung der kompromittierenden Abstrahlung von Bildschirmen, Druckern, Datenverarbeitungs- und Übertragungsgeräten kann nahezu ausgeschlossen werden. Entweder werden die Geräte mit einem zweiten abstrahlsicheren Gehäuse ummantelt oder sie legen über einen eigenen Sender ein Störfeld um sich herum oder sie verarbeiten nur codierte Signale. Diese Sicherungsmöglichkeiten sind derzeit in der Bundesrepublik entweder überhaupt nicht oder ausschließlich für sehr wenige besonders schutzbedürftige Datenverarbeitungen verfügbar und bedürfen einer Genehmigung der Zentralstelle für das Chiffrierwesen. Wenn unsere östlichen Nachbarn in einigen Jahren ebenfalls über solche Sicherungen verfügen, werden die Versuche aufgegeben, sich so gegen einen Transfer sensitiver Technik zu schützen. Bis dahin vermag die lückenlose Auskleidung eines Raumes einschließlich Fenster, Türen, Kabeldurchführungen oder Wasserleitungen mit Kupfer- oder Eisenfolie die kompromittierende Strahlung abzuschirmen. Das Ummanteln der Geräte mit einem Faradayschen Käfig kann die Abstrahlung zwar nicht verhindern, aber reduzieren.[11]

Durch die physischen Sicherungen können Angriffe von außen weitgehend erkannt und ausgeschlossen werden. Eine vollständige Sicherheit gegen solche Angriffe ist allerdings auch bei sehr hohem Aufwand nicht zu gewährleisten. Die physischen Sicherungen versagen immer dann, wenn die zur Wirkung gebrachte Gewalt größer ist als der Wert, für den die Sicherung ausgelegt ist. So dürften nur wenige Rechenzentren den Angriff mit einem Lastwagen voller Sprengstoff oder mit tragbaren Raketen überstehen, wie sie schon heute und erst recht morgen auf dem schwarzen Markt zu erwerben sind. Physische Sicherungen vermögen böswillige Insider nur von sehr plumpen Sabotage- oder Diebstahlsaktionen abzuhalten. Raffinierte Mißbrauchsmethoden von Insidern sind mit anderen Mitteln zu bekämpfen.

Zugangssicherung

Physische Schutzmaßnahmen können allerdings nur vor dem Angreifer schützen, der gewaltsam gegen Zentralen oder Vermittlungsknoten eines Netzwerkes vorgeht. Sie verhindern nicht, daß jemand immateriell von dezentral verteilten Terminals aus auf Daten und Programme zugreift. Gegen den unberechtigten logischen Zugang sollen daher Verfahren schützen, die bei jeder Konkaktaufnahme die Berechtigung des Benutzers prüfen.[12] Um Zugang zu einem so geschützten Rechner zu erhalten, muß ein Benutzer

9 S. Abel DuD 1987, 446.

10 S. Abel/Schmölz 279.

11 S. z.B. Schmidt DuD 1987, 276 ff.; Abel/Schmölz 306 ff.; Wirtschaftswoche 34/1986, 62 ff.

12 S. z.B. Weck 157 ff.; US National Computer Security Center 5 ff.; US-Department of Defense 15 ff.

heute eine ihm verliehene Benutzernummer und ein von ihm ausgesuchtes Paßwort eingeben. Da dieses Verfahren aber jedem den Zugang erlaubt, der beide irgendwie ausgespäht oder ausprobiert hat[13], wird der Systembenutzer künftig seine Berechtigung mit Hilfe einer Chipkarte und seine Identität mit einer elektronisch analysierten eigenhändigen Unterschrift nachweisen. Um die Chipkartenkennung oder die digitalen Signale der Unterschriftsanalyse gegen Abhören zu sichern, werden Prozessoren in die Terminals eingebaut, die diese Signale verschlüsseln. Ein so gesichertes System dürfte den Zugang Unberechtigter nahezu ausschließen. Sie könnten nur dann noch hineingelangen, wenn sie mit einem Berechtigten zusammenarbeiten oder in den Besitz einer Chipkarte kommen, wobei es ihnen gelingen muß, die Unterschrift ausreichend echt - vielleicht mit Roboterhilfe - nachzuahmen.

In den allgemein zugänglichen Telekommunikationsnetzen kann eine besondere Zugangsberechtigung zu einem Rechner auch dadurch gesichert werden, daß eine geschlossene Benutzergruppe gebildet wird und die Mitgliedschaft automatisch überprüft oder der Anrufende vom Rechner zurückgerufen wird. Allerdings verhindert die Identifikation an Hand der Anschlußkennung jede Mobilität des Nutzers.

Identifikation und Übertragungssicherheit

Um in einem allgemein zugänglichen Netz sicherzustellen, daß bei Teletransaktionen - Telebanking, Teleshopping, Informationsabruf und Behördenverkehr - derjenige, der eine Nachricht versendet, Geld umbucht oder eine kostenpflichtige Information abruft, immer auch derjenige ist, der zu sein er vorgibt, und um zu gewährleisten, daß rechtsverbindliche Nachrichten nicht unterwegs manipuliert werden, arbeitet die Gesellschaft für Mathematik und Datenverarbeitung (GMD) an dem Konzept 'TeleTrusT'.[14] Dieses Ziel soll erreicht werden durch ein öffentliches Verschlüsselungsverfahren, das mit asymmetrischen Schlüsseln arbeitet. Jeder Sender fügt seiner Nachricht eine mit seinem geheimen Schlüssel verschlüsselte Signatur hinzu, die der Empfänger mit dem öffentlichen Schlüssel des Absenders wieder entschlüsselt. Er kann die Signatur nur dann entschlüsseln, wenn sie mit dem zu ihr passenden geheimen Schlüssel verschlüsselt worden ist. Solange nur der Berechtigte über den Schlüssel verfügt, kann durch dieses Verfahren nachgewiesen werden, daß die Nachricht auch von ihm stammt. Die Signatur besteht aus einer eigens errechneten und dann verschlüsselten Kurzfassung der Nachricht. Die Nachricht selbst wird im 'Klartext' übermittelt. Wurde die Nachricht unterwegs verändert, unter-

13 Auf diese Weise wurde in nahezu allen 'Hacks' der Einstieg in das System ermöglicht.

14 S. hierzu näher Hammer DuD 1988, 391 ff.; Burkert GMD-Spiegel 1/1986, 43 ff.; Herda, GMD-Spiegel 1/1986, 17 ff.; ders., GMD-Spiegel 1/1988, 45 ff.; ders. 1985, 35 ff. Goebel, GMD-Spiegel 1/1988, 34 ff.; Kruse/Struif, GMD-Spiegel 1/1986, 37 ff.; Raubold, GMD-Spiegel 1/1986, 9 ff.; Rihaczek, GMD-Spiegel 1/1986, 13 ff; ders. DuD 1987, 240 ff.; Struif, GMD-Spiegel 1/1986, 27 ff.; ders., GMD-Spiegel 1/1988, 34 ff.; s. hierzu auch Chaum DuD 1988, 26 ff.; Abel/Schmölz 322 ff.; Harmsen/Weiß 34 ff.

scheidet sich die Kurzfassung der empfangenen Nachricht von der entschlüsselten Kurzfassung aus der Signatur. Solange das Kryptogramm der Signatur nicht gebrochen werden kann und die Kurzfassungen identisch sind, kann der Empfänger sicher sein, daß die Nachricht echt ist.

Um ausreichend sicher zu sein, muß TeleTrusT gewährleisten, daß der Schlüssel nicht berechnet und nur vom Berechtigten genutzt werden kann. Zu diesem Zweck wird das Schlüsselpaar automatisch und geheim errechnet. Der öffentliche Schlüssel wird in ein öffentliches Verzeichnis aufgenommen und der geheime auf einer Chipkarte gespeichert. Niemand, auch nicht der Berechtigte, soll den geheimen Schlüssel kennen. Damit nun nicht ein Dieb die Karte benutzen kann, wird die Funktion der Chipkarte nur ausgelöst, wenn die persönliche Identifikationsnummer eingegeben und eine eigenhändige Unterschrift geleistet wurde. Das Verschlüsselungsverfahren gilt derzeit als praktisch sicher. Es arbeitet mit modularer Arithmetik auf der Basis sehr großer Primzahlen.[15] Den geheimen Schlüssel mit einer Länge von 256 Bits aus dem öffentlichen zu berechnen dauert bei den derzeitigen Verahren zur Faktorisierung von Primzahlen und der heutigen Rechnerleistung etwa 10^{15} Jahre.[16]

Dieses Konzept dürfte vor allem Anwendung finden, um den elektronischen Zahlungsverkehr[17] und rechtswirksame Telehandlungen (Vertragsabschlüsse, Klagen, Anträge) abzusichern. Es könnte auch als Zugangskontrolle von Rechnern und Netzen genutzt werden[18]: Alle öffentlichen Schlüssel der zugelassenen Benutzer werden in dem Zugangskontrollsystem abgespeichert. Der Berechtigte muß sich mit einer jedesmal veränderten Zeichenfolge, die er vom Rechner erhält und mit seiner Chipkarte verschlüsselt, anmelden und wird zugelassen, wenn nach der automatischen Entschlüsselung der Text mit dem ursprünglichen übereinstimmt.

TeleTrust bringt einen hohen Sicherheitsgewinn durch die Einmaligkeit des Schlüsselpaares, dessen physische Bindung an eine Chipkarte und deren Aktivierung durch eine Identifikationsnummer und eine unverwechselbare Unterschrift. Alle diese Sicherheitsvorkehrungen schützen jedoch nicht davor, daß jemand sich unter einer falschen Identität eine Chipkarte ausstellen läßt. Die Identifikationssicherheit ist daher letztlich nur so hoch wie die Sicherheit staatlicher Ausweisdokumente.[19] Sie setzt außerdem eine voll vertrauenswürdige Schlüsselverwaltung voraus.[20]

---

15 S. hierzu z.B. Denning sowie unten Kap. 14.

16 S. Hammer DuD 8/1988, 394; bei einer Länge von 56 Bits benötigt man immerhin noch 3000 Jahre - s. Abel/Schmölz 317.

17 S. hierzu näher Harmsen/Weiß 51 ff.

18 S. z.B. für den Bankenbereich Harmsen/Weiß 50.

19 So ist es zum Beispiel einem Betrüger in Göttingen zweimal gelungen, sich auf falsche Namen Personalausweise austellen zu lassen - s. FR v. 18.6.1988.

20 Zu weiteren Sicherheitsrisiken in der Organisation von TeleTrusT s. Hammer DuD 8/1988, 398 ff.; für den Bankenbereich s. Harmsen/Weiß 31, 44.

Zugriffssicherung

Gegen unberechtigte Einsichtnahme, Veränderung oder Löschung von Daten und Programmen sollen Capability-Verfahren schützen, die differenzierte Zugriffsrechte verteilen und kontrollieren. Sie stellen dem Benutzer Daten, Programme und Handlungsmöglichkeiten nur in dem Umfang zur Verfügung, in dem er sie zur Erfüllung seiner Aufgaben oder im Rahmen seiner Berechtigung benötigt.[21] Der Sachbearbeiter kann also nur auf die Daten der Personen zugreifen, für deren Anfangsbuchstaben er zuständig ist, der Bankkunde nur sein eigenes Konto verändern, der Arzt nur die Krankheitsgeschichte des Patienten lesen, der ihm seine Versicherungs-Chipkarte gegeben hat. Die Programme zur Zugriffssicherung sind umso sicherer, je näher sie innerhalb der Systemarchitektur am Betriebssystem angesiedelt sind.[22] Sofern sie als Hardware-Modul im Betriebssystemkern realisiert werden, ist eine Umgehung der Zugriffssicherung weitgehend ausgeschlossen. Unkontrollierte Möglichkeiten, auf Dateien und Programme zuzugreifen, haben dann nur noch diejenigen, deren Kompetenzen nicht begrenzt werden, wie etwa der Systemmanager oder Wartungsspezialisten. Alle anderen könnten nur noch dann frei auf das System zugreifen, wenn sie Teile der Hardware austauschen oder in der Lage sind, ein manipuliertes Betriebssystem zu starten.

Verschlüsselung

TeleTrusT sieht nur vor, die Signatur zu verschlüsseln, um die Identität eines Absenders zu verifizieren und Manipulationen an seiner Nachricht erkennen zu können. Die Nachricht selbst aber bleibt unverschlüsselt. Um nun auch diese, oder ganze Dateien und Programme, gegen eine unberechtigte Einsichtnahme, Vervielfältigung, Manipulation oder Benutzung zu schützen, könnten sie vollständig verschlüsselt werden.[23] Sie werden durch Kryptoprozessoren automatisch nach der Bearbeitung ver- und vor der nächsten Einsichtnahme durch den Berechtigten wieder entschlüsselt.[24] Sie können zwar entwendet, betrachtet oder manipuliert werden. Doch wird sich der gewünschte Mißbrauchserfolg nicht einstellen, weil Daten und Programme ohne Schlüssel nicht lesbar sind. Sie können daher auch nicht zielgerichtet verändert werden. Sind sie manipuliert, erscheint nach der Entschlüsselung nur noch Unsinn, der vor einer weiteren Verarbeitung bemerkt

21 S. hierzu z.B. Levy; Rosenberg/Abramson 222 ff.; US-Department of Defense 19 ff.; US-National Coputer Security Center 32 ff.; Abel/Schmölz 85 ff.; Weck 205 ff.; Leicht iur 1987, 50.

22 S. z.B. Weck 119.

23 S. hierzu unten Kap. 14 sowie z.B. Abel/Schmölz 314 ff.; Weck 283 ff.; Harmsen/Weiß 20 ff.

24 Mit einem asymmetrischen Verschlüsselungsverfahren nach RSA können derzeit bei einer Schlüssellänge von 660 bit 64 kbit/s und mit einem symmetrischen Verfahren DES 15 Mbits/s verschlüsselt werden - s. Waidner/Pfitzmann/Pfitzmann DuD 1987, 296f. mwN; s. hierzu auch Harmsen/Weiß 21 mwN.

wird. Allerdings sind die Datei oder das Programm dann zerstört. Verschlüsselung schützt also nicht vor Beschädigung oder Vernichtung.

Die beiden Schwachstellen jedes Verschlüsselungsverfahrens, die Qualität des Verschlüsselungsalgorithmus und die Sicherheit des Schlüssels, können analog des 'TeleTrusT'-Konzepts gelöst werden. Ein auf Faktorierung von Primzahlen beruhendes Verfahren zur Ver- und Entschlüsselung scheint derzeit praktisch sicher zu sein, wenn der Schlüssel ausreichend lang ist. Das zweite Sicherungsproblem kann durch die automatische, nicht manipulierbare Erzeugung von Schlüsseln und deren Übertragung in 'versiegelte' Verschlüsselungsprozessoren gelöst werden. Der geheime Schlüssel ist dann nicht einmal seinem 'Besitzer' bekannt.[25]

Weder die Zugriffskontrolle noch die Verschlüsselung schützen allerdings davor, daß jemand im Rahmen seiner Berechtigung Manipulationen an den Klartextdaten vornimmt oder sie zur Kenntnis nimmt. Wenn es Aufgabe des Sachbearbeiters ist, Entscheidungen zu treffen und Daten zu verändern, kann er auch falsche Daten eingeben oder richtige löschen. Wenn er sensitive Informationen lesen soll, kann er sich diese auch merken und verraten. Stimmen die Daten mit der Realität nicht überein, kann es zu schwerwiegenden Fehlentscheidungen kommen. Ist einem Unternehmen bekannt, daß in seinen Produktionsdaten Fehler sind, kann dies die Produktion ebenso stoppen, wie Programmanipulationen oder die Vernichtung der Daten.

Verschlüsselung kann aber auch neue Abhängigkeiten schaffen. Um möglichst weitgehend auszuschließen, daß Unberechtigte verschlüsselte Informationen entschlüsseln können, existiert der niemandem bekannte geheime Schlüssel nur in einer Chipkarte oder einem Verschlüsselungsprozessor. Wird dieser verloren oder entwendet, können erhebliche Schäden entstehen, da dann die verschlüsselten Dokumente, Dateien und Programme wertlos sind. Ein Erpresser hätte also ein kompaktes Angriffsziel. Jede Maßnahme jedoch, die vorgesehen wird, um den geheimen Schlüssel rekonstruieren zu können, schwächt die Sicherheit des Verschlüsselungssystems. Kann zum Beispiel die Ausgabestelle einen verlorenen Schlüssel neu erzeugen, dann kann sie dies auch, wenn er nicht verloren ist. Wird ein Mitarbeiter 'überredet', die Karte einer Bank, einer Behörde oder eines Ministeriums ein zweites Mal auszustellen, könnten mit ihrer Hilfe hohe Geldbeträge transferiert, geheime Unterlagen eingesehen oder nachgeordnete Dienststellen angewiesen werden. Den Betroffenen wird es schwer fallen zu beweisen, daß die Anordnung oder die Überweisung nicht von ihnen stammt. Gelingen könnte ihnen dies nur, wenn sie das öffentliche Vertrauen in das als technisch sicher geltende Verfahren erschüttern.[26]

25 S. hierzu Hammer DuD 8/1988, 393; Rihazcek DuD 1987, 244; ders. DUD 1987, 302.

26 S. hierzu näher Hammer DuD 8/1988, 400f.; s. auch Harmsen/Weiß, 31, die die größten Betrugsrisiken bei den Kartenausgabestellen sehen.

Funktionalitätssicherung

Manipulationen in der Systementwicklung können künftig für einfachere Programme durch Deduktionssysteme erkannt werden. Sie überprüfen automatisch, ob das Programm seiner Funktionalität entspricht, also auch tatsächlich das tut, was es soll. Für große und komplizierte Programme ist eine automatische Überprüfung auch in 20 oder 30 Jahren nicht zu erwarten. In ihnen könnten Trojanische Pferde, logische Bomben oder Viren so versteckt sein, daß sie unter Millionen von Programmzeilen weder einem Revisor noch einem Deduktionssystem auffallen.[27] Liegt die Manipulation bereits in der Spezifikation, also in der Beschreibung dessen, was das Programm später können soll, kann sie überhaupt nicht automatisch festgestellt werden.

Manipulationen während des Betriebs an einer ursprünglich 'sauberen' Software können rechtzeitig bemerkt und der Start eines manipulierten Programms verhindert werden, wenn von dem Ausgangsprogramm eine Prüfsumme berechnet und jeweils vor dem Laden mit der aktuell aus dem Maschinencode berechneten verglichen wird.[28] Der anschließende Versuch, die Manipulation zu lokalisieren und zu beseitigen, gelingt jedoch nicht immmer.

So war in der Bundeswehrhochschule München bereits seit Mai 1984 bekannt, daß eine logische Bombe das Graphiksystem GURUGS in der Silversternacht zerstören wird. Sie konnte nicht entfernt werden.[29]

Durch den Programmvergleich läßt sich also eine bereits erfolgte Manipulation zwar erkennen, aber nur dann verhindern, wenn das Ur-Virus entdeckt ist. Wird das 'Wirtsprogramm' nicht gestartet, kann das Virus auch andere Programme nicht mehr infizieren. Sind aber schon andere Programme verseucht, können sich Viren trotz dieser Kenntnis weiter vermehren und in kurzer Zeit das gesamte System verseuchen. Sie aufzuspüren und zu entfernen, ist äußerst aufwendig und schwierig. Grundsätzlich kann nicht entschieden werden, ob ein Programmteil ein Virus ist oder nicht.[30] In der Praxis wird man sie finden können, wenn die Virenstruktur oder die Virenkennung bekannt ist. Aber auch diese Kenntnis hilft nicht weiter und ein Suchprogramm läuft ins Leere, wenn das Virus sich bei jeder neuen Infizierung selbst verändert.[31] Ein Virus kann auch dadurch seine Entdeckung sehr erschweren, indem es die Kennung durch ein komplexes Muster darstellt, das überdies nicht gespeichert wird, sondern nach einem bestimmten Verfahren

27 So Cohen nach Marshall, Science 240 (1988), 134.

28 S. hierzu z.B. Burger 87f., 355 ff.; Weck 250 ff.; Abel/Schmölz 77.

29 S. Spiegel 2/1985, 79.

30 S. Dierstein 103.

31 S. hierzu z.B. Burger 335 ff.; Dierstein 104f.

(z.B. Quersumme) errechnet wird.[32] Überhaupt keinen wirkungsvollen Schutz gibt es gegen diejenigen, die diese Sicherungsprogramme verwalten. Der Systemmanager könnte trotz dieser Sicherungsmaßnahmen jederzeit unentdeckt ein Virus in das System einpflanzen.[33]

Weil eine nachträgliche Bekämpfung von logischen Angriffen und insbesondere Viren sehr schwierig ist und oft zu spät kommt, muß verhindert werden, daß es überhaupt zu einer Manipulation oder Infektion kommt. Das Einschleusen des Ur-Virus ist umso schwieriger, je stärker das System abgeschottet und seine Arbeitsumgebung kontrolliert wird. Wo keine Daten und Programme transportiert werden, können sich auch keine Viren ausbreiten.[34] Wenn dagegen viele Benutzer in einem System Daten gemeinsam nutzen wollen - wie dies in Wirtschaft und Verwaltung allgemein üblich ist -, kann die Ausbreitung von Viren nicht prinzipiell verhindert werden. Sie kann allerdings erschwert werden, wenn das System über differenzierte Zugriffskontrollmechanismen verfügt. So bleiben etwa die einzelnen Bereiche voneinander getrennt und das Recht, schreibend Programme zu verändern, ist für jeden Benutzer auf seinen engen Bereich begrenzt. Nur sehr wenige haben das Recht, diese Grenzen zu überschreiten.

Vollständige Sicherheit gegen Viren wird es nicht geben.[35] Nur ein völlig isoliertes und kontrolliertes System ist gegen Virenbefall tatsächlich sicher. Da aber auf die gemeinsame Nutzung von Daten und Ressourcen und damit auf Datenfluß innerhalb und zwischen den Systemen nicht verzichtet werden kann, werden Viren eine ständig und latent drohende Gefahr bleiben. Gegen sie wird es kein Allheilmittel geben. Wohl aber ist ein begrenzter Schutz gegen spezifische Viren möglich. Sicherheitsexperten werden die Eigenschaften, das Verhalten und die Ausbreitungsmöglichkeiten unterschiedlicher Viren untersuchen und gegen einzelne Viren und Virenklassen von Fall zu Fall immer neue Verfahren entwickeln, sie aufzuspüren und ihnen mit geeigneten Mitteln zu begegnen. In der Praxis wird der Virenbefall begrenzt, aber keineswegs beseitigt werden können.[36]

Organisation und Arbeitsüberwachung

Da Manipulationen durch das Entwicklungs- und Betriebspersonal von Rechen- und Netzzentren technisch nur unzureichend verhindert oder kontrolliert werden können, sind die technischen Sicherungen durch eine klare Regelung der Berechtigungen und Verantwortlichkeiten zu unterstützen. Die Zahl der Berechtigten wird auf das jeweils notwendige Minimum begrenzt. Eine klare *Funktionstrennung* in der Systementwicklung und im Sys-

32 S. hierzu Burger 338; Brunnstein AI 1987, 401.

33 S. Abel/Schmölz 76.

34 S. hierzu z.B. Burger 56, 374 ff.;Brunnstein AI 1987, 401.

35 S. Abel/Schmölz 113; Dierstein 90, 109; Burger 89, 169; Harmsen/Weiß 68.

36 S. hierzu Dierstein 108.

tembetrieb verhindert in vielen Fällen, daß ein Beschäftigter alle zu einer Manipulation erforderlichen Schritte selbst unternehmen kann.[37] In größeren Betrieben werden die Entwicklungsaufgaben zwischen Spezifikation, Entwurf, Implementierung, Prüfung und Test sowie die Betriebsaufgaben zwischen Operator, Systemmanager und Wartung scharf getrennt. Wird diese Funktionstrennung trotz der durch sie entstehenden Kommunikationsprobleme durchgehalten, werden Manipulationen wesentlich erschwert und sind oft nur noch durch Zusammenwirken mehrerer Personen möglich. Solche Funktionstrennungen sind allerdings nur in großen Organisationen möglich. In kleinen und mittleren Unternehmen oder Behörden werden alle Funktionen oft nur von einem oder wenigen Beschäftigten erledigt.[38]

Alle Aktionen an IuK-Systemen werden gesondert aufgezeichnet. Durch *Auswerten der Logdateien* können manche Angriffe nachträglich erkannt, der Täter identifiziert und das Schadensausmaß bestimmt werden. Solche Kontrollmaßnahmen können vor kontinuierlichen Manipulationen abschrecken und den Schaden begrenzen.[39] Sie können jedoch keine Manipulation verhindern. Insbesondere gegen einmalige Aktionen, nach denen sich der Täter abzusetzen gedenkt, sind sie keine taugliche Sicherung.

Da die physischen Sicherungsmaßnahmen zwar gegen Angriffe von außen einen weitgehenden Schutz gewähren können, nicht jedoch gegen Saboteure oder Diebe von innen, sind die Zugangskontrollen um *Durchsuchungen* der in sensitiven Betriebsteilen Beschäftigten zu ergänzen.[40] Sie müßten verhindern, daß Sabotagemittel eingeschleust und Datenträger herausgeschmuggelt werden. Ob sie jedoch zuverlässig verhindern können, daß Spiritus oder Flüssigsprengstoff in der Thermoskanne hinein- oder die künftig kleinen Datenträger etwa in Körperöffnungen herausgebracht werden, dürfte zu bezweifeln sein. Außerdem ließen sich diese Gegenstände auch in Warensendungen, Betriebsmitteln oder Abfall verstecken.

Alle, die auftragsgemäß Programme entwickeln, implementieren und testen, alle, die Hardware und Peripherigeräte herstellen, alle, die für den Betrieb von Datenverarbeitungsanlagen und Kommunikationsnetzwerken verantwortlich sind oder diese zu warten haben, und alle, zu deren Aufgabe es gehört, sensitive Daten zu lesen oder zu verändern, haben die Möglichkeit zu unbemerkten Mißbrauchsaktionen. Solange alles gut geht, setzen viele Unternehmen und Behörden das Schwergewicht ihrer personenbezogenen Sicherungsmaßnahmen eher auf Schulung, Motivation und Überzeugung und weniger auf Überwachung und Sanktion.[41] Nach dem ersten größeren Schaden wird diese das *Arbeitsklima* fördernde Strategie jedoch kaum noch zu halten sein. Da Sabotageaktionen,

37 S. z.B. Müller DuD 1987, 484; Weck 64 ff.; Bschorr 97 ff.; Bequai 20.

38 S. z.B. Weck 65f.; Abel/Schmölz 51; Albers DuD 1985, 204; Schönberg 95.

39 S. z.B. Weck 181 ff.; Abel/Schmölz 61 ff., 94f., 105 ff.; Hofmann, K. 312 ff.; US-Department of Defense 16; US-National Computer Security Center 22; für den Bankenbereich Harmsen/Weiß 49.

40 S. z.B. Weese/Lessing KES 1987, 152 ff.

41 S. z.B. Pagalies CW v. 22.8.1986, 7; Breuer 205; Schönberg 93.

Diebstähle von Datenträgern, das Ausspionieren oder Kopieren geheimhaltungsbedürftiger Informationen und Manipulationen an Daten und Programmen durch die technischen Sicherungsmittel nicht ausgeschlossen werden können, kann dann auf eine Beobachtung, oft sogar *Überwachung* dieser Beschäftigten während der Arbeit nicht verzichtet werden. Überall, wo keine lückenlose technische Sicherung erreicht werden kann, dürfte die erforderliche Sicherheit nur dadurch erzielt werden, daß sensitive Arbeiten nach der Zwei-Mann-Regel durchgeführt werden.[42] Sie sind so zu organisieren, daß sie entweder nur von zwei Personen gemeinsam durchgeführt werden können oder daß sie von einem sachkundigen Kontrolleur beaufsichtigt werden.

Weil das Risiko von Manipulationen nach einer Kündigung besonders groß ist, empfehlen Sicherheitsexperten[43], mit dieser zugleich den entlassenen Mitarbeitern den weiteren Zugang zur Datenverarbeitung zu versperren. Die Computerfirma Applied Technology Inc. beispielsweise hat 60 Programmierern gekündigt und sie gezwungen, unter den Augen der Werkschützer ihre privaten Unterlagen in vorbereitete Pappkartons zu packen und unter deren Begleitung sofort das Betriebsgelände zu verlassen.[44]

Personenüberprüfung

Selbst wenn die technischen und organisatorischen Sicherungen auf hohem Niveau ihre Funktionen erfüllen, bleibt Insidern noch immer ein bedeutender Spielraum für Manipulationen, Entwendungen, Spionage und Sabotage. Hardware und Programme von Informationsverarbeitungs- und Kommunikationssystemen sicher und zuverlässig herzustellen, sie zu warten und zu betreiben, sensitive Informationen zu verarbeiten und zu übermitteln sowie die personalintensiven Sicherungsmaßnahmen wie Eingangskontrollen, Revision, Schlüsselverwaltung und Arbeitsüberwachung durchzuführen, setzt daher voraus, daß kein Mitarbeiter ein Sicherheitsrisiko darstellt. Die Zuverlässigkeit der in sensitiven Arbeitsbereichen Beschäftigten muß für die Verantwortlichen ein unverzichtbarer Bestandteil ihres Sicherungssystems sein. Sie kann aber nicht vorausgesetzt, sondern muß gewährleistet werden. Von daher wird es unumgänglich sein, die Vertrauenswürdigkeit von Insidern vor ihrer Einstellung zu überprüfen und in regelmäßigen Abständen durch Wiederholungsüberprüfungen sicherzustellen. Je nach Sensitivität der übertragenen Aufgaben werden sie entweder eigene Nachforschungen anstellen, die Hilfe von Auskunfteien oder kommerzieller Überprüfungsunternehmen in Anspruch nehmen oder - soweit es sich

42 S. z.B. Abel/Schmölz 57, 83, 126; Schönberg 119; Burger 56, 374 ff.; Müller DuD 1987, 483 ff.; für den Bankenbereich Harmsen/Weiß 49, 68.

43 S. z.B. Abel/Schmölz 12, 116; Weck 66f.; Breuer 205; Paul DuD 1985, 53.

44 S. Zeit v. 15.4.1988, 23.

um "sicherheitsempfindliche Stellen von lebens- und verteidigungswichtigen Einrichtungen"[45] handelt - die Überprüfung dem Verfassungsschutz überlassen.[46]

Bereits heute sollen zum Beispiel mindestens 20.000 Beschäftigte der Firma Siemens aus den als sicherheitsempfindlich deklarierten Unternehmensbereichen "Kommunikations- und Datentechnik", "Bauelemente" und "Nachrichtentechnik" mit dem Einverständnis des Bayrischen Datenschutzbeauftragten vom Verfassungsschutz überprüft worden sein.[47] Das Rechenzentrum der Bundesversicherungsanstalt für Angestellte in Berlin wurde 1977 vom Innenminister zu einem "lebens- und verteidigungswichtigen Betrieb" erklärt. Seither werden alle 300 Mitarbeiter der Abteilung Datenverarbeitung und die Angestellten aller Fremdfirmen, die für die Bundesversicherungsanstalt Programme entwickeln, vom Verfassungsschutz überprüft.[48]

In dem Maße, wie künftig alle Lebensbereiche von IuK-Technik durchdrungen werden und die Schadenspotentiale im Fall ihres Versagens steigen, werden auch die vergleichbaren sicherheitsempfindlichen Bereiche zunehmen. Ausgehend von der gegenwärtigen Praxis können künftig solche Überprüfungen nicht auf die Hersteller von IuK-Systemen beschränkt bleiben, sondern müssen auch auf all jene Beschäftigten ausgeweitet werden, die bei Anwendern Gelegenheiten hätten, größere Schäden zu verursachen. Die Zahl der zu überprüfenden Personen wird daher mit der wachsenden Abhängigkeit von IuK-Systemen zunehmen. Auch wenn die Intensität der Überprüfung nach der Schutzbedürftigkeit der Anlagen und Daten[49] und den Mißbrauchsmöglichkeiten der Beschäftigten differenziert wird, dürfte die Zahl der sehr streng zu Überprüfenden zwar eingegrenzt sein, aber gegenüber heute doch deutlich ansteigen.

Der Umfang künftiger Überprüfungen muß sich grundsätzlich auf all die Motive erstrecken, zu deren praktischer Umsetzung der Beschäftigte in der Lage wäre. Es kann also notwendig sein, seine politische Einstellungen zu überprüfen, um politisch motivierte Aktionen zu verhindern. Soll ausgeschlossen werden, daß er aus Bereicherungsabsicht handelt oder Ziel einer Bestechung wird, müssen zumindest die finanzielle Situation des Beschäftigten sowie sein Lebensstil und sein finanzielles Gebaren kontrolliert werden. Um die Einstellung kriminell motivierter Bewerber zu verhindern, müßten ihre Vorstrafen und ihre persönlichen Kontakte überprüft werden. Agenten fremder Mächte könnten nur entdeckt werden, wenn ihre Legende zeitlich möglichst weit zurückverfolgt wird. Einer Erpressung kann nur vorgebeugt werden, wenn - noch intensiver als Erpresser dies tun -

45 § 3 Abs. 2 Nr. 2 BVerfSchG.

46 S. hierzu z.B. Weck 46, 66; Abel/Schmölz 216; Heidinger/Andrich 132, 194; Bequai 19.

47 S. hierzu z.B. Metall Nr. 10 v. 15.5.1987, 19 und Nr. 11 v. 1.6.1987, 19.

48 S. z.B. den 5. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz 60; FR v. 17.10.1986. Leicht korrigiert wurde diese Praxis durch das Urteil des BAG v. 14.10.1986 - 6 AZR 331/83.

49 S. zu den Schutzstufen und Sicherheitsklassen oben zu Beginn des Kapitels.

nach Schwachstellen in den Lebensgewohnheiten und dunklen Flecken in der Vergangenheit geforscht wird.[50]

Die von den Beschäftigten ausgehenden Risiken für die Sicherheit und Zuverlässigkeit der IuK-Systeme können aber nur dann verläßlich abgeschätzt werden, wenn sie umfassend, also auch hinsichtlich ihres Privatlebens, überprüft werden. Um alle relevanten Einflußfaktoren vollständig erfassen zu können, wird auch ihr soziales Umfeld in diese Prüfung miteinbezogen werden müssen.[51]

Je nach Schadenspotential, vermutetem Anreiz, Leichtigkeit der Tatausführung und Funktion der Beschäftigten wird es unterschiedliche Sicherheitsstufen für die Überprüfungen geben. Die Beschäftigten könnten beispielsweise danach unterschieden werden, ob sie lediglich Systembenutzer sind, die keine Einflußmöglichkeit auf die Sicherungsfunktionen des Systems haben, ob sie für die Entwicklung, den Betrieb oder die Wartung der Systeme zuständig sind oder ob sie gar selbst Sicherungsfunktionen haben oder diese beeinflussen können. Je nach Sicherheitsstufe und Bedrohungseinschätzung werden die Überprüfungen unterschiedlich streng sein.

Wer ein hohes Sicherungsniveau anstrebt, könnte sich unter Umständen an Vorbildern in den USA orientieren. Dort müssen seit 1985 alle Regierungsbeamten und Vertragspartner der Regierung, die mit Geheimakten zu tun haben, Lügendetektor-Tests der Spionageabwehr akzeptieren.[52] Um zu verhindern, daß Beschäftigte oder Vertragspartner des US-Verteidiungsministeriums Opfer von Erpressungen werden, gilt bei ihnen seit Mai 1987 "sexuelles Fehlverhalten" wie Homosexualität, Ehebruch, Partnertausch, Sexorgien und Sodomie als Sicherheitsrisiko.[53]

Gesellschaftliche Prävention

Es genügt nicht, Mißbrauchsaktionen nur zu behindern oder mögliche Schadensfolgen zu begrenzen. Notwendig ist auch eine breite, in der Gesellschaft wirksame Prävention. Diese kann erreicht werden, indem Anwender und Benutzer von IuK-Systemen über die Risiken des Mißbrauchs aufgeklärt oder potentielle Täter durch rigorose Strafvorschriften und Strafverfolgungsbemühungen abgeschreckt werden. Das Herzstück gesellschaftsbezogener Prävention wird jedoch die Vorfeldaufklärung sein.

Für Sicherheitsexperten geht die Gefahr vor allem von Insidern aus.[54] Dennoch und obwohl sie die technischen Sicherungen gegen externe Angreifer erheblich effektiviert

50 S. zum notwendigen Umfang z.B. auch Dammert 288; ders. 129f.; Butti 122f.

51 S. zu dem insoweit vergleichbaren Beispiel der Überprüfung in atomtechnischen Anlagen Roßnagel 1983, 167, 178 ff.; ders., 1984a, 71 ff.; ders., 1987a, 134f.

52 S. FR v. 21.12.1985; bereits in den 70er Jahren wurde in US-Firmen vom Computer-Personal Fingerabdruckvergleiche und Lügendetektortests verlangt - s. Bequai 19.

53 S. z.B. FR v. 15.5.1987.

54 S. z.B. Paul DuD 1987, 84; Weck 63; Abel/Schmölz 8, 11: 98%; Sicherheitsberater 1986, 48: 80%.

haben, werden sie auch künftig mit physischen Angriffen und Manipulationsversuchen von außen rechnen. Keine der genannten Motive und Aktionsformen werden als Risiken ausgeschlossen werden können. Besondere Gefahren werden jedoch von zwei Entwicklungen ausgehen:

Wenn die Sicherungsmaßnahmen gegen physische Angriffe von außen optimiert werden, könnte dies zum einen sowohl einen Radikalisierungs- als auch einen Verdrängungseffekt hervorrufen. Wenige Angreifer werden so zu radikaleren Angriffsmitteln übergehen - etwa Lastwagen voll Dynamit oder tragbaren, sehr explosiven Raketen, die über mehrere Kilometer hinweg ihr Ziel treffen und in wenigen Jahren auf allen Waffenschwarzmärkten zu finden sein werden.[55] Vorbilder hierfür könnten die Zerstörung der französischen und amerikanischen Hauptquartiere im Libanon durch LKW-Bomben 1983[56] sein oder der Beschuß des spanischen Verteidigungsministeriums durch die ETA im Juli 1986[57] oder die Mörser-Attacke der IRA auf eine nordirische Polizeistation im Dezember 1985.[58] Weniger radikale Angreifer könnten abgedrängt werden auf die vielen schlechter geschützten Objekte[59] oder die über die Fläche verteilte und daher kaum zu schützende Infrastruktur der 'Informationsgesellschaft' zu ihrem Ziel wählen. Wie nach der Reaktorkatastrophe von Tschernobyl könnten dann Anschläge gegen Stromleitungen und -masten oder Telekommunikationsleitungen und -anlagen gerichtet werden.

Wenn zum anderen über offene Netze jedem der Zugang zu IuK-Systemen gewährt würde, der dafür zu zahlen bereit ist, erhielte jeder Kunde beinahe den Status von Insidern, ohne wie diese überprüft und überwacht zu werden. Je offener die Kommunikations- und Informationsstrukturen ausgestaltet werden, umso leichter wird es auch Außenstehenden fallen, Manipulationen vorzunehmen. Wie das Beispiel der Hacker zeigt, könnte die Zahl möglicher Angreifer unter Umständen so groß sein wie die Zahl der Rechnerbesitzer, die über einen Zugang zu Datennetzen verfügen.

Die für Sicherheit Verantwortlichen müssen außerdem darauf gefaßt sein, daß etwa ausländische Agenten zu Insidern Kontakt aufnehmen mit dem Ziel, sie zu verführen oder zu erpressen. Um sie zu einer Zusammenarbeit zu bewegen, könnten Verbrecherorganisationen versuchen, Beschäftigte zu bestechen, oder Terrorgruppen sich bemühen, Mitarbeiter zu verleiten oder zu überzeugen. Schließlich werden die Sicherheitsbehörden darauf achten, daß keine für die hochtechnologisierte Gesellschaft riskanten sozialen oder politischen Situationen entstehen.

Anlagenbezogene Sicherungsmaßnahmen haben somit nur eine begrenzte Effektivität. Sie vermögen Mißbrauchsrisiken nicht in ausreichendem Maße zu verringern. Die Behörden der inneren Sicherheit werden daher versuchen, die Sicherungslinie immer

55 S. hierzu z.B. Bequai 11; Jenkins/Rubin 237f.; Roßnagel 1987a, 89 ff. mwN.

56 S. z.B. Spiegel 44/1983, 158.

57 S. z.B. FR v. 22.7.1986

58 S. z.B. TAZ v. 21.12.1985.

59 Ebenso Bschorr 119.

weiter in die Gesellschaft hinein vorzuverlegen und Risiken schon im Vorfeld zu erkennen und zu beseitigen. Über den Objektschutz hinaus werden Abwehr und Verteidigung um Gegenaufklärung und Gegenangriffe ergänzt.[60]

Vorfeldaufklärung wird zum einen notwendig sein, um zu wissen, welche Anlagen oder welche Informationssammlungen wie gefährdet sind. Diese Kenntnis erst ermöglicht, die Sicherungsanstrengungen in die richtige Priorität zu setzen. Aufklärung soll zum anderen das Wissen liefern, welche Aktionsformen potentielle Täter wählen dürften. Dies ermöglicht, das Sicherungssystem der vermutlichen Bedrohung entsprechend zu konzipieren. Drittens soll die Aufklärung auch Hinweise geben, wer die möglichen Angreifer sind, welche Ziele sie verfolgen, welche psychologischen Profile sie besitzen, wer sie unterstützt und auf welche Hilfsmittel sie zurückgreifen können. Nur mit diesen Informationen kann das erforderliche Sicherungsniveau festgelegt und der jeweiligen Bedrohungssituation angepaßt werden. Schließlich ist es die Funktion der Vorfeldaufklärung festzustellen, von wo aus die Angreifer operieren, welche Verbindungen sie haben und wo ihre Schwachstellen sind. Informationen dieser Art sollen den Behörden ermöglichen, in einer weit vorgreifenden präventiven Strategie mögliche Täter und ihr Unterstützerumfeld zu isolieren und durch gezielte Maßnahmen der Verunsicherung abzuschrecken.

Um diese Aufgaben erfüllen zu können, benötigen die Sicherungsorgane einmal eine Basisaufklärung über alle Personen, Gruppen und Staaten, die möglicherweise Angriffe gegen die Nervenzentren und Nervenbahnen der 'Informationsgesellschaft' unternehmen könnten, über ihre Struktur, ihre Beziehungen und ihre Unterstützer. Zum anderen müssen sie eine permanente aktuelle Feldaufklärung betreiben, um im Fall einer Drohung, Erpressung oder einer Aktion zum Beispiel sofort feststellen zu können, wie ernst die Drohung gemeint ist, wer die Aktion durchführt, mit welchen weiteren Aktionen zu rechnen ist und welche Gegenmaßnahmen notwendig sind.[61]

All dies erfordert eine umfassende und tiefgehende Aufklärungsarbeit im In- und Ausland, die Sammlung und Auswertung aller verfügbaren Informationen und deren Austausch zwischen verschiedenen Geheimdiensten. Die Behörden der inneren Sicherheit werden hierfür versuchen, alle 'Risikogruppen' zu infiltrieren und die im Zukunftsbild dargestellten künftigen Möglichkeiten automatischer Überwachung und IuK-gestützter Kontrollmaßnahmen umfassend nutzen.[62]

60 S. zu den insoweit vergleichbaren Problemen nuklearer Sicherungssysteme Roßnagel 1983, 203 ff; 1987, 135 ff.

61 S. zu alledem auch Lutterbeck 1987, 48; Steinmüller Kursbuch 66 (1981), 184 ff.

62 S. hierzu näher Pordesch 1989.

13. Grenzen der Sicherung: das potentielle sicherungsniveau

Durch das Zusammenwirken all dieser Sicherungsmöglichkeiten in einem koordinierten System könnte ein relativ hohes Sicherungsniveau erreicht werden. Um dieses zu beschreiben, wurde im vorhergehenden Kapitel unterstellt, daß die Sicherungsmaßnahmen entsprechend ihrer Aufgabenstellung optimal funktionieren. Unter Ausschluß störender Randbedingungen konnten wir so gewissermaßen im Gedankenlabor feststellen, welches theoretische Sicherungsniveau möglich sein und welches Mindestrisiko verbleiben wird. Dabei wurde zum Beispiel davon abgesehen, daß viele der für die Zukunft unterstellten Sicherungskonzepte wie etwa die Zugriffssicherungen oder die Zugangskontrollen mittels Chipkarte und elektronisch geprüfter Unterschrift noch nicht ausgereift und mit Entwicklungsrisiken verbunden sind. Unberücksichtigt blieben bisher auch die Begrenzungen, die sich in der Anwendungsumgebung und unter den Bedingungen des 'wirklichen' Lebens ergeben. Jenen ist dieses Kapitel und diesen das folgende Kapitel gewidmet.

Wenn wir nun die Sicherungsmöglichkeiten in ihrer Anwendungsumgebung betrachten, bewegen wir uns weiterhin auf einer theoretischen Ebene und erweitern nur unser Blickfeld. Wir sehen noch immer von möglichen Widrigkeiten der Realität ab und berücksichtigen nur einige Schwierigkeiten, die eine Einordnung der Sicherungsmöglichkeiten in den Betriebsablauf mit sich bringt. Dadurch beschreiben wir das potentielle Sicherungsniveau und das kleinstmögliche Restrisiko. Grenzen der Sicherungsmöglichkeiten können sich ergeben, weil sie nur für begrenzte Aufgaben konstruiert sind und dadurch in der Anwendungsumgebung Sicherheitslücken bleiben. Ihr Sicherheitsbeitrag kann gemindert werden, weil sie in Konflikt mit anderen betrieblichen Erfordernissen geraten. Schließlich kann das Mindestrisiko erhöht werden, weil Sicherungsmaßnahmen zu kontraproduktiven Effekten führen. Wir wollen diese Begrenzungen jeweils an einigen Beispielen erläutern.[1]

Begrenzte Spezifikationen

Technische Sicherungsmaßnahmen greifen in der Regel nur in den Fällen, für die sie konstruiert sind. Schwachstellen sind daher nicht auszuschließen. So bieten etwa Verschlüsselungsverfahren nur Schutz gegen die Personen, die nicht über den Schlüssel verfügen. Alle Sachbearbeiter aber müssen in der Lage sein, die Texte zu entschlüsseln, um im Klartext Daten bearbeiten zu können. Sie sind also auch in der Lage, sie weiterzugeben. Verfügen sie über den Schlüssel, könnte auch dieser in falsche Hände geraten. Ebenso schützen logische Zugangskontrollen nur gegen Unberechtigte. Einen Mißbrauch durch Berechtigte verhindern sie nicht. Ihre Schwachstellen liegen vor allem in der Systemprogrammierung und -verwaltung sowie im Herstellungsverfahren für die verwendete

1 S. hierzu näher Hammer Arbeitspapier Nr. 8.

Chipkarte.[2] Capability-Verfahren schützen nur vor unberechtigtem Zugriff, soweit die Arbeitsaufgaben und damit die Zugriffsrechte eindeutig formal abgegrenzt werden können. Höher qualifizierte Tätigkeiten können aber meist nur qualitativ und selten rein formal beschrieben werden. Somit greift der Zugriffsschutz kaum für gerade die Tätigkeiten, die besonders schadensträchtige Manipulationen ermöglichen.

So gut theoretische Sicherungskonzepte auch sein mögen, bleibt immer als ein Hauptproblem ihrer Realisierung, Sicherungsanforderungen zu formalisieren. Könnte Mißbrauch von Gebrauch eindeutig abgegrenzt werden, könnten die Arbeitsaufgaben restlos formal beschrieben werden, könnten sie auch automatisiert werden. Aufgaben, die von Menschen erfüllt werden sollen, werden einen mehr oder weniger großen Ermessens- und Handlungsspielraum eröffnen müssen, der immer auch mißbraucht werden kann.

Andere Spezifikationsproblem sind das 'Täterbild' und das 'Bedrohungsmodell'. Die unausgesprochene Prämisse aller Sicherungssysteme ist meist, daß nur *eine* Person versucht, die IuK-Technik zu mißbrauchen. Die meisten Sicherungsmaßnahmen können daher untergangen werden, wenn zwei oder mehrere Personen in verschiedenen Funktionen zusammenarbeiten. Weder die organisatorische Funktionstrennung, noch die Zwei-Mann-Regel oder Zugangs- und Zugriffskontrollen können ihren Zweck erfüllen, wenn die zur Realisierung dieser Sicherungsfunktionen zuständigen Personen zusammenarbeiten.

Erfordernisse eines reibungslosen Betriebsablaufs

In schwierige Zielkonflikte führt das Problem des Super-Users. In komplexen IuK-Systemen können nicht alle möglichen Probleme vorausgesehen, geschweige denn gelöst werden. Um auf unvorhergesehene Fälle reagieren zu können, muß jemand über alle Rechte im IuK-System verfügen können. Ein solcher Super-User kann alle Operationen durchführen, da ihm von der Zugriffssicherung keine Beschränkungen auferlegt werden. Alle die diesen Status zu Recht besitzen oder unberechtigt durch Bestechung, Erpressung oder auch Hacking[3] erlangen, sind in der Lage, jede erdenkliche Manipulation durchzuführen und auch vor einer Revision anhand der Log-Dateien zu verstecken.[4]

Sicherheitsexperten denken daher darüber nach, wie ohne Verluste an Effektivität und Flexibilität der Betriebsabläufe diese Machtfülle reduziert werden kann. Eine Funktionstrennung, die dem Super-User nur die Systemverwaltung ermöglicht, ihm aber den Einblick in Dateien verwehrt, begrenzt zwar dessen Handlungsspielraum, erhöht aber die Abhängigkeit des Systemherrn vom einzelnen Anwender. In diesem Konzept könnte der Sachbearbeiter zum Beispiel Konstruktionsdaten, Buchhaltungskonten oder auch Mani-

2 S. hierzu näher Hammer DuD 8/1988, 398 ff.

3 S. die Beispiele in Kap. 11.

4 S. z.B. Abel/Schmölz 56f., 116f.; Bschorr 124; s. hierzu auch KES-Sicherheitsenquete 159.

pulationen vor seinem Arbeitgeber verbergen, ohne daß eine Kontrolle möglich wäre. Hat der Super-User keine umfassenden Eingriffsrechte können auch gewöhnliche Hardwarefehler, ein vergessenes Paßwort oder eine verlorene Code-Nummer verheerende Folgen haben, weil eine Rekonstruktion der Daten nicht mehr möglich ist.

Ein Kompromiß könnte die Verteilung von Aufgaben des Super-Users auf verschiedene Personen sein, die für besonders sensible Operationen zusammenarbeiten müssen. Diese könnten jedoch immer nur dann ausgeführt werden, wenn alle Super-User gleichzeitig anwesend sind. Bestehen starke Konflikte in der Gruppe der Super-User und einer von ihnen verweigert sich oder einer von ihnen ist verhindert, kann das System nicht mehr verändert werden. Außerdem müßten alle Super-User über annähernd gleiche Qualifikationen verfügen. Der in diesem Konzept erforderliche organisatorische Mehraufwand behindert möglicherweise flexible Reaktionen auf drängende Probleme des Betriebs. Im Notfall ist schnelle Hilfe durch das notwendige Zusammenwirken aller erheblich schwieriger. Es muß daher zweifelhaft bleiben, ob dies eine künftige Lösung des Super-User-Problems sein kann.

Zielkonflikte zwischen den Belangen eines flexiblen und reibungslosen Betriebs und Sicherungsmaßnahmen sollen noch an einem weiteren - weniger gravierenden - Beispiel illustriert werden. Um zu verhindern, daß jemand mit einer abgehörten Teilnehmeridentifikation in ein System eindringt, könnte vorgesehen werden, daß jeder Benutzer nur von seinem mit dem System vereinbarten Terminal aus in Kontakt tritt. Entweder erkennt das System das Terminal an einer automatisch übermittelten Anschlußkennung oder es ruft auf eine Verbindungsanfrage hin automatisch zu dem vereinbarten Terminal zurück.[5] Eine solche Sicherung würde jedoch der intendierten Flexibilisierung von Zugangsmöglichkeiten zum System widersprechen. Es könnten dann weder der Versicherungsvertreter vom PC eines Kunden noch der Manager auf Reisen von seinem Hotelterminal noch der Sachbearbeiter vom Tisch eines Vertragspartners oder Geschäftfreundes auf ihre Arbeitsunterlagen zurückgreifen. Sie würden vermutlich auf diese Sicherungsmöglichkeit verzichten.

Kontraproduktive Effekte

Einige Sicherungsmaßnahmen verhindern zwar bestimmte Mißbrauchsaktionen oder reduzieren spezielle Schäden, ermöglichen jedoch oder erleichtern sogar andere. So verringern Sicherungskopien das Verlustrisiko von Daten und Programmen, erhöhen aber gleichzeitig das der Ausspähung. Die Daten könnten während der Übermittlung abgehört oder durch Lesen oder Entwenden einer Sicherungskopie erlangt werden. Dieses Risiko wiederum läßt sich durch Verschlüsseln der Telekommunikation oder der gespeicherten Daten reduzieren. Doch hat auch dieses Sicherungsmittel kontraproduktive Effekte. Zum

5 S. hierzu z.B. Abel/Schmölz 155, 225 ff.

einen erhöht es die Abhängigkeit vom Besitzer des Schlüssels. Verfügt jeweils nur einer über den Schlüssel, kann er abhanden kommen oder als Druckmittel zur Durchsetzung bestimmter Forderungen benutzt werden. Besitzen ihn dagegen mehrere, wird das Risiko der Weitergabe und Einsichtnahme erhöht. Zum anderen verhindert die Verschlüsselung jede Kontrolle verschlüsselter Informationssammlung und Kommunikation. Dies wird zwar dem Datenschutz, aber auch Kriminellen oder Agenten zugute kommen. Lateinamerikas Drogensyndikate beaufsichtigen bereits heute ihren Drogenversand, lenken ihre Geldströme und überwachen ihre Mitarbeiter mit Hilfe von Computernetzen.[6] Solche Geschäfte oder gerade Computermanipulationen könnten dann unter verschlüsselten Datensammlungen und Telekommunikationen verborgen werden.

Widersprüchliche Effekte ergeben sich auch aus der Systemgestaltung. Werden die Kompetenzen innerhalb eines Systems zentralisiert, reduziert dies personell die Mißbrauchsmöglichkeiten auf eine oder wenige Personen. Gleichzeitig werden aber dessen oder deren Mißbrauchsmöglichkeiten inhaltlich erheblich erweitert. In verteilten Systemen kann zwar das Schadenspotential eines Ausfalls oder eines Mißbrauchs leichter auf das betroffene Teilsystem begrenzt werden. Dezentralisierung erschwert aber, auf Ersatzsysteme umzuschalten, wenn nicht nur ein Teilsystem, sondern die Infrastruktur des verteilten Systems betroffen ist. Außerdem ist es erheblich leichter, die vorgestellten Sicherungsmöglichkeiten für zentrale Großrechner zu realisieren als in verteilten Systemen und Arbeitsplatzcomputern.[7]

Es gibt Experten, die eine Fernprogrammierung des Systems über Telekommunikation empfehlen, weil die Funktionstrennung zwischen Betriebspersonal und Softwarefirmen Manipulationen beider Seiten erschwert. Das Betriebspersonal ist auf das reine Operating beschränkt und die Softwarefirma hat keinen Einfluß auf den Betrieb des Systems. Aus dem gleichen Grund wird empfohlen, die Anlage an das Fernwartungnetz der Herstellers anzuschließen, der über diese Verbindung Ferndiagnosen erstellen und Softwareeingriffe vornehmen kann.[8] Da aber in beiden Fällen eine Kontrolle der Programmierung und Wartung sehr schwer bis unmöglich ist, sehen andere Experten hierin ein sehr hohes Sicherungsrisiko.[9] In der Tat dürfte Fernprogrammierung und Fernwartung Manipulationen in Bereicherungsabsicht erschweren und gleichzeitig logische Angriffe in Zerstörungsabsicht erleichtern

Schließlich ist daran zu erinnern, daß alle zusätzlichen technischen Sicherungsmaßnahmen das Risiko komplexer Interaktionen von Fehlern erhöhen können.[10]

---

6 S. FR v. 6.8.1988.

7 S. hierzu auch Abel/Schmölz 181 ff.; Albers DuD 1985, 201 ff.

8 S. z.B. Bschorr 97 ff.

9 S. Abel/Schmölz 283 ff.

10 S.hierzu oben Kap. 9 und Perrow 39, 82f.

14. Die Verlässlichkeit künftiger Sicherungssysteme: Das reale Sicherungsniveau

Aber das Leben ist ja nicht so, wie der Konstrukteur eines Sicherungssystems es sich vorstellt. Wir wollen jedoch wissen, welches realistische Sicherungsniveau zu erwarten ist und welchem Restrisiko die Gesellschaft tatsächlich ausgesetzt sein wird. Daher müssen wir das Labor verlassen und uns mit den Widrigkeiten der Sicherungspraxis befassen. Jeder, der ein Sicherungssystem plant, muß schmerzlich erleben, wie sein Konzept in der Phase der Realisierung beschnitten und in der Phase des Betriebs durchlöchert wird. Probleme der Verwirklichung ergeben sich beispielsweise aus den begrenzten Finanzmitteln, aus organisatorischen Schwierigkeiten und aus widerstreitenden Interessen. Die Verläßlichkeit des gesamten Sicherungssystems basiert auf Voraussetzungen, die es selbst nicht gewährleisten kann. Zu ihnen gehören etwa das fehlerfreie Funktionieren der mit Sicherungsaufgaben betrauten Personen, die Stabilität der politischen und sozialen Verhältnisse und ein stets ausgeglichener Wettlauf zwischen Angreifern und Verteidigern.

Begrenzte Etats

Sicherungsmaßnahmen sind unproduktiv. Aber sie kosten Geld. Soll ein System redundant ausgelegt werden, kostet es mindestens das Doppelte. Geräte mit einer geringen kompromittierenden Abstrahlung sind bis zu fünfmal teurer als ungeschützte.[1] Das gleiche gilt für Software. Jede zusätzliche Sicherungsfunktionen in Programmen erfordert Mehrkosten. Jede Sicherungsroutine und jeder Test kosten Betriebszeit - und zwar oft mehr als das zu sichernde Programm benötigt. Bauliche Sicherungen gegen physische Angriffe sind teuer. Zusätzliches Personal für Sicherungszwecke ist oft nicht im Personalplan unterzubringen. Und alle Sicherungskosten steigen ab einem bestimmten Sicherheitsniveau exponentiell an. Jeder zusätzliche - aber eventuell notwendige - Sicherheitsgewinn erfordert dann den doppelten oder mehrfachen Aufwand.[2] Sein Konzept wird der Konstrukteur des Sicherungssystems daher nur verwirklichen können, wenn es zum einen die finanzielle Leistungsfähigkeit der Organisation nicht übersteigt, und er zum anderen die Finanzverwalter überzeugen kann, daß jedes Detail seines Konzepts wichtiger ist als alle konkurrierenden Ausgabenwünsche.

Allerdings müssen die Kosten nicht für alle Sicherungsmaßnahmen und für alle Zeiten ein limitierender Faktor sein. Zum einen werden die Anlagen und Daten in verschiedene Sicherheitsklassen eingeteilt. Damit wird verhindert, daß für alle gleichermaßen hohe

---

1 S. Abel/Schmölz 307.

2 S. z.B. Abel/Schmölz 28f.; Weck 19; s. auch KES-Sicherheits-Enquete: die Sicherungskosten stiegen im Durchschnitt von 1986 bis 1988 von 2% auf 5% des Datenverarbeitungs-Etats.

Sicherungskosten entstehen.[3] So ist zu erwarten , daß die reinen Hardwarekosten künftig an Bedeutung verlieren. Zum Beispiel dürften die Kosten für Verschlüsselungsprozessoren vernachlässigenswert sein.[4] Alle Arbeitsplatzcomputer mit den hier dargestellten Sicherungssystemen auszustatten, dürfte jedoch auch nach 2000 einen sehr großen finanziellen Aufwand bedeuten. Soweit Standardsoftware für Sicherungszwecke verwendet werden kann, fallen die Entwicklungskosten nur einmal an. Ihre Kopien könnten mit der Anzahl verkaufter Produkte im Preis sinken. Schließlich kann der Aufwand für Sicherungsmaßnahmen auch anderen Interessen dienen und dadurch teilweise abgedeckt werden: So lassen sich mit Chipkarten und Kryptoverfahren nicht nur Zugangssicherungen und Ausspähungsschutz gewährleisten, sondern auch Rechtssicherheit und Identifikation für Teletransaktionen. Elektronische Zutrittskontrollen dürften auch der Anwesenheitskontrolle, der Gleitzeit- und der Betriebsdatenerfassung dienen.[5] Capability-Verfahren ermöglichen nicht nur Zugriffskontrollen, sondern verbessern auch die Qualität von Softwaresystemen gegenüber herkömmlichen Programmfehlern und tragen so zur Kostensenkung in der Softwareentwicklung bei.

Allein die Hard- und Softwarekosten sind jedoch für die Finanzierung künftiger Sicherungssysteme nicht entscheidend. Ihr Hauptkostenfaktor dürfte langfristig eher aus dem organisatorischen und personellen Aufwand entstehen, der zum Beispiel für ein Schlüsselverwaltungssystem, für eine strikte Einhaltung der Zwei-Mann-Regel, für Zutrittskontrollen, für die Wartung der Sicherungssysteme oder für die Revision der Log-Dateien erforderlich ist.[6] Weitere Kosten verursachen die Sicherungsvorkehrungen durch Behinderungen des Betriebsablaufs, durch ihren Zeitaufwand[7] und durch die Notwendigkeit wiederholter Notfallübungen.[8] In Bezug auf die Anschaffungs- und Betriebskosten des Gesamtsystems werden sie in vielen Fällen als viel zu hoch erscheinen.

Da weder das genaue Schadensausmaß noch die Wahrscheinlichkeit eines Angriffs bekannt sein können, ist nie zu beweisen, welche Sicherungen sich ökonomisch rentieren. Welche Sicherungsmaßnahmen künftig finanziert werden, ist daher mehr eine Frage des Sicherheitsbedürfnisses und des Bedrohungsgefühls als eine ökonomisch klar kalkulierbare Funktion. Über ihre Notwendigkeit werden Sicherungsverantwortliche und Finanzverwalter meist unterschiedlicher Ansicht sein. *Sicherheit wird eine Frage des Preises sein*. Hart kalkulierende Organisationen werden jedenfalls jede vermeidbare Ausgabe

3 S. z.B. Breuer 211 ff.; Abel/Schmölz 29 ff., Weck 68 ff.

4 Waidner/Pfitzmann/Pfitzmann DuD 1987, 297 rechnen bei einer Massenproduktion mit Kosten unter 1 DM pro Chip.

5 Sicherheitsexperten warnen jedoch vor einer Funktionsvermischung - s. Sicherheits-Berater 1986, 170.

6 Schon heute betragen die Personalkosten durchschnittlich 80% der Sicherungskosten eines Unternehmens - S. Wirtschaftswoche 37/1986, 62.

7 Je nach Schlüssellänge und Verschlüsselungsverfahren kann für die Verarbeitung zu verschlüsselnder Daten ein vieltausendfacher Rechenaufwand erforderlich sein - s. Harmsen/Weiß 25 mwN.

8 S. hierzu z.B. Weck 54f., 73 ff.

scheuen[9] und in wirtschaftlich schwierigen Zeiten Einsparungen zuerst in diesem unproduktiven Bereich vornehmen.[10] Sie werden kostenintensive Sicherungsmaßnahmen in der Regel nur insoweit duchführen, als sie durch öffentliche Vorschriften oder von ihren Versicherungen dazu gezwungen werden.[11]

Jenseits dieser Effizienzüberlegungen finden alle Sicherungsanstrengungen in jedem Fall ihre Grenze an der finanziellen Leistungsfähigkeit der jeweiligen Organisation. Großorganisationen werden sich daher bessere Sicherungssysteme leisten können als kleine und mittlere. Eine weitere Differenzierung wird durch unterschiedliche Systemarchitekturen entstehen. Die Kosten zur Sicherung eines zentralen Rechners sind leichter aufzubringen als die Ausgaben zum Schutz eines verteilten System mit vielen autonomen Arbeitsplatzrechnern.

Organisationsprobleme

Eine umfassende und effektive Sicherung von IuK-Systemen kann nur mit erheblichen Anstregungen erreicht werden. Um Sicherungsmaßnahmen in betriebliche Abläufe einzubinden, sind viele organisatorische Anpassungen erforderlich: Einführung und Verwaltung von Ausweisen, Chipkarten oder kryptographischen Schlüsseln, Funktionstrennungen und die Verteilung von Betriebsmitteln, Richtlinien für die Klassifizierung der Daten und Anlagen, für den Notfall, für die Dokumentation oder die Auslagerung von Datenbeständen, Festlegung und Formalisierung von Aufgabenbereichen und Zugriffsrechten, Abstimmung von Kompetenzen und Kontrollaufgaben. Um geeignete organisatorische Rahmenbedingungen durchzusetzen, müssen bestehende Strukturen und Abläufe verändert werden. Schon allein die organisatorische Umsetzung verursacht Reibungsverluste. Erst recht problematisch wird die Einführung von Sicherungsmaßnahmen jedoch, wenn gleichzeitig Beharrungsbestrebungen und Kontrollängste überwunden, Interessenkonflikte um Aufgabenverteilung, Ausstattung, Arbeitsbedingungen und Einfluß gelöst sowie Konkurrenzprobleme zwischen Mitarbeitern und Abteilungen beigelegt werden müssen.[12] Mit steigender Vernetzung müssen komplexe Sicherungskonzepte mit viel Mühe unternehmensübergreifend - etwa für den elektronischen Zahlungsverkehr - zwischen vielen Kooperationspartnern ausgehandelt werden.[13] Die hier unvermeidlichen Kompromisse können jedes geschlossene Sicherungskonzept zum Stückwerk werden lassen.

9 S. z.B. Reusch 73; Bschorr 8, 141; Schönberg 90; Evens/Orr 5; Lindemann CW v. 27.4.1984, 1; Wong DuD 1987, 354.

10 S. Pagalies 205.

11 S. auch die Ausführungen im Kap. 9.

12 S. hierzu z.B. Pagalies 187 ff.; von zur Mühlen 119; Weese/Lessing DSB 8/1987, 17.

13 S. z.B. Harmsen/Weiß 74.

Wegen dieser organisatorischen Probleme dürften die Sicherungsmöglichkeiten nur über einen längeren Zeitraum hinweg durchzusetzen sein. Sensible und schadensträchtige Anwendungen werden früher und umfassender, andere, die als weniger sicherungsbedürftig eingeschätzt werden, später und vielleicht nur teilweise gesichert. Diese zeitlichen Verzögerungen können leicht eine Sicherheitslücke entstehen lassen, die zusätzliche Angriffsmöglichkeiten bietet.

Auch wenn die Sicherungssysteme verwirklicht sind, bleiben sie durch eine Fülle organisatorischer Schwierigkeiten in ihrer Effektivität begrenzt. Die besten Sicherungsmaßnahmen laufen ins Leere, wenn sie schlecht organisiert sind.[14]

Was nützt etwa die Parallelverarbeitung auf einer zweiten Maschine gegen einen Bombenanschlag, wenn beide Anlagen aus Platz- oder Organisationsproblemen in einem Raum nebeneinander stehen oder über eine gemeinsame Infrastruktur verfügen? Was bringen Sicherungskopien, wenn sie, im gleichen Raum untergebracht, bei einem Feuer zusammen mit den Originaldaten vernichtet werden.[15] Was helfen die effektivsten Einbruchs-, Bewegungs- und Brandmeldeanlagen, wenn der Alarm in die Hausmeisterwohnung oder die Pförtnerloge geleitet wird, die aber aus organisatorischen oder finanziellen Gründen nicht ständig besetzt sind?[16] Welchen Nutzen haben automatische Aufzeichnungsverfahren aller Tätigkeiten an einem System, wenn für die Auswertung das qualifizierte Personal fehlt.[17] Welche Sicherheit bieten Zugriffssicherungen, wenn in großen Organisationen zur Flexibilität des Betriebsablaufs Rechte zur Weitergabe von Zugriffsrechten vergeben werden müssen und nicht auszuschließen ist, daß unglückliche Kombinationen von mehrstufig verliehenen Rechten zu größeren Zugriffsmöglichkeiten führen, als eigentlich beabsichtigt ist (hidden capabilities)? Welchen Zweck können Sicherungsmaßnahmen noch erfüllen, wenn sich herumspricht, daß ihre Einhaltung nicht überprüft wird?[18]

Selbst einfach handhabare Zugangssicherungen sind nicht ohne praktisch-organisatorische Probleme.

Sie nutzen gegen ungebetene Eindringlinge wenig, wenn aus Mangel an Phantasie oder aus Bequemlichkeit die Zahlen des Geburtstages oder das Autokennzeichen als Kenncode oder der Name der Frau als Paßwort gewählt werden.[19] Selbst eine Institution wie das Fernmeldetechnische Zentralamt der Deutschen Bundespost hat als 'geheimes' Kennwort für seinen Btx-Anschluß die eigene Telefonnummer genutzt - was Hacker schnell herausfanden.[20] Andererseits kann eine komplizierte Ziffern- und Zahlenfolge zu schwierig sein, um sie sich zu merken, zumal sie nicht die einzige ist. In der 'Informationsgesellschaft' wird jeder einzelne viele Zugangsberechtigungen benötigen - zum

14 S. Abel/Schmölz 361; Abel RDV 1988, 75.

15 So 1987 in einem englischen Universitäts-Rechenzentrum geschehen - s. Wong DuD 1987, 352.

16 S. Wesse/Lessing KES 1987, 143, 156.; Sicherheits-Berater 1986, 167.

17 S. Abel RDV 1988, 74f. Aus diesem Grund wurden wiederholte 'Hacks' in das Rechenzentrum der Freien Universität Berlin lange Zeit nicht bemerkt - s. Datenschutz-Berater 7/1987, 1f.

18 S. hierzu Abel/Schmölz 361.

19 Nach Waldschmidt (TH Darmstadt) etwa 70% aller Paßwörter - Darmstädter Echo v. 24.3.1988.

20 S. hierzu TAZ v. 22.12.1984.

Rechner des Arbeitgebers, der Bank, der Informationsdatenbanken, der Versicherung, der Teleshops und vieler anderer. Sie werden also alle aufgeschrieben und in der Brieftasche aufbewahrt oder hinter das heimische Terminal geklebt.[21] Wer sie ausforschen will, weiß, wo er zu suchen hat.[22]

Praktikabilitätsprobleme dieser Art könnten zwar durch Chipkarten verringert werden, weil in ihnen der persönliche Schlüssel einprogrammiert ist. Um sie zu aktivieren, muß aber immer noch eine Code-Nummer eingegeben werden - mit den erwähnten Problemen. Für die unterschiedlichsten Anwendungen müßte jeder eine Vielzahl von Chipkarten bei sich tragen und sich für jede eine andere Codenummer merken. Eine Universal-Karte für alle Anwendungen ist datenschutzrechtlich nicht zulässig, weil sie der Schlüssel für ein lückenloses Persönlichkeitsprofil wäre. Außerdem wäre der Zugang zu allen Systemen verschlossen, ginge sie verloren oder würde gestohlen.

Entwickler von Programmen, Programmierer, Systemverwalter und Wartungstechniker müssen in ihrer Tätigkeit Freiheitsräume besitzen, um ihre Aufgaben erfüllen zu können. Dies erschwert automatische Kontrollen außerordentlich. Die Kontrolle nach der Zwei-Mann-Regel setzt voraus, daß der Kontrolleur mindestens über die gleichen Qualifikationen verfügt. Sie ist daher sehr teuer und kommt wohl nur für sehr sensitive Tätigkeiten in Frage. Außerdem ist sie nur effektiv, soweit sich die beiden Mitarbeiter mißtrauen. Ein so geprägtes Arbeitsklima wirkt sich jedoch negativ auf Kreativität und Produktivität aus. In der Regel schafft allerdings Zusammenarbeit Vertrauen und untergräbt dadurch den Kontrolleffekt. Ein häufiger Wechsel der Arbeitspartner wiederum ist teuer und wenig produktiv. Allzugroße Kontrolleffekte dürfen also von der Zwei-Mann-Regel nicht erwartet werden.[23]

Dieses Problem stellt sich insbesondere für die Wartung. Versagen Hardware-Komponenten, sind Programme fehlerhaft oder sollen erweitert werden oder laufen Routinekontrollen, dann müssen diese Wartungsaufgaben in der Regel von Vertretern der Hersteller oder Entwickler vorgenommen werden. Hierzu ist es erforderlich, Fremdpersonal unter Umgehung aller Schutzmechanismen Zugang zum System und Zugriff auf Programme zu ermöglichen. Es haben sich daher schon Angreifer als Wartungstechniker ausgegeben, um unkontrollierten Zugang zu einem Rechner zu erhalten.[24] Wartungstechniker sind meist hochqualifizierte Systemspezialisten, die dementsprechend geschickt Manipulationen vorbereiten und durchführen könnten. Wartungssicherungen wie das zeitweilige Abtrennen der Sekundärspeicher von der Anlage verhindern zwar den

21 Einen solchen Fall, der zum unberechtigten Bezug eines Programms führte, schildert Norman 94f.

22 Selbst wenn sie sich nicht auf diese Weise einem Angreifer offenbaren, könnte er versuchen, über Virenprogramme Trojanische Pferde in die Anlage einzuschleusen, die alle eingegebenen Paßworte abspeichern und dem Manipulator zur Ansicht bereit halten - s. hierzu Burger 159f.

23 S. hierzu näher Roßnagel 1983, 177f.

24 S. z.B. Weck 61; Abel/Schmölz 281.

unmittelbaren Zugriff auf Daten und Anwendungsprogramme[25], können aber keinen Schutz gegen das Einschleusen von Viren, logischen Bomben oder trojanischen Pferden in die zu wartenden Programme bieten. Eine differenzierte Aufgabentrennung in der Wartung ist äußerst aufwendig und widerspricht den Praxisanforderungen. Allein der hochqualifizierte Spezialist ist in der Lage, unter Zeitdruck Systemfehler zu analysieren, und hat gleichzeitig das Wissen, sie zu beheben.

Noch weiter verschärft werden diese Probleme im Fall der Fernwartung.[26] Greift Personal des Herstellers über Telekommunikation und den speziellen Wartungszugang auf die Anlage zu, bleibt dies in der Regel unbemerkt. Selbst wenn der Wartungszugang verschlossen wird und die Fernwartung angemeldet werden muß, kann der Wartungstechniker bei seiner Arbeit nicht beobachtet werden. Eigentlich müßte nach jeder Wartung eine vollständige Verifikation des Gesamt- oder Teilsystems durchgeführt werden. Sie unterbleibt jedoch, weil sie zu teuer und zeitaufwendig wäre.

Widerstreitende Interessen

Wieviel Sicherheit gut ist, wird nicht immer einhellig beurteilt. Je nach Interessenstandpunkt wird diese Frage sehr unterschiedlich beantwortet. Im konkreten Fall können widerstreitende Interessen zu gravierenden Abstrichen an dem geplanten Sicherungskonzept zwingen. Je lückenloser die Kontroll- und Überwachungspraktiken konzipiert sind, auf umso größeren Widerstand werden sie bei den betroffenen Beschäftigten stoßen. Im Rahmen ihrer Mitbestimmungsrechte haben Betriebs- und Personalräte schon so manche Kontrollmaßnahme vereitelt. Sie werden auch in Zukunft zum Schutz ihrer Kollegen die meisten Sicherungskonzepte zu Kompromissen zwingen.

Abstriche in der Sicherheitsproduktion werden auch von Institutionen verlangt, die eigentlich für größere Sicherheit eintreten müßten - nämlich von den Sicherheitsbehörden. Sie können kein Interesse daran haben, daß Informationen und Kommunikationen so sicher werden, daß sie sogar vor ihnen sicher sind. Denn hinter verschlüsselten oder abhörsicheren Kommunikations- und Informationsverarbeitungsverfahren könnten sich auch Kriminelle, Verbrechersyndikate, Agenten oder Terroristen verstecken. Die rechtlich vorgesehenen Abhörmöglichkeiten für Polizei und Geheimdienste[27] würden durch die technische Entwicklung unterlaufen.[28] Zu erwarten ist daher, daß diese zu verhindern suchen, daß solche Verfahren für das breite Publikum angeboten werden.[29]

25 S. z.B. Abel/ Schmölz 281 ff.; Weck 61 ff.

26 Sie hierzu näher Abel/Schmölz 283 ff.

27 S. z.B. § 100a StPO oder das Gesetz zu Art. 10 GG.

28 S. hierzu näher Rihaczek DuD 1987, 301.

29 Beispielsweise können abhörsichere Geräte nur mit Genehmigung der Zentralstelle für das Chiffrierwesen (ZfCh) bezogen werden - s. Wirtschaftswoche 34/1986, 64.

Die Akzeptanz von Teletransaktionen wird aber gerade in der Geschäftswelt davon abhängen, wie sicher sie sind. Europa- oder weltweit vernetzte Konzerne oder das Kreditgewerbe beispielsweise sind darauf angewiesen, Geldtransaktionen, Geschäftsgeheimnisse oder auch nur interne Informationen unmanipulierbar und unausforschbar zu speichern und zu übermitteln. Diesen vielfältigen Bedarf der Wirtschaft[30] können auch die Sicherheitsbehörden schwer ignorieren. Soweit sie auf dem Weg in die 'Informationsgesellschaft' der "Verschlüsselungsbewegung"[31] nachgeben müssen, werden sie jedoch versuchen, die Entwicklung so weit wie möglich zu kontrollieren. Daher haben in der Vergangenheit den Geheimdiensten nahestehende Institutionen wie die National Security Agency (NSA) in den USA oder die Zentralstelle für das Chiffrierwesen (ZfCh) in Bonn bisher erfolgreich ihren Einfluß geltend gemacht, die Normierung von Verschlüsselungsverfahren national wie international zu verhindern. Sie versuchen, die dadurch entstandene Lücke selbst zu füllen und auch den zivilen Nutzern vorzuschreiben, welche Kryptosysteme sie verwenden dürfen, um dadurch letztlich ein Staatsmonopol für die Datenverschlüsselung zu erreichen.[32] Allerdings wollen sie ihre Systemstandards nicht veröffentlichen, sondern den Nutzern lediglich die Schlüssel zuteilen.[33] Dies hätte für die Nutzer einen dreifachen Effekt: Sie könnten sicher sein, daß die Geheimdienste und die Behörden der inneren Sicherheit über ihren Schlüssel verfügen. Sie könnten daher nicht sicher sein, daß diese ihre Insider-Probleme beherrschen und dadurch der Schlüssel nicht noch in weitere Hände gelangt. Schließlich müßten sie einen Schlüssel verwenden, dessen Sicherheit gegen Brechungsversuche sie nicht beurteilen können.

Die künftige Entwicklung steht offenbar vor der grundsätzlichen Alternative: Entweder unterbleibt die öffentliche Normung von Verschlüsselungsstandards - dann könnten offene Systeme nur unter den genannten Unsicherheitsbedingungen betrieben werden.[34] Oder die Sicherheit offener Netze wird durch genormte und nicht restringierte Verschlüsselungsverfahren erhöht. Dies ist allerdings nur zu erwarten, wenn der technische 'Fortschritt' der 'nachrichtendienstlichen Mittel' den dadurch benachteiligten Behörden ausreichenden Ersatz bietet.[35]

30 S. hierzu z.B. den Eureka-Projektvorschlag: Offene und sichere Informations-Systeme (OASIS) eines internationalen Konsortiums von Unternehmen, dokumentiert in RDV 1987, 23 ff.; für den Bankenbereich, in dem sensitive Nachrichten verschlüsselt werden s. Harmsen/Weiß 24; Nixdorf bietet z.B. DES-verschlüsselnde und Racal-Milgo RSA-verschlüsselnde Systeme an - s. Bäumler DSB 8/1987, 3.

31 Rihaczek DuD 1987, 243.

32 S. Rihaczek DuD 1987, 300.

33 S. hierzu näher Rihaczek DuD 1987, 240 ff.; Waidner/Pfitzmann/Pfitzmann DuD 1987, 297f.; Coy 83 ff; Fölsing 92 ff.

34 S. hierzu näher Rihaczek DuD 1987, 301.

35 Zu Kompromißvorschlägen, den Bedürfnissen dieser Behörden durch technische Einschränkungen von Verschlüsselungsmöglichkeiten weiter entgegenzukommen - s. Rihaczek DuD 1987, 302f.

'Menschliche Schwächen'

Sicherungssysteme sind darauf angewiesen, daß die Menschen, die sie betreiben, zuverlässig funktionieren. Menschen aber sind mitunter überfordert, leichtgläubig, abgelenkt, unaufmerksam, vergeßlich, übermüdet, gelangweilt, zu zuversichtlich oder für Stimmungsschwankungen anfällig. Jedes Sicherungssystem ist nur so stark wie das schwächste Glied in der Sicherungskette. Soweit Menschen Sicherungsfunktionen ausüben - und dies wird in unterschiedlichem Maße immer der Fall sein -, ist die Sicherheit von IuK-Systemem immer durch sogenannte 'menschliche Schwächen' gefährdet.

Das Sicherheitsbewußtsein ist im Bereich der IuK-Technik sehr unterschiedlich ausgeprägt, im Durchschnitt jedoch niedrig.[36] Nur 6% der deutschen Unternehmen haben nach der schon erwähnten EG-weiten Umfrage unter Managern bisher den Notfall vollständig getestet.[37] Noch erheblich weniger haben Verträge mit Ersatzrechenzentren abgeschlossen.[38] Das Sicherungsbewußtsein steigt zwar an, wird aber auch künftig nicht sehr hoch sein. Bezogen auf die Vielzahl der IuK-Anwendungen werden Angriffe gegen das einzelne System relativ seltene Ereignisse sein, die nicht in Erfahrung repräsentiert sind. Der einzelne hat daher auch keine intuitive Möglichkeit, die Mißbrauchsrisiken abzuschätzen. Sie werden verdrängt oder systematisch unterschätzt.[39]

Soweit Sicherungen nicht automatisiert sind, erweisen sie sich in der Regel als umständlich und behindern den alltäglichen Betriebsablauf. Die Versuchung ist groß, sie zu umgehen oder zu ignorieren.[40]

Die mit einer automatischen Ein- und Ausgangskontrolle versehenen Türen des abgeschlossenen Rechenzentrums nutzen nichts, wenn sie aus Bequemlichkeit mit einem Keil offengehalten werden.[41] Ebenso kann die beste logische Zugangskontrolle nicht verhindern, daß ein Unbefugter an einem Terminal arbeitet, wenn der Berechtigte, um sich nicht jedesmal neu anmelden zu müssen, in den Arbeitspausen den Bildschirm nur abschaltet, und sich nicht abmeldet. Eine solche Situation nutzten Darmstädter Hacker aus, um die Paßwortdatei eines Schulinformationssystems im Kommunalen Gebietsrechenzentrum abzuschreiben und mit deren Hilfe ein intensives Hacking zu betreiben.[42]

Auch andere 'Schwächen' wie Neugierde oder Leichtgläubigkeit können Sicherungsmaßnahmen außer Kraft setzen.

---

36 S. hierzu z.B. Evens/Orr 5, 17 ff.; Schönberg 92; für den Bankenbereich Harmsen/Weiß 75.

37 S. Evens/Orr 17.

38 S. Harmsen/Weiß 69 ff., 75.

39 S. hierzu z.B. Weise CW v. 22.8.1986, 7.

40 S. z.B. Pagalies 199f.; Schönberg 93.; Weck 55.

41 S. z.B. Weck 55.

42 S. Darmstädter Echo v. 24.3.1988.

Kein Zugriffsschutz und keine Abschottung der Benutzer kann verhindern, daß ein neugieriger System-Operator in einer langweiligen Nachtschicht ein neues Telespiel ausprobiert oder ein hilfsbereiter Systemmanager das defekte Programm eines Benutzers auf seine Ebene überspielt, um den Fehler zu analysieren - und dadurch unbewußt eine Virenverseuchung des gesammten Systems ermöglichen.[43] Ein Paßwortschutz verliert jeden Wert, wenn ein leichtgläubiger Mitarbeiter einem Fremden, der sich am Telefon als Mitarbeiter einer Wartungsfirma ausgibt, das Paßwort verrät: so geschehen, als ein Hacker gegenüber einem FTZ-Beschäftigten erklärte, die Paßwortdatei des Telebox-Systems sei teilweise zerstört und ganz nebenbei nach dem alten Paßwort fragte.[44] Schließlich wurde sogar schon einmal eine ganze Zentraleinheit von einem angeblichen Wartungstechniker ausgebaut und mitgenommen.[45]

Dynamische Angriffe, statische Abwehr

Die Sicherung von IuK-Systemen wird bürokratisch organisiert. Die Definitionen der Auslegungsbedrohung und der Sicherheitsklassen, die Anforderungen an technische Sicherheitseinrichtungen und die Organisation der Sicherung werden in Regeln fixiert. Die potentielle Bedrohung dagegen entwickelt sich sehr dynamisch. Die Diskrepanz zwischen der Statik des Sicherungssystems und der Dynamik der Bedrohung wird immer wieder Sicherungslücken schaffen, die zu spät erkannt werden können.[46]

In der Vergangenheit wurden immer wieder neue, bis dahin nicht bekannte Angriffsformen entwickelt, gegen die dann wiederum passende Sicherungskonzepte erst erfunden werden mußten. So ist zum Beispiel die Möglichkeit von Virenangriffen erst seit wenigen Jahren bekannt. Sicherheitsexperten haben dies erst nicht ernst genommen und belächelt. Auch für die Zukunft ist daher zu erwarten, daß die dynamische Entwicklung der Technik und die Phantasie motivierter Personen bisweilen neue, überraschende Angriffsformen hervorbringen.[47]

Immer wieder sind 'unüberwindliche' Sicherheitsbarrieren letztlich doch überwunden worden. Ein plastisches Beispiel hierfür ist der neue 'fälschungssichere' Personalausweis. Bereits kurze Zeit nach seiner Einführung wurden mit Hilfe von hochwertigen Fotokopierern und Folienschweißgeräten täuschend echte Ausweise hergestellt.[48] Manche Sicherungsmaßnahmen beruhen auf unbewiesenen Annahmen - so zum Beispiel die Ausforschungssicherheit der Chipkarte. Zwar konnten auch keine Aussagen gefunden werden, die bestätigen, daß sie ausforschbar ist. Sollte jedoch jemals ein Verfahren hierzu entwickelt werden - es würde auch von Kriminellen genutzt. Sie könnten dann die geheimen

43 S. zu diesen Beispielen von Fix in Burger 305 ff.

44 S. Chaos Computer Club 144.

45 S. Weck 54.

46 S. auch für den Bankenbereich Harmsen/Weiß 74.

47 S. hierzu auch Abel/Schmölz 24.

48 S. hierzu z.B. Stern v. 4.2.1988 sowie die Aussage des BKA, geschultes Fachpersonal könne die Fälschung erkennen - FR v. 11.2.1988.

Schlüssel auslesen, damit Chipkarten fälschen und sie mit Bereicherungsabsicht zu Transaktionen nutzen.[49] Ob der ständige Wettstreit zwischen Angreifern und Verteidigern immer zugunsten der letzteren ausgeht, ist also keineswegs gesichert.

Ein besonders gravierender Einbruch der 'Sicherungsfront' wäre das Brechen der Verschlüsselungsalgorithmen. Dies ist keineswegs ausgeschlossen. Denn die Sicherheit der heute gebräuchlichen Verschlüsselungssysteme ist im strengen Sinn nicht bewiesen. Das symmetrische 'Data Encryption Standard' (DES), ein auf organisiertem Chaos beruhendes System, hat bisher allen veröffentlichenten Versuchen widerstanden, es zu brechen. Dies kann bis zum Beweis des Gegenteils als Validierung angesehen werden. Die Sicherheit des asymmetrischen - nach seinen 'Erfindern' Rivest, Shamir und Adleman benannten - RSA beruht im Gegensatz dazu auf teilweise unbewiesenen Annahmen über den Lösungsaufwand zahlentheoretischer Probleme. Es wird allgemein vermutet, daß das Ableiten des privaten aus dem öffentlichen Schlüssel so schwer ist wie die Gewinnung von Primfaktoren einer gegebenen Zahl. Eine Faktorisierung von Zahlen, die aus sehr großen Primfaktoren zusammengesetzt sind, ist bisher praktisch unmöglich.[50]

Seit 2000 Jahren wurden bislang alle Algorithmen, auf die es ankam, auch geknackt. Sollten neue Lösungsalgorithmen[51] und die Steigerung der Rechnerleistung es irgendwann einmal ermöglichen, Verschlüsselungsverfahren zu brechen, wäre ein wichtiges Glied der Sicherungskette zerrissen. Keine der Chipkarten, die mit diesem Verfahren arbeiten, würde mehr Sicherheit bieten. Keines der Dokumente und Datensätze, die mit seiner Hilfe verschlüsselt wurden, wäre mehr manipulations- und spionagesicher.[52] Wie sollten aber in kürzester Zeit alle Zugangs- und Zugriffssicherungen auf ein neues Verschlüsselungsverfahren umgestellt, allen Nutzern neue Chipkarten zugeteilt und alle bereits verschlüsselten Texte neu verschlüsselt werden? Unter Umständen könnten diese Folgen schon allein durch den begründeten Verdacht ausgelöst werden, ein potentieller Gegner könnte Kryptographieprogramme entschlüsselt haben.[53]

Gesellschaftliche Instabilität

Die Sicherungssysteme funktionieren nur in Zeiten und Gegenden sozialer und politischer Stabilität. Gerade in zugespitzten gesellschaftlichen Konfliktsituationen ist die Verläßlichkeit von Sicherungssystemen besonders wichtig. Wie aber könnte in einem existenziellen

49 S. hierzu Hammer DuD 8/1988; Waidner/Pfitzmann/Pfitzmann DuD 1987, 298.; weniger skeptisch Rihaczek DuD 1987, 302.

50 S. hierzu z.B. US-National Bureau of Standards; Rivest/Shamir/Adleman CACM 1978, 120 ff.; Herda; Waidner/ Pfitzmann/ Pfitzmann DuD 1987, 293 mwN; Pfitzmann/Pfitzmann/Waidner, Informatik Spektrum 1987, 126 mwN; Rihaczek DuD 1987, 244.; Abel/Schmölz 314 ff.; Coy 86 ff.; Fölsing 104f.; Harmsen/Weiß; US-National Computer Security Center 171.

51 S. hierzu z.B. CW v. 5.9.1986 einerseits und Spiegel 19/1988, 216 ff. andererseits.

52 S. hierzu z.B. Hammer DuD 8/1988.

53 S. hierzu z.B. Burger 160f.

Konflikt garantiert werden, daß die Sicherungskräfte und die in IuK-Systemen Beschäftigten sich jeder politischen Entwicklung gegenüber loyal verhalten? Wie könnte verhindert werden, daß sie die Abhängigkeit der Gesellschaft von dem von ihnen kontrollierten IuK-System für ihre Partikularinteressen mißbrauchen? Zu befürchten ist dagegen, daß die sozio-technischen IuK-Systeme aufgrund ihrer Verwundbarkeit gesellschaftliche Unruhen nicht stabilisieren, sondern eher dynamisieren.[54]

Zusammenfassend ist zu erwarten, daß künftig das praktische Restrisiko erheblich höher sein wird als das theoretische oder potentielle Mindestrisiko. Die Probleme der Praxis werden die konsequente Durchsetzung optimaler Sicherungskonzepte verhindern. Die vielfältigen Kompromisse in der praktischen Einführung und täglichen Umsetzung von Sicherungsmaßnahmen führen ebenso wie menschliche Unzulänglichkeiten und bürokratische Verfestigungen zu erheblichen Sicherheitsabstrichen. Nur wenige hochsensible Anwendungen werden optimal geschützt sein. Die überwiegende Mehrzahl der IuK-Systeme dürfte dagegen weit unter dem möglichen Sicherungsniveau liegen. In der Regel wird ein angespannter Optimismus vorherrschen: Man hat eine Reihe von Sicherungsmaßnahmen ergriffen, weiß, daß diese nicht ausreichend sind, hofft aber, daß es nicht zu größeren Schäden kommt.

54 S. z.B. Lutterbeck 1985, 18; Steinmüller Kursbuch 66 (1981), 184 ff.; zur insoweit parallelen Problematik der Sicherungs der Atomenergie Roßnagel 1983, 237 ff.; 1987, 140 ff.

15. Gesellschaftliche Kosten der Sicherung

Technische Sicherungsmaßnahmen allein sind unzureichend. Ergänzend muß daher versucht werden, Sicherheit durch Strategien herzustellen, die gegen Menschen gerichtet sind. Diese Sicherungsmaßnahmen gibt es nicht kostenlos. Sie fordern neben einem finanziellen auch einen gesellschaftlichen Preis. Ihn wollen wir am Beispiel der Freiheits- und Demokratieeinbußen näher untersuchen. Je nach seiner Höhe kann er Rückwirkungen auf das tatsächliche Sicherungsniveau haben. Steigen die Kosten zu sehr an, könnten Abstriche am Sicherheitsziel folgen. Ihre Höhe steht jedoch nicht fest. Sie ist neben der tatsächlichen Leistung technischer Sicherungen vor allem abhängig von dem künftigen Bedrohungspotential und dessen - davon zu unterscheidender - Rezeption in der Öffentlichkeit. Je nachdem kann die folgende Kostenkalkulation - mit der wir wieder versuchen eine Trendentwicklung zu erfassen - zu hoch oder zu niedrig sein.

Freiheitskosten

Wer früher Informationen mit Papier und Bleistift verarbeitete und mittels Brief und Telefon kommunizierte, war von der Tätigkeit her - abgesehen vom Bereich der Geheimhaltung - keinen Sicherungsmaßnahmen unterworfen. Wer künftig an vernetzten Computersystemen oder gar in deren Zentren tätig sein wird, sieht sich, auch wenn er die gleichen Informationen verarbeitet wie sein altmodischer Vorgänger, vielfältigen Sicherungsmaßnahmen gegenüber. Die Arbeitsplätze dieser Mitarbeiter sind gegenüber der Außenwelt sorgsam abgeschirmt. Um zu ihrem Arbeitsplatz zu gelangen, müssen sie Zu- und Ausgangskontrollen überstehen. Kollegen in anderen Abteilungen können sie nur besuchen, wenn sie mit ihrer Chipkarte die Türen dorthin öffnen können. Während ihrer Arbeit werden sie überwacht. Sie dürfen nur dann in sensitiven Betriebsteilen arbeiten, wenn ihre Zuverlässigkeit vor der Anstellung als ausreichend bewertet wurde. Da sie nach der Einstellung weiterhin gesellschaftlichen Einflüssen unterliegen, muß ihre Verläßlichkeit immer wieder durch Wiederholungsüberprüfungen bestätigt werden.

Die von ihnen ausgehenden Risiken für das Funktionieren der IuK-Systeme können aber nur dann zuverlässig abgeschätzt werden, wenn sie umfassend, also auch hinsichtlich ihres Privatlebens, überprüft werden. Um alle möglichen Einflußfaktoren vollständig erfassen zu können, wird auch ihr soziales Umfeld in diese Prüfung mit einbezogen. Daß dadurch nicht nur ihre Grundrechte betroffen sein werden, sondern auch die ihrer Verwandten und Bekannten, die nicht in den Eingriff eingewilligt haben, ja von ihrer Überprüfung vielleicht nicht einmal etwas erfahren, wird im Interesse eines effektiven Sicherungssystems nicht zu vermeiden sein.

Die Betroffenen wissen nicht genau, welches Verhalten einen Risikofaktor begründet oder einmal begründen kann. Während der Beschäftigung, aber auch schon lange zuvor,

führt die Kenntnis künftiger Überprüfungen und die Unkenntnis der genauen Kriterien zu einer Eigenkontrolle des Verhaltens. Sie machen von bestimmten Grundrechten wie der Meinungsfreiheit, der Versammlungs- und Demonstrationsfreiheit und der Vereinigungsfreiheit oder der Freiheit der Parteimitgliedschaft oft lieber keinen Gebrauch. Sie wollen keinen Anlaß für Spekulationen über ihre Zuverlässigkeit bieten.

In einem informatisierten Betrieb fallen so viele Informationen über den einzelnen Beschäftigten an, daß es bei einer geschickten Verknüpfung all dieser Informationen leicht möglich ist, über jeden Beschäftigten ein Persönlichkeitsabbild zu erstellen. Aus diesen könnten Risikoprofile entwickelt werden, die Anfälligkeiten und Schwachstellen eines jeden Beschäftigten aufzeigen und erlauben, ihn risikogerecht bestimmten Arbeitsplätzen zuzuweisen oder von ihnen fernzuhalten.

Es ist sehr zweifelhaft, ob die Voraussetzungen für das lebenswichtige Funktionieren von IuK-Systemen Gegenstand von Mitbestimmungsrechten der kollektiven Interessenvertretung der Beschäftigten oder Verhandlungsgegenstand der Sozialpartner sein kann, auch wenn durch sie die Arbeitsbedingungen intensiv beeinflußt werden. Schon derzeit ist zu beobachten, daß immer mehr solcher sensitiver Funktionen aus dem Blickwinkel des Allgemeininteresses durch staatliche Vorschriften geregelt werden, die beide Sozialpartner oder Arbeitgeber und Betriebsrat gleichermaßen binden. Dadurch schwindet der sachliche Gegenstandsbereich von betrieblichen Vereinbarungen und Tarifverträgen beträchtlich.[1]

Bereits heute beeinträchtigen die präventiven und repressiven Aufklärungsmaßnahmen die Freiheit vieler Bürger. Denn um wenige potentielle Gegner zu finden, müssen sehr viele Unbeteiligte überprüft und überwacht werden. Vor allem werden von diesen Maßnahmen die Bürger betroffen sein, die mit der jeweils herrschenden Politik unzufrieden sind und dagegen protestieren wollen. Wer aber "damit rechnen muß, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten". Dies beeinträchtigt "nicht nur die individuellen Entfaltungschancen des einzelnen ..., sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist".[2]

In erheblich stärkerem Maße aber werden die zu erwartenden Verschärfungen der Aufklärungsanstrengungen die Freiheit aller beeinträchtigen[3]: Raster-und Gitternetzfahndungen, beobachtende Fahndung, Muster- und Spracherkennung und -verarbeitung sowie computergesteuerte Überwachung der Telekommunikation. Um die oben genann-

1 S. hierzu z.B. Simitis/Rydzy; Roßnagel 1984a, 125 ff.; Beck/Wendeling-Schröder, WSI-Mitteilungen 1985, 745 ff.

2 BVerfGE 61, 1 (43).

3 S. hierzu z.B. Hase DuR 1984, 39 ff.

ten Aufgaben der Prävention erfüllen zu können, müssen vielfältigste Anzeichen für Mißbrauchsaktionen erkannt, erfaßt, gespeichert und bewertet werden. Als solche könnten insbesondere Infiltrationsversuche von 'Risikopersonen' in sensitive Datenverarbeitungszentren, Kontaktaufnahmen mit Insidern oder der Erwerb von geeigneten Gegenständen gelten. Damit aber gelangen sehr weite Bereiche des normalen Verhaltens in den Informationszugriff der Sicherungsorgane. Von ihrer Situationseinschätzung hängt es ab, welches Verhalten als Risiko gilt und damit Gegenstand einer vorbeugenden Fahndungsmaßnahme wird. Wer dieser entgehen will, paßt sich der Konformitätsdefinition der Sicherungsorgane an. Jede zusätzliche Maßnahme des vorbeugenden Schutzes wird so die Freiheit Stück um Stück verkürzen.[4]

Steht einer solchen Entwicklung aber nicht das Grundgesetz entgegen, das uns doch die Ausübung von Grundrechten garantiert? Für diese Hoffnung gibt es leider nur wenig Anlaß. Die Rechtsprechung wird eher die Verfassung dem Sicherungszwang anpassen und die Grundrechte in einem modifizierten Sinn verstehen, als die Freiheit einzelner auf Kosten der Sicherheit der Allgemeinheit durchsetzen. Freiheitsbegrenzungen im Rahmen des Sicherungssystems von IuK-Techniken stehen im Spannungsfeld zwischen individueller Freiheit und der Schutzpflicht des Staates für Rechtsgüter einzelner und der Allgemeinheit. Das Bundesverfassungsgericht entscheidet Konflikte, in denen verschiedene Verfassungsziele zum Ausgleich gebracht werden müssen, in der Regel nach den Prinzipien der Güterabwägung und der Verhältnismäßigkeit. In künftigen Entscheidungen wird es im Rahmen einer Güterabwägung berücksichtigen, daß die IuK-Systeme zum Teil lebenswichtige soziale Funktionen übernommen haben und daher auch von den Verfassungswerten geschützt werden, welche die Aufrechterhaltung gesellschaftlicher Funktionszusammenhänge gewährleisten sollen. Je größer daher das Schadenspotential der IuK-Anwendungen ist, desto stärkere Einschränkungen von Freiheitsrechten erlauben auch die Prinzipien der Güterabwägung und der Verhältnismäßigkeit.

Hat das Bundesverfassungsgericht einen Konflikt zwischen verschiedenen 'Verfassungswerten' zu entscheiden, bemüht es sich, die Wirksamkeit beider Konfliktgüter durch schonendsten Ausgleich zu optimieren. Wegen deren unterschiedlicher 'Wertigkeit' kann dieses Bemühen jedoch selten zu beiderseitigem Nachgeben führen. Vielmehr folgt in der Rechtsprechung des Verfassungsgerichts gerade aus dem Prinzip der Güterabwägung beinahe ausschließlich ein einseitiger Vorrang des Bestands der Bundesrepublik Deutschland und ihrer freiheitlichen demokratischen Grundordnung, der Volksgesundheit und anderer Gemeinschaftswerte gegenüber fast allen Grundrechten.[5]

Je höher das Risiko der mißbräuchlichen IuK-Nutzung sein wird, desto gewichtiger wird das Argument werden, Datenschutz dürfe nicht zum Tatenschutz werden.[6] Dann könnten sich auch leichter Abwägungen durchsetzen wie die von Generalbundesanwalt

4 S. z.B. auch Lutterbeck 1987, 47.

5 S. hierzu die Nachweise in Schneider, H. 1979, 211, 217, 225f. und Roßnagel 1984a, 64 ff.

6 S. z.B. Honnacker DuD 1987, 221.

Rebmann: Sicherheit vor Datenschutz - denn es gehe "gerade im sogenannten Sicherheitsbereich ... um - auch dem Datenschutz weit überlegene - vitale Gemeinschaftsinteressen".[7]

Das Verhältnismäßigkeitsprinzip, das zweite Konfliktregelungsmuster, ist für den Freiheitsschutz ambivalent. Es begrenzt freiheitsbedrohende Eingriffe, wenn deren Notwendigkeit zum Schutz hochrangiger Interessen nicht nachgewiesen werden kann - ermöglicht sie aber, wenn dieser Nachweis gelingt.[8] Es darf "nur das unbedingt Notwendige (hier heimliche Abhörmaßnahmen) zum Schutz eines von der Verfassung anerkannten Rechtsgutes - hier der Bestand des Staates und seiner Verfassungsordnung - im Gesetz vorgesehen und im Einzelfall angeordnet werden".[9] Die unbedingt notwendigen Sicherungsmaßnahmen sind dann aber auch unbedingt zu ergreifen. Sie sind - wie etwa umfassende Hintergrundüberprüfungen - dann geeignet, erforderlich und in Relation zur Größe der Gefahr nicht übermäßig belastend.[10] Gegen Maßnahmen, die für die Funktionsfähigkeit des Sicherungssystems unerläßlich sind - und hierüber entscheiden die Sicherungsbehörden nach weitgehend politischen Erwägungen in eigener Verantwortung[11] - kann es keinen Schutz gewähren. Im Gegenteil, es wird eine der Einbruchsstellen sein, durch die sich das Sicherungssystem rechtliche Anerkennung erobert. Denn "es kann nicht Sinn der Verfassung sein", etwa den Verfasssungschutzbehörden "zwar eine Aufgabe zu stellen", ihnen aber "die Mittel vorzuenthalten, die zur Erfüllung (ihres) Verfassungsauftrags notwendig sind".[12]

Kann etwa nachgewiesen werden, daß die künftigen Möglichkeiten rechnergestützten Stimmenvergleichs, Sprach- und Bilderkennung sowie -verarbeitung die gesellschaftliche und betriebliche Sicherheit erhöhen können, dürfte dies zu einer veränderten Konkretisierung des Rechts am eigenen Bild und eigenen Wort führen. Es insoweit einzuschränken ist dann verhältnismäßig, weil diese Sicherungsmittel tauglich und notwendig sind, um überragende Rechtsgüter zu schützen. Ähnliche Bedeutungsänderungen dürften auch die übrigen dargestellten Sicherungsmaßnahmen für die Grundrechte der Beschäftigten und vieler Bürger verursachen.[13] Beide Konfliktregelungsmuster würden eine faktische Beschränkung der Mitwirkungsmöglichkeiten des Betriebsrats oder der Verhandlungsgegenstände der Tarifpartner im Bereich der Sicherungssysteme ebenso rechtfertigen wie eine Einschränkung des Streikrechts oder Arbeitsverpflichtungen legitimieren. Die dahinterstehenden 'Sachzwänge' könnten mit ihrer Hilfe zu einem faktischen Grundrechts-

7 Rebmann KR 1982, 153f.

8 S. hierzu auch Schneider, Hans 1976, 391; Mayer-Tasch 1984, 74.

9 S. BVerfGE 30, 1 (20); vgl. auch 7, 377 (397 ff.).

10 Vgl. hierzu ausführlich Roßnagel 1984a, 95 ff.

11 S. BVerfGE 12, 45 (52); 46, 160 (164); 48, 127 (160); 49, 89 (131).

12 BVerfGE 30, 1 (20).

13 S. hierzu im einzelnen Roßnagel 1984a, 68 - 202 mwN.

schwund durch die stille und allmähliche Veränderung der Rechtsbegriffe führen. Verläßliche Grenzen eines solchen Grundrechtswandels gibt es nicht.[14]

Demokratiekosten

Offene Systeme sind logischen Angriffen fast schutzlos preisgegeben. Weitgehenden Schutz gegen Viren, logische Bomben und trojanische Pferde gewährleisten nur eine rigorose Abschottung der Systeme, die Isolation der Benutzergruppen und die Überprüfung und Überwachung der Mitarbeiter.[15] In den meisten Anwendungsbereichen müssen aber die Benutzer auf einen gemeinsamen Bestand von Daten und Programmen zugreifen und diesen mit anderen austauschen können. Mehrfachnutzung von Rechnern, Arbeitsplatzsysteme, Rechnerverbund sowie offene Netze auf der einen und eine rigorose Abschottung auf der anderen Seite widersprechen sich. Die 'Informationsgesellschaft' gerät in das Dilemma, zwischen Offenheit und Sicherung wählen zu müssen. In der Praxis wird sie für jeden Anwendungsfall einen Weg zwischen beiden Extremen suchen. Das wird jedoch nicht immer der Mittelweg sein. Für alle IuK-Nutzungen, die mit einem hohen Schadenspotential behaftet sind, wäre das Risiko viel zu hoch.[16]

Angesichts der Verletzlichkeit der 'Informationsgesellschaft' wird ihre Offenheit zur leeren Versprechung. Die psychische Mobilität und die intellektuelle Bereicherung in freien weltweiten Computernetzen und offenen Informationssammlungen, der unbegrenzte Zugriff auf den geistigen Reichtum der Gesellschaft, der freie Austausch von Ideen und Informationen - alle diese Träume zerschellen an den geschlossenen Benutzergruppen, den Chipkarten- geschützten Zugangskontrollen, den eng beschränkten Zugriffsrechten, den verschlüsselten Datensammlungen und den abgekapselten Informationsbunkern. Statt 'free flow of information' und offener Netze werden Abschottung, Kontrolle, Überprüfung und Überwachung das Bild der 'Informationsgesellschaft' prägen.

Über die Notwendigkeit einer Sicherungsmaßnahme entscheiden nicht die Betroffenen. In Unternehmen und Behörden bestimmen dies die obersten Vorgesetzten oder ihre Sicherheitsbeauftragten. In der Öffentlichkeit entscheiden darüber die Sicherheitsbehörden nach weitgehend politischen Erwägungen in eigener Verantwortung.[17] Denn die Sicherungskräfte allein verfügen über die erforderlichen Informationen. Wie zwingend der Sicherungszwang, wie notwendig die Machtsteigerung der Sicherungskräfte jeweils ist, können Außenstehende schwer beurteilen. Die Gefahr des Mißbrauchs wächst jedoch im

14 Nicht einmal die in Art. 19 Abs. 2 GG normierte Garantie des Wesensgehalts der Grundrechte kann eine Anpassung des Rechtsverständnisses an neue Funktionsbedingungen wichtiger Allgemeininteressen verhindern. S. hierzu näher Roßnagel 1984a, 66f.

15 S. hierzu z.B. Müller DuD 1987, 483 ff.; Abel/Schmölz 12; Dierstein 99 ff.; Brunnstein AI 1987, 401; Burger 56, 374 ff.

16 S. hierzu auch Dierstein 109.

17 S. hierzu z.B. BVerfGE 12, 45 (52); 46, 160 (164); 48, 127 (160); 49, 89 (131).

Quadrat der Heimlichkeit. Die peinliche Sorgfalt, mit der alle Maßnahmen im Sicherungsbereich geheimgehalten werden, erschwert selbst eine interne Überwachung und schließt die Kontrolle durch die Öffentlichkeit weitestgehend aus.

In einer von Sicherheitsdenken geprägten Gesellschaft geht die Definitionsmacht für sozial und politisch verträgliches Verhalten weitgehend vom Parlament auf die Sicherungskräfte über. Sie handeln auf der Grundlage von unbestimmten Generalklauseln unter einem umfassenden Präventionsauftrag.[18] Sie bestimmen, indem sie diese konkretisieren, was als verdächtig oder riskant gilt, was erfassungs- und untersuchenswert erscheint, was 'gefährlich' oder 'verfassungsfeindlich' ist. Sie beeinflussen durch ihre Kontroll- und Überprüfungstätigkeit das Verhalten von Bürgern und Gruppen. Sie steuern über deren Anpassungsverhalten in starkem Maß die gesellschaftliche Entwicklung.

Die personenbezogenen Sicherungsmaßnahmen sind jedoch keineswegs allein in der gesellschaftlichen Verletzlichkeit durch IuK-Technik begründet. Die in die Gesellschaft hinein vorverlagerten Aufklärungsmaßnahmen werden - noch mehr als die objektbezogenen Sicherungsvorkehrungen - auch ergriffen, wenn diese durch andere hochriskante Techniken verletzlicher würde[19], wenn ihre Kriminalitätsrate weiter ansteigt, wenn sie sich vermehrter Spionage und Sabotage erwehren muß oder ihre politische Stabilität gefährdet erscheint. Verstärkte Vorfeldaufklärung und die Anwendung neuer elektronischer Fahndungsmethoden entsprechen ohnehin der gegenwärtigen Umorientierung der Polizei von dem rechtsstaatlich-liberalen Modell eingegrenzter Handlungsbefugnisse hin zu einem umfassenden, an der gesellschaftlichen Stabilität orientierten Aufgabenverständnis.[20] Die Nutzung katastrophenträchtiger IuK-Systeme ist daher bei weitem nicht der einzige Grund für eine Steigerung gesellschaftlicher Überwachung. Aber sie ist ein hinreichender.

Die Verletzlichkeit der 'Informationsgesellschaft' schafft eine neue und nur sehr schwer zu widerlegende Legitimationsgrundlage für einen weiteren Ausbau der Sicherheitsapparate. Schon sie allein würde die geschilderte Verstärkung von Sicherungsanstrengungen rechtfertigen. Denn durch den Mißbrauch der IuK-Technik werden katastrophale Schäden möglich, die sich nie ereignen dürfen. Um sie zu verhindern, müssen alle möglichen Anstrengungen unternommen werden. Die Logik dieser Katastrophenprävention wird zu einem Imperativ gesellschaftlicher Entwicklung.

Der Sicherungszwang der IuK-Technik trägt so mit dazu bei, daß die gesellschaftlichen Verhältnisse erstarren und zu verhärten drohen. Wegen ihrer Verletzlichkeit fordert die 'Informationsgesellschaft' eine hohe gesellschaftliche Stabilität.[21] Soziale oder politische Experimente, die diese in Frage stellen könnten, dürfen nicht mehr geduldet werden. Politische Alternativen, die mit einem Stabilitätsrisiko verbunden sind, haben wenig

18 S. hierzu näher z.B. Stümper KR 1980, 242 ff.; ders. KR 1981, 76 ff.; Boge KR 1982, 240f.

19 S. hierzu z.B. Roßnagel 1983; 1986, 337 ff.; 1987a.

20 S. hierzu z.B. Busch u.a. 227 ff. ; Roßnagel 1983, 87f., 204; Pordesch 1989.

21 S. hierzu auch Lenk 330 ff.; Lutterbeck 1985, 18.

Umsetzungschancen. Die erhöhte Flexibilität von Produktionsstrukturen und Organisationssystemen und die vielfältigen sozialen Veränderungen, die durch den Einsatz der IuK-Technik ermöglicht bzw. erzwungen wurden, werden auffällig kontrastieren zur politischen Unbeweglichkeit dieser Gesellschaft.

Ereignet sich dennoch eine informationstechnische Katastrophe, ist neben den materiellen und immateriellen Schäden, die bereits erörtert wurden, auch eine drastische Veränderung der politischen Kultur zu befürchten. Bisherige Erfahrungen zeigen, daß bereits als Folge eines spektakulären Terroranschlags ein "symbolischer Belagerungszustand"[22] eintreten kann. Für diesen ist kennzeichnend, daß das allgemeine Empfinden der Bedrohung auch den Verdacht verallgemeinert und an die Stelle liberalen Gewährenlassens in Zeiten innerer Ruhe einen Konsensuszwang und einen Entscheidungszwang setzt. Eine vorher mögliche Neutralität oder Ambivalenz gegenüber der gegebenen Gesellschaftsverfassung wird ersetzt durch einen von Freund-Feind-Denken geprägten Entscheidungszwang. "Es genügt nicht mehr, den Staat und seine Verfassung zu akzeptieren, man muß sie bedingungslos befürworten, wenn nicht sogar lieben."[23] Die Verunsicherung durch einen Anschlag fordert eine positive Versicherung der Solidargemeinschaft. Durch den Konsensuszwang wird Homogenität und soziale Dichte angestrebt. Die Grenzen des moralisch Erlaubten verengen sich, und die Sanktionen für Abweichungen werden erhöht. Dies führt zur Ausgrenzung von Bevölkerungsgruppen, deren Folgebereitschaft gegenüber den politischen Instanzen zu Zweifeln Anlaß geben. Wenn solche oder ähnliche Reaktionen schon bei einem für die Bevölkerung vergleichsweise 'harmlosen' Terroranschlag wie der Schleyer-Entführung zu beobachten waren, um wieviel stärkere Reaktionen werden nach einem Anschlag zu befürchten sein, dessen Folgen unser Eingangsbeispiel noch bei weitem übertreffen.

Der Staat schließlich wird auf die Negation seines Gewaltmonopols mit einer Demonstration seiner Stärke reagieren. Er muß dokumentieren, daß er fähig und bereit ist, seinen Monopolanspruch zu verteidigen, und in der Lage ist, die Sicherheitsbedürfnisse einer verunsicherten Bevölkerung zu befriedigen. Er wird daher nach einem Anschlag nicht nur instrumentell effektive Maßnahmen ergreifen, um die Situation in den Griff zu bekommen und den Schaden zu begrenzen, sondern auch weit darüber hinaus symbolisch reagieren und durch Fahndungs- und Verhaftungsaktionen oder Gesetzesverschärfungen Entschlossenheit und Härte demonstrieren.[24]

In echten oder vermeintlichen Ausnahmesituationen könnten sich die Verantwortlichen gezwungen sehen, die Grenze der Rechtsordnung zu deren eigenem Schutz zu durchbrechen. Bis dahin noch illegale Aufklärungsmethoden und Überwachungsmaßnahmen dürften dann wie in den 'Fällen' 'Traube', 'Stammheim' und 'Kontaktsperre' mit Hilfe eines ungeschriebenen 'Staatsnotrechts' oder eines 'überverfassungsgesetzlichen

22 Scheerer 120.

23 Steinert 46.

24 S. hierzu z.B. Steinert 45f.; Fetscher 74 ff.; Blankenburg 11 ff.; Roßnagel 1983, 92 ff., 212 ff.

Notstandes'[25] gerechtfertigt werden. Dann wäre "Not kennt kein Gebot" die heimliche Ersatzverfassung des nicht erklärten inneren Notstandes. Über diesen entschieden aber kraft ihres Informationsmonopols allein die Sicherungskräfte. Der Rechtsordnung wären sie nur nach Maßgabe ihrer eigenen Lagebeurteilung unterworfen.

Freiheit oder Sicherheit?

Die aufgeführten Kosten der Sicherung sind in einer dem Trend folgenden Entwicklung recht wahrscheinlich. Sie sind jedoch keineswegs zwingend. Zum einen ist es denkbar, daß sich - wider Erwarten - die Gefährdung weniger bedrohlich entwickelt und dadurch geringere Sicherungskosten verursacht. Zum anderen aber könnte trotz steigender Bedrohung der Preis vielen Bürgern zu hoch sein. Es ist zum Beispiel vorstellbar, daß nicht zu vernachlässigende Gruppen in der Bevölkerung in einem Machtzuwachs der staatlichen und betrieblichen Sicherungskräfte die Gefahr eines Überwachungsstaates sehen. Sie könnten versuchen, zum Schutz von Freiheit und Demokratie auf eine Beschränkung der Kompetenzen und Befugnisse von Polizei und Geheimdiensten hinzuwirken. Ihre Abwehrhaltung gegen Befugnisausweitungen der Sicherheitsbehörden würde durch das Festhalten an dem bisherigen Rechtsverständnis gestärkt. Wer sich im Konfliktfall durchsetzen kann, wird von dem jeweiligen gesellschaftlichen Kräfteverhältnis abhängen.

Diese Entwicklung vermag sich auch auf die prognostizierten Abwägungen des Bundesverfassungsgerichts auszuwirken. Der ergebnisoffene Prozeß der Güterabwägung würde an sich auch Entscheidungen zulassen, die die individuelle Freiheit sichern. Doch erwartet werden können solche Urteile wohl nur in einer anderen Gesellschaft - einer Gesellschaft, in der Sicherheit und Systemrationalität erheblich an Bedeutung verloren haben.

Zum einen müßte die Freiheit des Individuums höher bewertet werden als die Funktionsfähigkeit des gesellschaftlichen Zusammenhangs und seiner Subsysteme. Bisher jedoch begrenzen die Funktionsimperative gesellschaftlicher und staatlicher Institutionen noch immer Inhalt und Reichweite von Grundrechten.[26]

Zum anderen müßte diese Gesellschaft die Freiheitsrechte so hoch schätzen, daß sie dafür auch große Risiken einzugehen bereit wäre. Und sie müßte vor allem einen völlig anderen Sicherheitsbegriff entwickeln. Dazu wäre es notwendig, Abschied zu nehmen von einer technokratischen Sicherheitsproduktion, die Prinzipien des technischen Sicherheitsdenkens auf soziale Phänomene überträgt, indem sie diese in 'Risikofaktoren' aufzuspalten und zu isolieren versucht. Solange aber keine soziale Sicherheit hergestellt ist, die die gesellschaftlichen Ursachen der Bedrohung beseitigt, und dennoch gleichzeitig verwundbare Hochrisikosysteme zu schützen sind, solange dürfte die hier prognostizierte

25 S. hierzu und zur Kritik an diesen Konstruktionen Roßnagel 1984a, 198f. mwN.

26 S. hierzu Roßnagel 1984a, 212 sowie Roßnagel/Wedde/Hammer/Pordesch mwN aus der Rspr. des BVerfG.

Entwicklung auch die wahrscheinlichste bleiben. Ohne eine vollkommene Wende im Sicherheitsdenken aber wird die Waagschale der Freiheit zu leicht bleiben.

Sollte die 'Informationsgesellschaft' tatsächlich einmal den Preis für ihre Sicherheit nicht mehr zahlen wollen, muß sie umgekehrt die Freiheit ihrer Bürger teuer erkaufen. Denn jede unterlassene Sicherungsmaßnahme erhöht ihre Verletzlichkeit. Je abhängiger sie sich von IuK-Techniken gemacht hat, desto schmerzhafter muß sie sich in jedem Einzelfall zwischen Freiheit und Sicherheit entscheiden. Sie kann dann Sicherheit nur noch auf Kosten der Freiheit erreichen und Freiheit nur noch auf Kosten der Sicherheit erhalten.

16. Zehn Thesen zur Verletzlichkeit der 'Informationsgesellschaft'

Als Ergebnis unseres bisherigen Gedankenexperiments wollen wir die Verletzlichkeit einer künftigen 'Informationsgesellschaft' zusammenfassend bewerten. Um noch einmal an die 'Versuchsbedingungen' zu erinnern: Wir haben in unserem Zukunftsbild (Kap. 3 bis 6) versucht, eine im Trend liegende Entwicklung der Gesellschaft zu beschreiben. Darauf aufbauend wurde untersucht, wie sich die beiden Komponenten der Verletzlichkeit, das Ausmaß möglicher Schäden (Kap 7 und 8) und die Wahrscheinlichkeit ihres Eintritts (Kap 9 bis 15), - ebenfalls dem Trend entsprechend - gegenüber heute verändern werden. Vorgestellt wurde also eine Zukunft, die sich mit hoher Wahrscheinlichkeit so ereignen könnte, wenn keine entschiedene und wirksame Gegensteuerung erfolgt. Selbst unter diesen Voraussetzungen wird die künftige Wirklichkeit erheblich vielfältiger und widersprüchlicher sein, als wir dies hier beschreiben konnten. Unsere Untersuchung darf daher nur als Versuch angesehen werden, einen abstrakten Querschnitt durch eine trendmäßige Entwicklung darzustellen. Sie soll nun - als Wahrscheinlichkeitsaussage und mit dem gebotenen Mut zur Zuspitzung - in zehn Thesen zusammengefaßt werden:

1. Die Verletzlichkeit der Gesellschaft wird künftig ansteigen und zu einem zentralen Problem der 'Informationsgesellschaft' werden.

Der wachsenden Bedeutung dieses Problems ist bisher keine gebührende Beachtung geschenkt worden - weder in den Zukunftsplanungen der Entscheidungsträger noch in der öffentlichen Diskussion. Wie sehr die Verletzlichkeit ansteigt, hängt sehr stark ab von politischen Gestaltungsentscheidungen.

2. Die Struktur der Verletzlichkeit wird sich im Tatsächlichen wie im Wissen gegenüber heute verändern.

Während die Chancen steigen, Fehler zu vermeiden und Mißbrauchsaktionen zu verhindern, wird sich das Ausmaß der Schäden für den Fall, daß ein IuK-System dennoch ausfällt oder nicht korrekt funktioniert, deutlich erhöhen. Eine ebenso disparate Entwicklung zeichnet sich für das Wissen über die beiden Faktoren der Verletzlichkeit ab. Während das Ausmaß möglicher Schäden weitgehend bekannt ist, lassen sich viele Faktoren, die die Wahrscheinlichkeit solcher Schäden bestimmen, schwer oder gar nicht einschätzen - etwa Fehlermöglichkeiten in komplexen Systemen, Störungen durch die elektronische 'Umweltverschmutzung', neue Softwareangriffe oder kollektive Aktionen. Soweit die Wahrscheinlichkeit von Schäden unbekannt ist, kann die Verletzlichkeit der Gesellschaft nur nach dem Schadenspotential einer Technikanwendung bewertet werden.

3. Das Sicherungsniveau könnte sehr hoch sein, wird in der Praxis aber deutlich unter den theoretischen Möglichkeiten liegen.

Die IuK-Technik selbst bietet zusammen mit gezielten organisatorischen Maßnahmen theoretisch viele Möglichkeiten, die Verletzlichkeit zu verringern. Wenn für alle schadensträchtigen Anwendungen das jeweils optimale Konzept zur Reduzierung des Schadenspotentials und zur Sicherung gegen Mißbrauch und Versagen des Technik-Systems realisiert würde, wäre ein hohes Schadensniveau trotz zunehmender Nutzung der IuK-Technik zu erreichen. In der breiten Anwendung erfährt jedoch jedes Sicherungskonzept Abstriche durch wirtschaftliche Überlegungen, organisatorische Schwierigkeiten, Interessen der inneren Sicherheit und den Widerstand der von ihm Betroffenen. Die Verläßlichkeit des Sicherungssystems wird folglich immer gefährdet sein, weil es weder das stets fehlerfreie Funktionieren der mit Sicherheitsaufgaben betrauten Personen noch die soziale und politische Stabilität, die es voraussetzt, sicherstellen kann.

4. Die Sicherungssysteme werden sich sehr unterschiedlich entwickeln und immer wieder Lücken aufweisen.

Die begrenzte Wirksamkeit, kontraproduktive Effekte und organisatorische Koordinationsschwierigkeiten von Sicherungsmaßnahmen lassen immer wieder Sicherungslücken entstehen. Während sich Mißbrauchsmotive und Aktionsformen dynamisch entwickeln, ist das Abwehrsystem durch seine technische und organisatorische Verfestigung eher statisch. Es wird immer wieder Angriffen ausgesetzt sein, die neu sind und auf die es nicht vorbereitet ist.

Wenigen gut gesicherten werden viele unzureichend geschützte Anwendungen gegenüberstehen. Viele Sicherungsmaßnahmen dürften sich nur langsam durchsetzen. Neben modernsten Sicherungs- und Sicherheitssystemen werden auch ältere, längst überholte Konzepte zu finden sein. Zwischen den Sicherungssystemen von Großbetrieben oder wichtigen Verwaltungen und denjenigen von Klein- und Mittelbetrieben oder weniger finanzstarken Behörden wird eine große Effektivitätskluft entstehen.

5. Zahl und Intensität der Mißbrauchsmotive nehmen überproportional zu.

Künftig werden nicht nur alle Varianten aus dem breiten Spektrum bisheriger Mißbrauchsmotive entsprechend dem Anstieg von IuK-Anwendungen vermehrt zu finden sein, sondern außerdem zusätzliche spezifisch durch die IuK-Technik hervorgerufene Mißbrauchsmotive entstehen. IuK-Technik wird das wirtschaftliche, gesellschaftliche, politische und private Leben nachhaltig verändern - und dabei nicht allen Menschen lediglich Vorteile bringen. Zerstörung überkommener Lebensformen, wirtschaftlicher Ab-

stieg, berufliche Dequalifizierung, erzwungene Anpassungsleistungen und andere Benachteiligungen bringen neue Mißbrauchsmotive hervor. Zusätzlich zu den bekannten Motiven werden IuK-Systeme auch zu Objekten von Agressionen. Die IuK-Technik bleibt damit nicht - wie bisher - vorrangig Mittel zur Erreichung eines Mißbrauchszwecks, sondern wird künftig auch primäres Ziel von Aktionen.

6. Während die Erfolgswahrscheinlichkeit von Angriffen einzelner Externer erheblich reduziert werden kann, wird es keine ausreichende Sicherheit gegen Mißbrauchsaktionen von Insidern geben. Insbesondere gegen die Angriffsformen des 21. Jahrhunderts sind keine zuverlässigen Sicherungen in Sicht.

Angriffsformen des 19. und 20. Jahrhunderts, wie Bomben- oder Brandanschläge, können durch Sicherungsmaßnahmen erheblich erschwert und durch Ersatzrechenzentren und Sicherungskopien in ihrer Wirksamkeit begrenzt werden. Dadurch werden Zerstörungsaktionen auf weniger gut gesicherte IuK-Systeme abgedrängt. Auch die Chancen für das Eindringen Externer oder nichtprivilegierter Benutzer in ein Computersystem können reduziert werden. Dagegen ist noch nicht abzusehen, wie gegen den Mißbrauch durch privilegierte Insider ausreichende Sicherheit gewährleistet werden könnte, die gerade aufgrund ihrer umfassenden Aufgaben und Funktionen weitreichende Schäden verursachen können. Insbesondere für sie bietet die IuK-Technik neue, effektive Formen der Sabotage und Spionage, des Betrugs und der Untreue. Sie erst hat die Möglichkeit geschaffen, mit Hilfe von Trojanischen Pferden, Viren, Würmern, Falltüren und logischen Bomben die IuK-Technik mit ihren eigenen Mitteln anzugreifen.

Sicherungssysteme sind in der Regel gegen einen, selten gegen mehrere Angreifer konzipiert. Sie setzen das sozialkonforme Verhalten aller übrigen Beteiligten voraus. Schon das Zusammenwirken von zwei Angreifern setzt viele Sicherungsmaßnahmen außer Kraft. Kaum oder keinen Schutz vermögen sie zu bieten, wenn viele Angreifer koordiniert vorgehen oder in gesellschaftlichen Konfliktsituationen ein sozialkonformes Verhalten nicht mehr erwartet werden kann.

7. Komplexe IuK-Systeme sind nicht beherrschbar.

Während gegen Hardwarefehler sowie Software- und Anwendungsfehler in einfach strukturierten Systemen künftig ausreichende Sicherungen möglich erscheinen, muß in komplexen und eng gekoppelten IuK-Systemen immer damit gerechnet werden, daß unerkannte Systemfehler auftreten, die mit anderen Fehlern auf undurchschaubare Weise interagieren und zu einem Systemversagen führen. Komplexe Softwaresysteme können nicht ausreichend getestet und verifiziert werden. Ob sie fehlerfrei sind, bleibt unsicher. Ebenso ungeklärt muß bleiben, ob ihr Modell allen Situationen der Wirklichkeit

angemessen ist. Werden Systeme, von denen zwar bekannt ist, *daß* sie versagen können, jedoch nicht, an welchen Stellen und in welchem Maße, mit hohen Schadenspotentialen verknüpft, entstehen unverantwortbare Hochrisikosysteme.

8. Das Schadenspotential von IuK-Systemen wird deutlich zunehmen. Die Gesellschaft wird in nahezu allen Bereichen vom richtigen Funktionieren dieser Technik-Systeme abhängig sein. Gesamtgesellschaftliche Katastrophen durch den Ausfall wichtiger sozialer Funktionen, die Techniksystemen übertragen wurden, sind nicht auszuschließen.

Die IuK-Technik kann das Schadenspotential von Informationsverarbeitungs- und Kommunikationsprozessen auf spezifische Weise erhöhen. Sie ermöglicht vielfältige schädigende Aktionen und damit Kumulationsschäden. Sie kann zu einer automatischen Vervielfachung eines Schadens und damit zur Verursachung von Multiplikationsschäden genutzt werden. Die Zentralisierung von Daten und Kommunikationsverbindungen kann zu einem hohen Einzelschaden führen. In vernetzten Systemen können sich Schäden in viele angeschlossene Systeme ausbreiten und einen Komplexschaden hervorrufen. Schließlich werden durch standardisierte Software selbst weit verteilte und isolierte Systeme sehr eng gekoppelt und können durch deren Manipulationen sogar allesamt gleichzeitig ausfallen.

Die Abhängigkeit von IuK-Technik und damit das spezifische Schadenspotential wird in dem Maße ansteigen, wie die IuK-Technik bisherige Formen der Informationsverarbeitung und der Kommunikation verdrängt. Sie kann dadurch reduziert werden, daß Substitutionsmöglichkeiten erhalten bleiben. Macht sich die Gesellschaft von einem einzigen Technik-System abhängig und erhält auch keine funktionalen Äquivalente, kann der Ausfall dieses IuK-Systems Katastrophen nationalen Ausmaßes verursachen.

9. Sicherheit der IuK-Technik ist nur auf Kosten von Freiheit und Demokratie möglich, Freiheit und Demokratie können nur auf Kosten der Sicherheit erhalten werden.

Die genannten Schäden müssen unbedingt vermieden werden. Sicherheit ist nicht allein durch technische Maßnahmen herzustellen, sondern setzt Sicherungsstrategien voraus, die gegen Menschen gerichtet sind. Da Angriffe künftig wahrscheinlicher und schadensträchtiger werden und keine Möglichkeit besteht, IuK-Systeme in zugespitzten gesellschaftlichen Konflikten angemessen zu schützen, wird es zum einen notwendig sein, die Sicherungslinie in die Gesellschaft hinein vorzuverlegen. Den Verantwortlichen wird daran gelegen sein, als Risiko definierte Personen oder Entwicklungen vorbeugend in den Griff zu bekommen. Die Technisierung gesellschaftlicher Funktionen (nicht nur, aber auch

durch die IuK-Technik) erfordert immer nachdrücklicher gesellschaftliche Stabilität und Vertrauen in das sozialkonforme Verhalten jedes einzelnen. Diese Aufgabe legitimiert den Einsatz von Überwachungselektronik und wird das Überwachungspotential von Staat und Unternehmen anwachsen lassen - mit allen Risiken für eine sich frei entwickelnde Demokratie. Sicherheit setzt zum anderen die Vertrauenswürdigkeit der Beschäftigten voraus. Diese muß gewährleistet werden durch Überprüfungen, Verhaltensüberwachung und Arbeitskontrollen. Die Sicherung der IuK-Technik ist somit ohne Freiheitseinschränkungen nicht möglich. Und die Bereiche, in denen Freiheitseinschränkungen unumgänglich werden, wachsen mit der IuK-Nutzung.

10. Die 'Informationsgesellschaft' setzt sich einem Sicherungszwang aus, den sie nicht mehr beherrschen kann und dessen Dynamik in sozialunverträgliche politische und soziale Verhältnisse zu führen droht.

Die Stärke des Sicherungszwangs folgt aus dem Schadenspotential und der Bedrohung von IuK-Systemen. Da die Gründe für eine solche Bedrohung zu unterschiedlich und zu komplex sind, um sie politisch zu steuern, bleibt als Instrument zur Regulierung des Sicherungszwangs nur die Beeinflussung der Schadensmöglichkeiten. Macht sich die Gesellschaft jedoch von Hochrisikosystemen abhängig, setzt sie sich dem Dauerzwang zur Ernstfallvermeidung aus. Sie verliert die Fähigkeit, den Sicherungszwang zu beherrschen, da dessen Stärke dann von der nicht beeinflußbaren künftigen Bedrohung bestimmt wird. Steigt diese an, entsteht eine Dynamik immer größerer Sicherungsanstregungen. Sie kann durch einige katastrophale Schäden erheblich beschleunigt werden. Je sicherer die 'Informationsgesellschaft' jedoch wird, desto weniger wird sie dem Bild entsprechen, das sich heute viele von ihr machen: Ihre Verletzlichkeit fordert eine hohe gesellschaftliche Stabilität und erlaubt keine gesellschaftlichen Experimente. Die sichere 'Informationsgesellschaft' ist rigide, geschlossen, unfrei und autoritär.

IV. TECHNIKGESTALTUNG

17. Gestaltungsaufgaben

Die Verletzlichkeit der 'Informationsgesellschaft' ist nicht zu verantworten. Schäden, die von Hochrisikosystemen wie Hochgeschwindigkeitszügen, enggekoppeltem Luft- und Straßenverkehr, hochkomplexen und vernetzten Systemen zur Produktionssteuerung, zur Lenkung der Warenströme und des Zahlungsverkehrs ausgehen können, sind gesellschaftsgefährdend. Die Gesellschaft macht sich von der Zuverlässigkeit und Mißbrauchssicherheit technischer Systeme abhängig, die sie nicht gewährleisten kann. Insbesondere ein softwarevermitteltes Universalnetz ist als alternativloses Kommunikationssystem solange ein untragbares Risiko, wie ein Ausfall mit Katastrophenfolgen nicht sicher ausgeschlossen werden kann.

Das Ausmaß möglicher Schäden steigt, und ihre Wahrscheinlichkeit ist ungewiß. Letzlich bleibt das Gesamtrisiko, das in der 'Informationsgesellschaft' aufgebaut wird, unbekannt - wenn auch zu vermuten ist, daß es erheblich ansteigen wird. Die Folgen tragen jedoch überwiegend diejenigen, die diese hohe Verletzlichkeit nicht zu verantworten haben - entweder in einem katastrophalen Schadensfall oder durch die Bemühungen, die Risiken auf Kosten ihrer Freiheit und demokratischen Teilhabe zu bekämpfen. *Der Weg in die 'Informationsgesellschaft' ist daher nicht sozialverträglich*.

Wie zwingend ist unsere in den vorherigen Kapiteln dargestellte konditionale Prognose? Kann ihre warnende Darstellung sie zu einer sich selbst aufhebenden Prognose machen? Das wäre dann und nur dann der Fall, wenn Mittel verfügbar wären, eine solche Entwicklung zu verhindern, ihr entgegenzusteuern oder sie zumindest zu kompensieren. Aber welche Einflußmöglichkeiten gibt es?

Die steigende Verletzlichkeit der Gesellschaft ist eine der großen Krisenerscheinungen der industriegesellschaftlichen Entwicklung. Die Verletzlichkeit durch schadensträchtige und hochkomplexe informationstechnische Systeme entspringt letztlich dem gleichen Ursachenzusammenhang wie die Risiken, die sich in Bhopal oder Tschernobyl manifestiert haben. Sie werden aus der Effizienzlogik naturwissenschaftlich-technischen Denkens entwickelt, stehen unter einem hohen, vom Weltmarkt diktierten Anwendungsdruck und kommen in der Risikoumgebung hochindustrialisierter Gesellschaften zum Einsatz. Über ihre Anwendung und Ausgestaltung wird zu sehr aus der isolierten Perspektive privater ökonomischer Interessen oder einzelner Verwaltungsbürokratien entschieden. Das Tempo auf dem Weg in die 'Informationsgesellschaft' ist zu hoch, als daß alle Folgen dieser

dynamischen Entwicklung ausreichend bedacht werden könnten.[1] Neben vielen anderen Technikfolgen werden auf diesem Weg in Form hochgradig komplexer und eng gekoppelter sozio-technischer Systeme ungeheure Schadenspotentiale sowie wesentliche Ursachen für die Bedrohung von IuK-Systemen gesetzt.

Eine Lösung des Verletzlichkeitsproblems ist daher nur nach einer umfassenden und tiefgreifenden Neuorientierung der Industriegesellschaft zu erwarten. Solange die Logik industrieller Entwicklung nicht umgekehrt wird, sind die Bestimmungsfaktoren für die steigende Verletzlichkeit nicht aufzuheben. Solange Technikanwendungen durch partikulare Interessen, eine hohe Weltmarktabhängigkeit, eingeschränktes Effizienzdenken und eine rasante Entwicklungsdynamik bestimmt werden, kann die Verletzlichkeit der Gesellschaft nur beschränkt aufgehoben werden.

Ob die Gesellschaft der Herausforderung einer Neuorientierung gerecht wird, ist jedoch nicht abzuschätzen. Gegenwärtig jedenfalls sind hierfür die Weltmarktabhängigkeit zu hoch, die politische Unterstützung zu gering und die geistige Verwurzelung in mechanistischem Denken zu stark. Die Gestaltung der Technik nach dem Kriterium der Verletzlichkeit kann jedoch nicht auf diese gesamtgesellschaftlichen Veränderungen warten, sondern ist bereits unter den bestehenden Verhältnissen notwendig. Auch wenn ohne grundsätzliche gesellschaftliche Umorientierung sich niemand illusionistischen Hoffnungen auf eine widerspruchsfreie Lösung des Verletzlichkeitsproblems hingeben darf, müssen dennoch mindestens zwei Fragen aufgegriffen werden: Wie und wo kann auch unter den gegebenen Verhältnissen Verletzlichkeit verringert werden, wie können deren soziale und politische Kosten reduziert werden? Welches sind die ersten Schritte in die richtige Richtung auf das langfristige Ziel einer gesellschaftlichen Umorientierung hin?

Wir haben gesehen, daß IuK-Technik je nach Entwicklungs- und Anwendungsbedingungen Verletzlichkeit ebenso reduzieren wie auch erhöhen kann. Diese Erkenntnis verleitet zu der Vermutung, daß die Verletzlichkeit der Gesellschaft beeinflußt werden kann, wenn es gelingt, diese Bedingungen unter gesellschaftliche Kontrolle zu bekommen und unter anderen nach dem Kriterium der Verletzlichkeit zu steuern. Gestaltung der IuK-Systeme nach gesamtgesellschaftlichen Kriterien, nicht mehr nur nach beschränkten partikularen Interessen, könnte die Verletzlichkeit der 'Informationsgesellschaft' möglicherweise so sehr reduzieren, das die verbleibenden Risiken vertretbar sind.

Wie aber können die technische Entwicklung gesteuert und technische Systeme gestaltet werden? Sollen diese Bemühungen effektiv sein, ist eine staatliche Kontrolle der Technikentwicklung und -nutzung erforderlich. Sie muß durch betriebliche Mitbestimmung und gesellschaftliche Partizipation ergänzt, kann aber nicht durch diese ersetzt werden. Für gruppenübergreifende Allgemeinrisiken ist im "Dschungel der korporatistischen Gesellschaft" kein Platz.[2] Allenfalls eine eigenständige, demokratisch kontrollierte Institution

1 S. hierzu auch Lenk 331; Lutterbeck 1985, 22.

2 Beck 64.

könnte versuchen, das Allgemeininteresse an einer geringen Verletzlichkeit der Gesellschaft auch gegenüber Partikularinteressen durchzusetzen.

Sind also zusätzliche staatliche Kontrolle und eine weitere Machtsteigerung staatlicher Bürokratie die Patentlösung des Verletzlichkeitsproblems? Kann das Risiko großer Schäden und Katastrophen nur beseitigt werden, indem staatliche Organe zusätzliche Eingriffsbefugnisse erhalten? In der Tat könnte sich herausstellen, daß Technikgestaltung ohne Kontrolle und Regulierung nicht möglich ist. Andererseits ist aber ohne soziale Gestaltung die künftige Nutzung der IuK-Technik nicht zu verantworten. Es wäre also möglich, daß unter den gegebenen Verhältnissen keine Ideallösung zu finden ist. Gesucht werden kann nur nach Vorschlägen, Technikgestaltung möglichst effektiv zu organisieren und gleichzeitig staatliche Machtsteigerung zu begrenzen. Die strukturellen Bedingungen für die Nutzung der IuK-Technik könnten etwa so verändert werden, daß in manchen Aspekten Kontrolle überflüssig wird. Dennoch notwendige Überwachungs- und Regulierungsmaßnahmen wären demokratisch zu kontrollieren.

Technikgestaltung, die erst erfolgt, wenn ein Technik-System bereits entwickelt ist und seine Anwendung bevorsteht, kann zu spät kommen. Wenn in das Technik-System bereits investiert wurde, läuft staatliche Techniksteuerung Gefahr, an den bereits formierten Interessen zu scheitern. Je früher in dem Entwicklungsprozeß einer Technik sie einsetzt, umso größer ist ihr Gestaltungsspielraum.

Ohne jede Erfahrung mit einem Technik-System wird aber jeder Versuch, es zu gestalten, zu einem politischen Experiment, dessen Ergebnis ungewiß ist. Greift die Politik regelnd in die technische Forschung und Entwicklung ein, muß sie in Kauf nehmen, auch eine sinnvolle technische Fortentwicklung zu hemmen. Außerdem muß sie damit rechnen, an der künftigen Wirklichkeit vorbei zu entscheiden, da die Wirkungen der Technik nur ungenau vorherzusagen sind.[3] Die Alternative, nichts zu tun und problematische Entwicklungen abzuwarten, ist jedoch noch riskanter. Denn die Verletzlichkeit nimmt zu und es entsteht ein ernst zu nehmendes Risiko gesellschaftlicher Katastrophen. Ist ein Sicherungszwang erst einmal entstanden, kann er nur noch vollzogen werden. Politik steht dann unter dem Imperativ der Katastrophenprävention.

Die Ungewißheit, die mit der Gestaltungsalternative verbunden ist, kann zwar nicht aufgehoben, aber doch stark reduziert werden. Andere Technik-Systeme wie atomtechnische oder wasser- und luftverunreinigende Anlagen, Kraftfahrzeuge und Maschinen unterliegen bereits staatlicher Kontrolle. Und auch der IuK-Technik gelten schon heute staatliche Gestaltungsanforderungen, soweit mit ihrer Hilfe personenbezogene Daten verarbeitet werden. Es gibt also bereits Erfahrungen, mit welchen Vollzugsproblemen und Regelungsdefiziten Techniksteuerung zu kämpfen hat.[4] Auch wenn IuK-Systeme sich von diesen 'alten' Techniken durch die Universalität ihres Verwendungszwecks und durch ihre ubiquitäre Verfügbarkeit durch vernetzte Strukturen unterscheiden, müssen Gestal-

3 S. hierzu Lutterbeck 1985, 31.

4 S. hierzu auch näher Roßnagel UPR 1986, 46 ff.

tungsversuche nicht bei 'Null' beginnen, sondern können aus der Geschichte der Technikkontrolle lernen. Schließlich wollen auch Studien wie die vorliegende die Handlungsvoraussetzungen aller, die an Technikgestaltung interessiert sind, verbessern.

Wenn einerseits also Gestaltung notwendig und möglich ist, so muß andererseits ihre Reichweite doch begrenzt bleiben. Zum einen ist die Wirklichkeit viel zu komplex, als daß sie einer planvollen Konstruktion nach Kriterien der Sozialverträglichkeit zugänglich wäre. Zum anderen bleibt das Wissen, das wir über die Zukunft haben können, stets hinter dem zurück, das wir haben müßten, um konstruierend zu gestalten. Die Durchsetzung der sozialen und technischen Voraussetzungen der 'Informationsgesellschaft' wird ein sehr langwieriger und komplexer Prozeß sein. Niemand kann heute die künftigen technischen Nutzungsmöglichkeiten oder Anwendungsformen der IuK-Technik und damit erst recht deren gesellschaftliche Auswirkungen sicher vorhersagen.[5] Ihre Konturen werden erst im Laufe der Zeit erkannt und bewertet werden können. Angesichts dieser verbleibenden Ungewißheit und der großen Verletzlichkeitsgefahren IuK-technischer Entwicklung muß Technikgestaltung vor allem darauf achten, daß wir die Randbedingungen für eine nichtkatastrophische Entwicklung günstig gestalten.[6]

Gefordert ist daher weniger eine bewirkende und vorwärtstreibende als vielmehr eine präventiv bewahrende Gestaltung sozio-technischer Systeme. Vor allem müssen wir die Lernfähigkeit der Gesellschaft erhalten. Die künftigen Strukturen und Formen der 'Informationsgesellschaft' werden in langwierigen und weitverzweigten Entscheidungsprozessen gestaltet. In diesen kann die Ungewißheit über die Folgen der Techniknutzung im Zeitablauf nur nach und nach aufgehoben werden. Die Entscheidungsstrukturen müssen daher so gestaltet werden, daß die Gesellschaft aus der Entwicklung lernen und diese jederzeit korrigieren kann. Technikgestaltung hat daher vorrangig darauf zu achten, daß die Zukunft offenbleibt und Entscheidungen rückgängig gemacht werden können. Sie muß versuchen, die Abhängigkeit von IuK-Technik zu verringern und Substitutionsalternativen zu erhalten. Schließlich muß sie darauf zielen, das Schadenspotential einzelner Technikanwendungen zu verringern und damit den Sicherungszwang der IuK-Technik zu beseitigen.[7]

Die in den vorherigen Kapiteln beschriebene Entwicklung zu einer verletzlichen Gesellschaft ist keineswegs unausweichlich, sondern nur dann wahrscheinlich, wenn keine Gegenstrategien eingeleitet werden. Die IuK-Technik ist wie keine andere Technik gestaltungsfähig und gestaltungsbedürftig. Viele ihrer Verwendungsmöglichkeiten würden es auch erlauben, die Verletzlichkeit der Gesellschaft erheblich zu reduzieren. Es geht daher nicht wie bei der Atomtechnik um ein 'Ja' oder 'Nein', sondern um ein 'So' oder 'Anders' für jede einzelne Entwicklungslinie.[8] Allerdings dürfen sich solche Gestaltungsversuche

5 S. hierzu näher Kubicek CM 10/1986, 28 ff.

6 S. Guggenberger 141f.

7 S. hierzu auch Lutterbeck 1985, 37; Roßnagel/Wedde DVBl 1988, 570f.

8 S. hierzu auch Kubicek 1988, 93; Lutterbeck 1987,54; Steinmüller 1986, 71 ff.

nicht auf das technische System als solches beschränken, sondern müssen darauf abzielen, das gesamte sozio-technische System, in dem die Technik ihre Anwendung findet, einzubeziehen.

Technikgestaltung setzt voraus, zwischen mehreren sozio-technischen Alternativen wählen zu können. Sie ist darauf angewiesen, daß ihr keine einspurigen Problemlösungen, sondern ein breites Spektrum von Gestaltungsmöglichkeiten geboten werden, die nach ihrer Verletzlichkeit vergleichend bewertet werden können. Die Anstrengungen müssen darauf gerichtet sein, historische Verzweigungssituationen für die weitere technische Entwicklung im jeweiligen Anwendungbereich zu erkennen. Dabei ist immer auch zu berücksichtigen, soziale Funktionen nicht auf die Technik zu übertragen, sondern im gesellschaftlichen Raum zu belassen. Alternativen sind auf allen Ebenen zu suchen - von der konkreten Ausgestaltung eines Arbeitsplatzes bis hin zum gesellschaftspolitischen Entwurf. Wir wollen hierzu beitragen, indem wir im folgenden Kapitel am Beispiel von vier 'Optionen der Telekommunikation' und von zwei Entwicklungsmöglichkeiten zur 'Zukunft der Arbeit' untersuchen, welche Alternativen in gesamtgesellschaftlicher Perspektive für die Technikgestaltung bestehen und wie in diesen die Verletzlichkeit der Gesellschaft zu bewerten ist. Danach greifen wir die Ergebnisse unsere Verletzlichkeitsanalyse auf und entwickeln daraus konkrete Empfehlungen, IuK-Systeme und ihr Anwendungsumfeld so zu gestalten, daß die Verletzlichkeit reduziert wird. Schließlich erörtern wir im letzten Kapitel, welche politischen Voraussetzungen notwendig wären, um IuK-Technik nach dem Kriterium der Verletzlichkeit verantwortlich zu steuern.

18. Die Verletzlichkeit von Entwicklungsalternativen

Da unter der Annahme, daß sich die gegenwärtigen Entwicklungstrends fortsetzen, die Verletzlichkeit der Gesellschaft ansteigen wird, stellt sich die Frage nach möglichen Entwicklungsalternativen - und deren Verletzlichkeit. Leider ist die Diskussion über alternative Zukunftsentwürfe noch nicht so weit fortgeschritten, daß sich deutliche systemare alternative 'Pfade' für die gesamtgesellschaftliche Entwicklung abzeichneten. In einzelnen Bereichen ist die Diskussion um Alternativen jedoch bereits eröffnet. In zwei dieser 'Arenen': in die Diskussion um die künftige Infrastruktur der Telekommunikation und in die Debatte um die Zukunft der Industriearbeit, wollen wir uns kurz begeben. Dabei verfolgt dieses Kapitel zwei Ziele. Zum einen will es exemplarisch zeigen, daß nicht nur die bisher beschriebene Trendentwicklung möglich ist, sondern daß unterschiedliche Entwicklungszukünfte möglich sind. Zum anderen soll dargestellt werden, daß die Gesellschaft unterschiedlich verletzlich werden kann, je nachdem für welche der Zukunftsentwürfe sie sich entscheidet. Die untersuchten Alternativen können hier allerdings nur knapp hinsichtlich einiger weniger Strukturmerkmale dargestellt und nach einigen Aspekten der Verletzlichkeit, nämlich der Entwicklung von Mißbrauchsmotiven, Angriffsformen, Sicherungsmöglichkeiten und Schadenspotentialen, befragt werden. Die hierbei gefundenen Ergebnisse sind keine abschließende Bewertung der Alternativen, sondern sollen lediglich die Diskussion über sie anregen.

Optionen der Telekommunikation

An den Plänen der Deutschen Bundespost, die Infrastruktur für die Telekommunikation auszubauen, wird von allen politischen Seiten Kritik geübt. Diese bleibt jedoch meist partiell und wird selten bis hin zu einem Alternativkonzept weitergedacht. Hier hat das Forschungsprojekt "Optionen der Telekommunikation" angesetzt. Es hat die unterschiedlichen Kritikpunkte aufgenommen und zu vier idealtypischen Zukunftsoptionen gebündelt.[1] Diese Wunschvorstellungen werden im folgenden auf ihren spezifischen positiven oder negativen Beitrag zur Verletzlichkeit der Gesellschaft hin geprüft. Die vergleichende Betrachtung nimmt den Endzustand der Optionen um das Jahr 2020 in den Blick und wählt als Vergleichsmaßstab die für unser Zukunftsbild festgestellten Ergebnisse.

1. Die reine '*Postoption*' entspricht den bisherigen langfristigen Vorstellungen der Deutschen Bundespost. In ihr haben technische Innovationen und wirtschaftliches Wachstum hohe Priorität. Sie unterscheidet sich von unserem Zukunftsbild hauptsächlich dadurch, daß in ihr der Staat im Bereich Telekommunikation stärker engagiert bleibt, die

1 S. Berger u.a. III, 1 ff.; zur Verletzlichkeit dieser Optionen näher Pordesch Arbeitspapier 6.

Entwicklung wesentlich von der Bundespost bestimmt und als Endstufe eine Integration aller Kommunikationsarten in einem einzigen Glasfaseruniversalnetz erreicht wird.

Die Telekommunikationspolitik wird von der Leitvorstellung geprägt, durch das Angebot modernster Telekommunikation die technische Innovation und das wirtschaftliche Wachstum zu unterstützen. Hierfür soll die Post unabhängig von der Nachfrage 'Hebammendienste' leisten. Öffentliche Massendienste sollen rasch standardisiert und breit angeboten werden. Ein flächendeckendes Universalnetz für die Übertragung von Sprache, Texten, Daten und bewegten Bildern wird deshalb zügig ausgebaut. Um hierfür die Investitionsmittel aufbringen zu können, bleibt die Post ungeteilt und behält ihr Fernmeldemonopol.

Das 'endgültige' Universalnetz beruht auf Glasfaserleitungen und einheitlichen Breitbandvermittlungsstellen für alle Formen der Telekommunikation. Eine einheitliche IBFN-Software steuert das Breitbandkoppelnetz und die Vermittlungsleistungen. Rundfunk und Fernsehen werden über eine Empfangsstelle für Satellitensignale in den einzelnen Vermittlungsstellen in dieses Netz eingespeist. Irgendwann nach 2020 sind alle Haushalte an das Glasfasernetz angeschlossen. Telepost wird dann die Briefpost im geschäftlichen wie im privaten Bereich fast völlig verdrängen. Bildschirmtext wird zu einem interaktiven Videosystem weiterentwickelt. In allen Haushalten und Unternehmen setzt es sich als das zentrale Medium durch, um Zahlungen zu tätigen, Waren zu bestellen, Informationen abzufragen und sonstige standardisierte Vorgänge abzuwickeln. Wo im Kontakt mit Behörden, Ärzten, Rechtsanwälten, Steuerberatern oder sonstigen Anbietern von Dienstleistungen noch ergänzende persönliche Gespräche erforderlich sind, werden diese überwiegend über Bildfernsprechen geführt.[2]

Einige Aspekte der Verletzlichkeit könnten sich in dieser Option positiv entwickeln. Von der Größe her wäre die Bundespost in der Lage, aufwendige Reserveeinrichtungen bereitzustellen und damit begrenzte Ausfälle relativ kurzfristig zu ersetzen. Das staatliche Monopol könnte eine gleichmäßige Versorgung gewährleisten und einen sozialen Ausgleich in der Nutzung von Telekommunikationsdiensten erlauben. Möglicherweise würden dadurch einige politisch motivierte Angriffe unterbleiben. Mit Hilfe von TeleTrusT könnten die Kommunikationsbeziehungen und mit einem von der Bundespost angebotenen standardisierten Verschlüsselungsverfahren auch die Kommunikationsinhalte gegen Ausforschung geschützt werden. Allerdings dürften in einer so etatistisch geprägten Zukunft die Behörden der inneren Sicherheit solche Schutzmaßnahmen verhindern.

Andererseits wird jedoch die Gesellschaft durch die Integration aller Telekommunikation in einem Mega-System vom Funktionieren dieses einzigen Kommunikationsnetzes völlig abhängig. Unternehmen, Behörden und Haushalte, alle von den technischen Möglichkeiten fasziniert, nutzen die angebotenen Dienste. Alternative 'altmodische' Kommunikationsmöglichkeiten werden vernachlässigt. Schon lokale Ausfälle würden unter diesen

2 S. hierzu näher Berger u.a. III, 17 ff.

Bedingungen größere Schäden nach sich ziehen als in unserem Eingangsbeispiel beschrieben sind.

Ein softwareinduzierter Zusammenbruch wäre eine nicht mehr beherrschbare Katastrophe, weil auch die Notfallmaßnahmen nur über Telekommunikation organisiert werden könnten. Die hohe Abhängigkeit erschwert auch effektive Improvisationen. Jede Art der Kommunikation außerhalb der Rufweite wäre ausgeschlossen und nicht ersetzbar. In der Folge wären alle gesellschaftlichen Subsysteme funktionsunfähig. Nach kurzer Zeit könnte nichts mehr produziert, transportiert, verkauft werden. Die total-integrierte Telegesellschaft würde mit einem Schlag in einen vorindustriellen Zustand zurückversetzt. Ob in einer solchen Situation, in der auf nichts mehr Verlaß ist, zivilisierte Verkehrsformen erhalten bleiben, ist mehr als fraglich.

Das Verletzlichkeitsrisiko der Gesellschaft durch Angriffe gegen ein solches Universalnetz dürfte im Vergleich zu anderen Optionen größer sein. Zum einen verspricht ein Angriff einen größeren Erfolg. Zum anderen würde es als die zentrale Struktur, die die gesellschaftlichen Bedingungen der 'Informationsgesellschaft' konstituiert, zum herausragenden Angriffsobjekt für die militanten Gegner dieses Gesellschaftssystems.

2. In der '*Wettbewerbsoption*' haben technische Innovation und wirtschaftliches Wachstum eine hohe Priorität. Sie erfordern ein Zurückschneiden staatlicher Telekommunikationspolitik auf eine dienende Funktion für die privatwirtschaftlichen Wettbewerber. Diese Option will durch eine weitgehende Deregulierung Marktkräfte freisetzen. Das Fernmeldemonopol wird daher aufgehoben, die Bundespost aufgeteilt und privaten Unternehmen erlaubt, Telekommunikationsnetze[3] und -dienste anzubieten. In der Folge entstehen viele spezielle Netze und Dienste. Private Betreiber unterhalten Mobilfunksysteme, Richtfunkstrecken, lokale Kabelnetze, Fernverbindungsnetze bis hin zu Satellitensystemen. Der Ausbau der Netze und Dienste folgt der Gewinnorientierung ihrer Anbieter. Lukrative Strecken, Gebiete und Dienste sind sehr gut versorgt. In diesen herrscht reger Wettbewerb. Weniger Gewinn versprechende Regionen oder Dienste werden vernachlässigt.

Die staatliche TELEKOM ist nur noch ein Anbieter unter mehreren. Durch die Konkurrenz mit privaten Anbietern kann sie die Investitionen für ein Universalnetz nicht mehr aufbringen. Sie unterhält vor allem noch ein weitgehend flächendeckendes modernisiertes Fernsprechnetz mit ISDN-Standard als Zubringer zu den privaten Netzen.

Für den Geschäftsverkehr sinken die Kosten der Telekommunikation. Die Unternehmen nutzen daher die angebotenen Dienste ausgiebig. Auch die privaten Haushalte haben trotz Gebührensteigerungen Teletransaktionen als Form akzeptiert, mit Unternehmen, Behörden und sonstigen Institutionen zu verkehren.[4]

---

3 Private Netzbetreiber sind in der 'Wettbewerbsoption' von Berger u.a. III, 30 nicht vorgesehen. Wir wollen hier jedoch die Folgen einer konsequenten Liberalisierung für die Verletzlichkeit der Gesellschaft erörtern.

4 S. hierzu Berger u.a. III, 26 ff.

Zwar sinkt in dieser Alternative das Schadenspotential. Ein völliger Ausfall der Telekommunikation wäre ausgeschlossen. Verschiedene Netzbetreiber dürften je nach ihren speziellen Bedürfnissen unterschiedliche Systeme einsetzen. Allerdings können nur einige wenige Großunternehmen Vermittlungstechnik anbieten, da nur sie die extrem hohen Kosten für deren Erforschung und Entwicklung aufzubringen vermögen. Der Ausfall eines dieser Systeme in einem oder mehreren Netzen würde immer noch einen kaum zu verkraftenden Schaden verursachen.

Durch die Verteilung der Telekommunikation auf verschiedene Anbieter sinkt aber nicht nur das Schadenspotential, sondern auch deren Zuverlässigkeit. Schon allein die Komplexität des Gesamtsystems wird häufiger zu Betriebsstörungen führen sowie auch mehr Angriffsobjekte und mehr Mißbrauchsmöglichkeiten bieten. Aufwendige Maßnahmen zur Schadensvermeidung und Schadensbegrenzung sind für die privaten Betreiber nicht lukrativ. Redundanz, Vermaschung, Diversifikation von Systemen oder Netznotbetrieb werden sie nur dann vorsehen, wenn es sich kurzfristig auszahlt. Verschlüsselungsstandards werden sich folglich auch nicht durchsetzen. Gegen besondere Bezahlung werden jedoch Dienste mit Nachrichtenverschlüsselung nach betreiberspezifischen Verschlüsselungsverfahren angeboten. Es ist daher mit einigen wenigen teuren Netzen und Diensten zu rechnen, die für sehr sensitive Geschäfts- oder Behördenkommunikation angeboten werden. Insgesamt dürfte das Sicherungsniveau deutlich niedriger sein als in unserem Zukunftsbild.

In dieser Alternative dürfte auch das Risiko politisch motivierter Angriffe sinken, da die vielen einzelnen Netze und Dienste nicht so sehr im Vordergrund gesellschaftlicher Konflikte stehen. Andererseits wird eine von Wettbewerb geprägte Gesellschaft sozial tief gespalten sein.[5] Die hohe materielle Sicherung der Mehrheit wird ständig konfrontiert mit der Not einer starken Minderheit. Vor allem bei denen, die als Verlierer der technischen Innovation in diese Minderheit abzurutschen drohen, könnten Streß und Aggressionen zu Aktionen gegen IuK-Systeme motivieren.

Die Netz- und Dienstbetreiber wären faktisch nicht mehr zu kontrollieren. Das Risiko, daß Verbindungs- und Inhaltsdaten der Teilnehmer ausgewertet, verkauft und für Marketingstrategien oder andere Zwecke genutzt werden, steigt daher beträchtlich an. Jedenfalls wären das Fernmeldegeheimnis und der Datenschutz bei privaten, gewinnorientierten Anbietern weniger gut aufgehoben als bei einer staatlichen, dem Allgemeinwohl verpflichteten Institution. Das Hauptproblem dieser Option dürfte jedoch darin liegen, daß es keine Instanz und keine Instrumente mehr gibt, um die Entwicklung der Telekommunikation zu kontrollieren, ihr Sicherungsniveau zu steuern und die Verletzlichkeit der Gesellschaft zu beeinflussen.

3. Die '*sozialtechnokratische Option*' sieht den gesellschaftlichen Nutzen der IuK-Technik als umso größer an, je massenhafter deren Anwendung erfolgt. Der Staat über-

5 S. Berger u.a. III, 33 f.

nimmt die Rolle des Innovationsmotors. Er stellt sich die Aufgabe, eine größtmögliche Akzeptanz in der Bevölkerung für die Technik herzustellen. Aus diesem Grund werden an den Brennpunkten der Kritik Maßnahmen ergriffen, um eine größere Sozialverträglichkeit sicherzustellen. Bedenken des Datenschutzes werden bei den neuen Netzen und Diensten durch eine aufwendigere Netztechnik ausgeräumt. Einem Anstieg der Arbeitslosigkeit wird durch Umverteilung der Arbeit entgegengewirkt. Diese Strategie trägt zu einer rascheren Diffusion der Technik gerade auch in den Haushalten bei und stärkt dadurch die Nachfrage auf dem Binnenmarkt.[6]

Diese Option erstrebt als Infrastruktur ein programmvermitteltes, digitales Telekommunikationsnetz für alle schmalbandigen Nachrichtenformen, das aber datengeschützt und anonym betrieben wird. Diese beiden Anforderungen werden dadurch gewährleistet, daß ein Mißbrauch technisch unmöglich gemacht wird.[7]

Um einen solchen technischen Datenschutz sicherzustellen, bleibt das Fernmeldemonopol erhalten. Europaweit werden Verschlüsselungsstandards durchgesetzt und veröffentlicht. Der Widerstand der Behörden der inneren Sicherheit gegen den technischen Ausschluß von Abhörmöglichkeiten ist überwunden. Die Risiken, daß das organisierte Verbrechen sowie ausländische Agenten das anonyme Netz am meisten begrüßen, werden zur Sicherung des Datenschutzes in Kauf genommen. Dabei herrscht die Überzeugung vor, daß Verbrecher- und Agentenringe in anderen Netzen andere Wege finden würden, ihre geheime Kommunikation zu verschlüsseln. Als Ersatz nutzen Polizei und Geheimdienste verstärkt 'geheimdienstliche Mittel' wie Richtmikrophone oder 'Wanzen'.[8]

Um diese Absichten zu verwirklichen, werden in einem zweistufigen Verfahren zunächst eine Verschlüsselung der Kommunikationsinhalte und der Kommunikationsbeziehungen realisiert und in einem zweiten Schritt sogar die Tatsache des Sendens und Empfangens vor jeder Abhörmöglichkeit geschützt. In der ersten Stufe werden alle vorhandenen Telekommunikationseinrichtungen weiter genutzt. Lediglich die Vermittlungsstellen, die ohnehin auf digitale Technik umgerüstet werden, sollen datenschutzgerecht erneuert werden. In jeden Anschluß wird ein Mikroprozessor zur Verschlüsselung der Nutzungsdaten und der Verbindungsdaten eingebaut. In den Vermittlungsstellen, bei den Kommunen und bei einer dritten öffentlich-rechtlichen Institution (z. B. Industrie- und Handelskammer) werden spezielle Computer (MIXe) als besondere Netzstationen eingebaut.[9] Diese MIXe verschlüsseln die abgesandten Nachrichten erneut und senden sie in

6 S. Berger u.a. III, 35 ff.

7 Das Datenschutzkonzept dieser Option wird hier ergänzt um neuere Konzeptionen einer Karlsruher Forschungsgruppe zur technischen Gewährleistung des Datenschutzes in Netzen - s. z.B. Pfitzmann DuD 1986, 353 ff; Pfitzmann/Pfitzmann/Waidner DuD 1986, 178 ff.; Pfitzmann/Waidner/Pfitzmann CR 1987, 712 ff., 796 ff., 898 ff.; Waidner/Pfitzmann/Pfitzmann DuD 1987, 293 ff.; Waidner/Pfitzmann DuD 1986, 16 ff.; Pfitzmann/Pfitzmann/Waidner, Informatik Spektrum 1988, 118 ff.

8 S. z.B. Pfitzmann/Pfitzmann/Waidner, Informatik Spektrum 1988, 123.; Waidner/Pfitzmann/Pfitzmann DuD 1987, 294.

9 Pfitzmann/Pfitzmann/Waidner, Informatik Spektrum 1988, 136 sehen als Betreiber der Mixe auch Kirchen oder Parteien vor.

zufälliger Reihenfolge an die nächste MIXe. In einer MIX-Kaskade von zwei oder mehr MIXen gelangt die Nachricht zum Empfänger, ohne daß festgestellt werden könnte, welchen Weg sie genommen hat. Die Verkehrsbeziehungen könnten nur noch aufgedeckt werden, wenn alle MIXen zusammenarbeiten.[10] Um dies weitgehend auszuschließen, werden die MIXen auf verschiedene, kontrollierbare Betreiber verteilt. Das Fernmeldemonopol wird insoweit modifiziert.

In einem zweiten Schritt wird dieses Konzept dadurch ergänzt, daß im Zuge der Glasfaserverkabelung im Teilnehmeranschlußbereich ringförmige Verteilnetze für bis zu 10 000 Teilnehmer verlegt werden. Innerhalb der Ringnetze werden alle Kommunikationsinhalte verschlüsselt unterschiedslos an alle Teilnehmer verteilt. Nur der vorgesehene Adressat jedoch kann die Nachrichteninhalte zur Kenntnis nehmen. Dadurch wird auch das Senden und Empfangen vor Kenntnisnahme geschützt. Obwohl in diesem Konzept ein Vielfaches an Kommunikationsleistung gefordert wird, können wegen der hohen Übertragungsrate des breitbandige Glasfasernetzes und seiner Vermittlungssysteme alle die Dienste angeboten werden, die in einem schmalbandigen Netz realisiert werden können. Bewegtbildübertragung erfolgt in diesem Konzept vor allem über direktstrahlende Satelliten. Soweit es in diesem anonymen Netz zur Rechtssicherheit von Teletransaktionen notwendig ist, können sich die Beteiligten mit Hilfe von TeleTrusT gegenseitig identifizieren.[11]

In dieser Option würde die Verletzlichkeit der einzelnen Telekommunikations-Teilnehmer verringert, das Abhören und Auswerten von Verbindungsdaten wäre ausgeschlossen. Da sehr viele Lebensäußerungen telekommunikativ erfolgen, ist die Sicherheit vor einer Kommunikations- und Verhaltensüberwachung ein großer Fortschritt. Transparent könnte die Kommunikation eines Teilnehmers nur dann werden, wenn es gelingt, in seinen Netzabschluß ein Trojanischen Pferd zu installieren, das diese Informationen speichert und weitergibt. Die höhere Akzeptanz der Techniknutzung würde zugleich die Angriffsflächen für politische Konflikte verringern und die Wahrscheinlichkeit politisch motivierter Angriffe gegen die Infrastruktur als solche reduzieren.

Allerdings birgt diese Konzeption auch eine Reihe spezifischer Risiken. Fällt ein MIX aus, gehen alle Nachrichten, die über ihn laufen, verloren. Fällt eine Station im Ring-Netz aus, kann in diesem überhaupt nicht mehr kommuniziert werden. Deshalb wurden umfangreiche Maßnahmen zur Erhöhung der Fehlertoleranz, zum Erkennen fehlerhafter Systemkomponenten oder aktiver Angreifer zur Herstellung von Redundanz und Vermaschung erwogen.[12] Je komplexer jedoch die Maßnahmen zur Erhöhung der Fehlertoleranz werden, desto größer wird die Gefahr, daß Manipulationen der Netzsoftware nicht entdeckt werden können. Außerdem macht die Vermaschung des Ringnetzes zur Erhö-

10 S. hierzu näher Chaum, CACM 1981, 84 ff.; Pfitzmann/Pfitzmann/Waidner Informatik Spektrum 1988, 130 ff., 135 ff.

11 S. hierzu z.B. Pfitzmann/Pfitzmann/Waidner Informatik Spektrum 1988, 134, 137; Abel/Schmölz 159f.

12 S. hierzu Pfitzmann/Mann DuD 1987, 393 ff.

hung der Sicherheit diese Konzeption um ein Vielfaches teurer.[13] In der unter ökonomischen Gesichtspunkten realisierbaren Version verbleibt ein erhebliches Restrisiko gegen physische und logische Angriffe. Schließlich sei noch einmal daran erinnert, daß alle Verschlüsselungsverfahren auf unbewiesene und nur nach Kräften validierte Annahmen aufbauen, daß die Faktorisierung großer Zahlen auch künftig ein praktisch unlösbares Problem bleiben wird. Neue mathematische Algorithmen könnten all den darauf aufbauenden Sicherungsmaßnahmen die Grundlage entziehen.

Da nicht mehr kontrolliert werden kann, wer mit wem kommuniziert und was sich beide zu sagen haben, könnten kriminelle Aktionen, die sich der Telekommunikation bedienen, zunehmen. Denn das Risiko, daß eine betrügerische Transaktion, die Übermittlung eines Betriebs- oder Staatsgeheimnisses, die Verabredung zu einem Verbrechen oder die Anstiftung eines Medienreferenten zu einer ehrenrührigen Straftat jemals erkannt werden könnten, ist sehr gering.

Die hohe Sicherheit des Datenschutzes führt zu einer verbreiteten Nutzung von Telekommunikationsangeboten. Die 'gelbe' Post wird durch elektronischen 'Briefverkehr' nach und nach ersetzt. Sie könnte nicht mehr als Ersatzsystem für den Kommunkationsbedarf der Gesellschaft fungieren. Deren Abhängigkeit vom Funktionieren des Mega-Systems Telekommunikation ist ähnlich hoch wie in der Postoption. Und wie in dem dort angestrebten Universalnetz kann ein Ausfall des gesamten Basisnetzes durch gezielte Softwarefehler nicht ausgeschlossen werden.[14] Wegen der einfacheren Netzsoftware könnte eine Manipulation aber wohl eher entdeckt werden.

4. Die '*Technikbegrenzungsoption*' greift die Sorge aus Teilen der Bevölkerung vor den Gefahren großtechnologischer Projekte auf. Sie verfolgt als vordringliches Ziel, die Entwicklung zur 'Informationsgesellschaft' technisch, politisch und sozial beherrschbar zu machen. Daher bleibt das Fernmeldemonopol ebenso erhalten wie die Einheit der Bundespost. Jedoch wird diese demokratisiert.

Eine hohe Integration von Telekommunikationsdiensten ist dabei nicht vorgesehen. Statt dessen wird zum einen das Telefonnetz zu einem sprachoptimierten Netz mit anonymer programmgesteuerter Vermittlungstechnik ausgebaut. Im Anschlußbereich bleibt die Übertragungstechnik analog. Telefonverbindungen werden auf der Ortsebene ebenfalls wie bisher schrittweise durchgeschaltet. Die Vermittlungstechnik ist digital, erfolgt aber nicht über Softwareprogramme, sondern über monofunktionale Hardware-Bausteine. Nur auf der Fernebene werden die Vermittlungsstellen programmgesteuert. So fallen nirgendwo im Netz teilnehmerbezogene Gebührendaten an.

Zum anderen wird das Integrierte Datennetz für die Geschäftskommunikation zu einem Integrierten Professionellen Netz (IPN) mit einer identifizierenden Vermittlungstechnik ausgebaut. Datensicherheit wird durch Ende-zu-Ende-Verschlüsselung realisiert.

13 Allerdings wäre zu prüfen, ob eine ähnliche Sicherheit gewährleistende Version der 'Postoption' oder der 'Liberalisierungsoption' geringere Kosten verursachen würden.

14 Wegen der einfacheren Netzsoftware könnte eine Manipulation aber wohl eher entdeckt werden.

Zwischen den Fernebenen des Fernsprechnetzes und der IPN bestehen Übergänge, die einen Lastausgleich ermöglichen.

Dienste werden nur zugelassen, wenn ausreichende datenschutztechnische, rechtliche und soziale Gestaltungsmaßnahmen vorgesehen und realisiert wurden. Politisch durchgesetzt werden diese über demokratische Einflußnahme auf die Postpolitik und durch organisierte öffentliche Diskussionen im Rahmen eines 'Bürgerdialogs'.[15]

Die Abhängigkeit der Gesellschaft von der Telekommunikation ist auch in dieser Option hoch. Sie ist höher als heute, aber niedriger als in den anderen Optionen. Die Kommunikation zwischen Unternehmen oder Behörden wird ähnlich vom Funktionieren der Telekommunikation abhängig werden wie in unserem Zukunftsbild. Fällt sie aus, sind auch keine Just-in-Time-Produktion, kein elektronischer Zahlungsverkehr, kein Informationsabruf und keine Behördenkoordination in Verwaltungssystemen mehr möglich. Für den Kontakt zu Kunden und Klienten werden jedoch die neuen elektronischen Dienste kaum genutzt. Insbesondere die Haushalte integrieren in erheblich geringerem Maße Teletransaktionen in ihren Alltag. Die Briefpost, der Einkauf um die Ecke oder der Besuch auf der Bank bleiben erhalten und mit ihnen eine auf persönlicher oder schriftlicher Kommunikation aufbauende Infrastruktur. Auf sie kann in begrenztem Umfang zurückgegriffen werden, selbst wenn im Extremfall die Telekommunikation ausfällt.

In dieser Option dürften die Motive zum Mißbrauch der Telekommunikation im geringsten Maße zunehmen. Zwar werden sie mit der Übertragung konventioneller Tätigkeiten auf die Telekommunikation ansteigen. Die politischen Steuerungsmechanismen erlauben jedoch in größerem Umfang - verglichen mit den anderen Optionen -, sozialunverträgliche oder individuell sehr belastende Nutzungsformen der Telekommunikation zu verhindern. Einige persönliche und politische Mißbrauchsmotive der Trendentwicklung dürften daher entfallen.

Zwar wird im Fernsprechnetz erschwert, daß die Vermittlungsdaten bestimmter Teilnehmer gespeichert und ausgewertet werden können. Das wäre nur möglich, wenn - wie heute - besondere Aufzeichnungsgeräte installiert würden. Einer wirkungsvollen Verschlüsselung der Kommunikationsinhalte sind aufgrund der analogen Übertragungstechnik jedoch Grenzen gesetzt. Das im Fernsprechnetz mögliche 'Zerhacken' der Sprachübertragung kann das Schutzniveau von Verschlüsselungsverfahren nicht erreichen und ist überdies erheblich teurer. Die Telefonkommunikation bleibt daher zumeist ungeschützt gegen Abhörversuche. Zur Unterstützung solcher Abhörversuche können künftig die Techniken der Sprecher- und Spracherkennung eingesetz werden. Mit Hilfe von Rechnern ist die automatisierte Überwachung vieler Teilnehmer und die Auswertung aller gespeicherten Inhaltsdaten automatisch möglich.[16] Die Verletzlichkeit der einzelnen Fernsprechteilnehmer nimmt daher gegenüber dem Zukunftsbild ab, gegenüber heute jedoch zu.

15 S. hierzu Berger u.a. III, 44 ff.

16 S. hierzu die Kritik von Pfitzmann/Pfitzmann/Waidner PIK 1988, 5 ff.; dies. Informatik Spektrum 1988, 122.

Die physischen Schwachpunkte der Netze sind die gleichen wie in unserer Trendbeschreibung. Auch die Manipulationsmöglichkeiten durch Trojanische Pferde oder logische Bomben sind im IPN und in den Fernvermittlungsstellen des Telefonnetzes vergleichbar. Durch die Entkopplung beider Netze wäre der Schaden eines Totalausfalles allerdings geringer. Die flexiblen Netzübergänge ermöglichen weitere Maßnahmen zur Schadensbegrenzung. Ausfälle des ganzen IPN oder der Fernebene im Fernsprechnetz durch Softwarefehler bleiben allerdings ein erhebliches Risiko dieser Option.

Zusammenfassend kann festgestellt werden, daß jede Option zum Ausbau der Telekommunikation die Verletzlichkeit gegenüber heute erhöht. Bisher gibt es noch keine optimale Lösung dieses Problems. Allerdings unterscheiden sich die Optionen im Grad ihres Beitrags zur Verletzlichkeit erheblich. Entscheidend dürfte das Ausmaß der Integration, der Abhängigkeit von einem technischen System und seiner Substituierbarkeit sowie die Erhaltung bzw. Herstellung politischer Steuerungsinstrumente sein.

Danach schneiden die 'sozialtechnokratische Option' und die 'Technikbegrenzungsoption' noch am besten ab. Letztere weist mit der Begrenzung des Schadenspotentials in die richtige Richtung. Sie bietet allerdings schlechte Voraussetzungen für eine technische Gewährleistung des Datenschutzes. Hier liegen die eindeutigen Vorteile der 'sozialtechnokratischen Option'. Diese führt jedoch in eine hohe Abhängigkeit der Gesellschaft von der Telekommunikation. Das nicht auszuschließende Risiko, daß sie vollständig ausfällt, ist nicht tragbar.

Alternative Produktionskonzepte

Wir wollen noch in einem zweiten Bereich sozio-technische Alternativen, die bereits in die Diskussion eingebracht wurden, auf ihre Verletzlichkeit hin untersuchen. Die Zukunft der Industriearbeit muß keineswegs so aussehen, wie sie in unserem Zukunftsbild beschrieben wurde. Aus der Vielzahl möglicher Entwicklungsalternativen[17] wollen wir idealtypisch der dargestellten zentral-technikorientierten Entwicklungsstrategie eine zweite dezentral-humanorientierte Konzeption gegenüberstellen. In beiden Alternativen wird IuK-Technik intensiv genutzt. Sie unterscheiden sich jedoch in der Gestaltung des sozio-technischen Systems.[18]

17 Weitere Alternativen, die sich auch durch eine erheblich geringere Technikorientierung auszeichnen, untersuchen Müller-Reißmann u.a.. Um die Gestaltungsfähigkeit der IuK-Technik erörtern zu können, beschränken wir uns hier auf die zwei Alternativen mit den wohl größten Verwirklichungschancen.

18 S. zum folgenden näher Wengel/Schneider 26 ff.

Nach der dezentral-humanorientierten Strategie[19] wird die funktionale Differenzierung der Industriearbeit wieder zurückgenommen und statt auf zunehmende Automatisierung der Kopfarbeit auf die technik-unterstützten Fähigkeiten der Beschäftigten gesetzt. In einem Fertigungsbetrieb sind beispielsweise neben wenigen zentral zusammengefaßten Abteilungen die Maschinen und Betriebsmittel für einzelne 'Teilefamilien' zu 'Fertigungsinseln' zusammengefaßt. Für jede von ihnen sind jeweils mehrere relativ breit und hoch qualifizierte Beschäftigte mit vielfältigen Fertigungsaufgaben betraut. Bisher meist zentralisierte Aufgaben wie die Arbeitsvorbereitung werden in den Fertigungsbereich zurückverlagert. Hand- und Kopfarbeit werden wieder zusammengeführt und die Arbeiten weitgehend von denen geplant und strukturiert, die sie auch erledigen.

Hierfür stehen den Beschäftigten dezentral installierte Rechnerleistung und spezifisch auf die Arbeitsbedürfnisse zugeschnittene Anwendungssoftware zur Verfügung. Die 'Fertigungsinseln' halten und pflegen ihre Daten und Programme selbst. Auch die NC-Programme für ihre computergesteuerten Werkzeugmaschinen erstellen sie selbst, wobei sie auf CAD-Daten zurückgreifen können. Zur Koordination der Fertigungseinheiten, zur Kommunikation mit den Abteilungen für Vertrieb und Konstruktion und zur Steuerung des Materialflusses werden die 'Inseln' vernetzt. Da sie Ein- und Ausgangspuffer haben, sind nur ihre 'groben' Betriebsdaten zentral zu erfassen und zu koordinieren. Die Feinsteuerung der 'Fertigungsinseln' ist Aufgabe der dort Beschäftigten. Hierfür stehen ihnen automatisch erfaßte und aufbereitete Betriebsdaten ihrer 'Insel' zur Verfügung. Eine automatische Leistungskontrolle des einzelnen Beschäftigten ist nicht möglich. Insgesamt funktioniert die 'Fertigungsinsel' praktisch als 'Fabrik in der Fabrik'.

Hinter dieser und der bereits dargestellten zentral-technikorientierten Konzeption stehen unterschiedliche 'Philosophien': Eine zentral-technikorientierte Strategie setzt auf vergegenständlichte Arbeit als wesentliche Produktivkraft und stellt daher perfektionierte, zentralisierte Rechnerkonzepte in den Mittelpunkt. Diese werden von wenigen Spezialisten 'gefahren'. Entscheidungs- und Handlungskompetenzen sind zentralisiert. So wird versucht, die menschliche Entscheidungsfindung und den Produktionsablauf zu formalisieren, als Modell im Computer abzubilden und damit eine möglichst vollständige, aber noch weitgehend flexible Automatisierung des Produktionsablaufs zu erreichen.

Die dezentral-humanorientierte Konzeption stützt sich auf menschliche Fähigkeiten als wesentliche Produktivkraft und nutzt IuK-Technik als dezentrale, aber zum Zweck des Informationsaustauschs vernetzte Werkzeuge für breit qualifizierte Fachkräfte. Der Druck, die Betriebsabläufe zu automatisieren und an die begrenzten Abbildungsfähigkeiten eines Computermodells anzugleichen, wird hier geringer sein.

Ähnlich unterschiedlich wäre die Verletzlichkeit beider Alternativen zu bewerten.[20] In der dezentral-humanorientierten Alternative beträfe der Ausfall eines Rechners oder der

19 S. hierzu z.B. näher Wengel/Schneider 26 ff.; Brödner 145 ff.; Priore/Sabel 258f.; Kern-Schumann 164 ff.; Müller- Reißmann u.a. 12 ff.

20 S. hierzu auch Wengel/Schneider 42 ff.

Verlust von Daten in der Regel nur einen Teilbereich der Produktion. In diesem stände möglicherweise bereits Ersatzkapazität zur Verfügung - zum Beispiel der Computer des Kollegen. Selbst wenn zugleich das Netz ausgefallen wäre, könnten Sicherungskopien auch von Datenträgern eingelesen werden und vom verantwortlichen Mitarbeiter schnell an den aktuellen Stand herangeführt werden. Da hier qualifizierte Mitarbeiter für einen überschaubaren Bereich zuständig sind, könnten sie kleinere Fehler unter Umständen selbst beheben und durch Improvisationen den Betrieb aufrechterhalten - etwa indem sie ein Steuerungsprogramm nach einer CAD-Zeichnung direkt an der Steuerung der Werkzeugmaschine eingeben. Die durch Puffer reduzierte Kopplung des Systems würde sie hierbei unterstützen. Der Schaden jedenfalls wird häufiger begrenzt bleiben.

In der zentral-technikorientierten Alternative mit zentralisierter Rechnerleistung und Datenhaltung greift im Produktionsablauf ein Rädchen ins andere. Bearbeitungsschritte werden mehr oder weniger automatisch angestoßen. Der größte Teil der Mitarbeiter füllt lediglich Automatisierungslücken aus oder überwacht die automatischen Prozesse. Sie sind daher weniger qualifiziert. Das komplexe Produktionssystem ist intransparenter. Daten und Programme werden automatisch in die Werkzeuge übermittelt. Die Mitarbeiter können daher Fehler weniger schnell erkennen und beheben. Bei ihnen wird sich langfristig ein 'Vertrauen' in die unverstandenen Abläufe entwickeln, das handlungshemmend sein kann: "Es wird schon stimmen." Fehler oder Manipulationen bleiben so möglicherweise länger unerkannt. Werden sie bemerkt, kann ihre Diagnose und Beseitigung in einem so komplexen System Tage dauern. Mindestens ebenso aufwendig wird es sein, verlorene Daten wieder an den aktuellen Produktionsstand heranzuführen. Die Folgen einer Störung des betrieblichen IuK-Systems werden deutlich größer sein und zu längeren Stillständen führen.

Ein entscheidender Unterschied liegt auch in der Wahrscheinlichkeit von Fehlern und Manipulationen. Sie wird auf dem dezentral-humanorientierten Pfad vermutlich geringer sein. Denn die höher motivierten und besser qualifizierten Mitarbeiter werden weniger Fehler machen und weniger Sabotagemotive entwickeln. Gleichzeitig ist auch der Symbolwert für politisch motivierte externe Angriffe geringer. Der dezentrale Aufbau des Produktionssystems macht eine aktuelle, komplette und detaillierte Simulation des gesamten Betriebsgeschehens überflüssig. Seine geringere Komplexität reduziert das Risiko von Systemfehlern.

Je komplexer und zentralisierter ein Produktionssystem dagegen ist, desto leichter kommt es zu undurchschaubaren Computerinteraktionen und desto stärker wird es von externen Spezialisten abhängig sein. Zwar werden CIM-Systeme schon aus Gründen der Funktionsfähigkeit mit ausgefeilten Sicherungssystemen versehen sein. Doch helfen die wenig, wenn sie für externes Wartungspersonal weitgehend außer Kraft gesetzt werden müssen. Außerdem werden zahlreiche interne Systembetreuer mit weitreichenden Vollmachten notwendig sein. Das Super-User-Problem wird dadurch weiter wachsen. Beides könnte sich als zusätzliches Risiko gerade zentral-technikorientierter Vernetzung erwei-

sen. Es wird verschärft, wenn außerdem mit der Auslagerung betrieblicher Funktionen eigene Fähigkeiten zur Störungsbehebung und zur Weiterentwicklung und Anpassung von Software verkümmern oder gar nicht aufgebaut werden.

Im Vergleich scheint also die dezentral-humanorientierte Strategie zu einer geringeren Verletzlichkeit zu führen. Sowohl das Schadensausmaß als auch die Wahrscheinlichkeit von Fehlern und Mißbrauchsaktionen dürften deutlich niedriger sein als im konkurrierenden Konzept. Dies gilt allerdings nur, wenn ein großer Teil der Unternehmen tatsächlich auf dieses Konzept 'setzt', und das Berufsbildungssystem deshalb weiterhin eine breite und intensive Qualifizierung gewährleistet. Dieses Ziel wird schwer zu erreichen sein: Ein dezentrales Produktionskonzept führt zu Konflikten mit althergebrachten Unternehmensstrukturen und den Zwängen des Maschinendenkens in den Köpfen von Managern, Arbeitern und Arbeitnehmervertretern. Vor allem aber könnte die Teilautonomie der Basiseinheiten in der Produktion zu einem Kontrollverlust des Managements führen und die Herrschaftsansprüche des Kapitals über die lebendige Arbeit beeinträchtigen.

19. Gestaltungsvorschläge

Nach dieser exemplarischen Erörterung gesamtgesellschaftlicher Entwicklungsstrategien werden wir uns nun einige Stufen hinab auf die Ebene konkreter Technikanwendungen begeben und Vorschläge erörtern, wie einzelne Technik-Systeme zu sichern sind. Die Sicherungsmöglichkeiten haben wir als Gegenstrategien gegen Fehler und Mißbräuche der IuK-Technik bereits alle vorgestellt und wollen sie daher nicht noch einmal aufführen. Auch sollen sie hier nicht zu einer ausgefeilten Sicherungskonzeption zusammengefügt werden. Dies wäre angesichts der Vielfalt möglicher Anwendungen nur auf einer zu abstrakten Ebene und nach unserer bisherigen Analyse auch nicht widerspruchsfrei möglich. Wir wollen uns in unseren Empfehlungen vielmehr bewußt darauf beschränken, ein ganz bestimmtes Spektrum von Risikominderungsstrategien hervorzuheben.

Wir haben gesehen, daß es sowohl zur Fehlerbekämpfung als auch zur Sicherung gegen Mißbrauch zwei verschiedene, in der Praxis einander ergänzende Konzepte gibt. Das eine versucht - passiv -, das Ausmaß möglicher Schäden zu reduzieren; das andere bekämpft - aktiv - Technikunsicherheit mit zusätzlicher Sicherheitstechnik oder mit Sicherungsmaßnahmen, die gegen Menschen gerichtet sind. Maßnahmen nach dem zweiten Konzept werden unvermeidlich sein, doch empfehlen wollen wir sie nicht: Zusätzliche Sicherheitstechnik erhöht die Komplexität technischer Systeme und damit die Wahrscheinlichkeit von Systemfehlern.[1] Personen- und gesellschaftsbezogene Sicherungsmaßnahmen kosten Freiheitseinschränkungen und Demokratieverluste. Das Schwergewicht auf aktive Sicherungsmaßnahmen zu legen, führt aber noch aus einem weiteren Grund in die falsche Richtung.

Werden Hochrisikosysteme, also Systeme mit hohem Schadenspotential und einer letztlich unbekannten Wahrscheinlichkeit für ihr Versagen oder ihren Mißbrauch, aufgebaut und durch aktive - statt schadensmindernde - Maßnahmen zu sichern versucht, kann das Sicherungssystem nicht mehr im Ernstfall getestet und daher auch nicht mehr nach dem Prinzip von Versuch und Irrtum weiterentwickelt werden. Da die Irrtumskosten zu hoch wären, läßt sich nicht mehr testen, was geschieht, wenn das Telekommunikationsnetz ausfällt, der elektronische Zahlungsverkehr kollabiert, die Warenwirtschaftssysteme zusammenbrechen oder wichtige Behörden ihre Dateien verlieren.

Aktive Sicherungstechnik für Hochrisikosysteme kann nur noch nach dem Prinzip der Hypothetizität entwickelt werden.[2] Da sich die Katastrophe als Folge eines Irrtums oder Mißbrauchs nie ereignen darf, muß versucht werden, durch prognostische Systemanalysen alle möglichen Fehlerquellen und Mißbrauchsmöglichkeiten gedanklich vorwegzunehmen und durch entsprechende Sicherungsmittel zu beseitigen.[3] Der Forderung der

1 S. hierzu Perrow 108f.

2 S. hierzu Häfele 303 ff.

3 S. hierzu auch Roßnagel UPR 1986, 52f.

Hypothetizität können aber, wie wir gesehen haben, IuK-Systeme gar nicht gerecht werden. Dennoch zwingt sie allen Beteiligten das inhumane "Gesetz der Irrtumslosigkeit" auf.[4] Fehler darf sich niemand mehr erlauben. Kann von der Verläßlichkeit eines Sicherungssystems das Eintreten einer Katastrophe abhängen, dürfen weder die Technik versagen, noch Softwarefehler auftreten, noch eine Personenüberprüfung einen Terroristen übersehen. Das hohe Gefährdungspotential zwingt dazu, alles an der Vermeidung des Ernstfalls auszurichten. Die Spielräume werden eng, die Verhältnisse rigide, es bleibt nur noch die "Einbahnstraße harter Gewißheit".[5] Gelingt dieser Kraftakt eine gewisse Zeit, nährt er nur die Illusion, mit noch besserer Sicherheitstechnik auch noch größere Gefährdungen wagen zu können.

Wirkliche Sicherheit gibt es dagegen nur dort, wo 'absolute' Sicherheit erst gar nicht gefragt ist.[6] Sicherheit ist nur zu erzielen, wenn das unvermeidbare Quantum 'Unsicherheit' keine katastrophalen Schäden bewirkt. Die bessere Sicherungsstrategie ist daher, Verhältnisse zu schaffen, in denen ein Irrtum keine verheerenden Folgen hat. Es kommt also darauf an, durch passive Sicherungsmaßnahmen das Schadenspotential zu reduzieren oder die Möglichkeiten katastrophaler Schadensentwicklungen zu unterbinden. Gelingt dies, werden viele aktive Sicherungsmaßnahmen überflüssig. Ist es möglich, aus Versuch und Irrtum wieder zu lernen, haben auch Freiheit und Demokratie wieder bessere Chancen. Viele Maßnahmen der Prävention, der Arbeitsüberwachung und der Personenüberprüfungen verlieren dann ihre Rechtfertigung.

Wir möchten aus der bisherigen Untersuchung einige Empfehlungen ableiten, dieses Gestaltungsziel zu erreichen. Sie sind nicht ohne kontraproduktive Effekte, nicht ohne finanzielle oder organisatorische Nachteile. Sie lösen das Verletzlichkeitsproblem nicht vollständig. Aber sie könnten die ersten Schritte auf dem Weg in die richtige Richtung sein. Sie sind in jede Abwägung der Interessen, die für oder gegen eine bestimmte soziotechnische Alternative streiten, einzubeziehen.

(1) Der Ausschluß von Schäden und die Reduzierung von Schadensfolgen haben Vorrang vor Maßnahmen zur Verhinderung von Fehlern und mißbräuchlichen Aktionen.

Vorrangiges Ziel jedes Sicherungssystems hat zu sein, den Sicherungszwang der IuK-Technik zu vermeiden oder zu verringern, nicht aber ihn optimal zu erfüllen. Wenn ein bestimmter Schaden gar nicht eintreten kann, ist dies immer sicherer als jeder Versuch, ihn durch zusätzliche Maßnahmen zu verhindern. Schadensmindernde Maßnahmen können nicht wie aktive Sicherungsmaßnahmen durch Verläßlichkeitsprobleme in Frage

4 Beck 71.

5 Guggenberger 13.

6 S. auch Guggenberger 24.

gestellt werden. Werden industrielle Prozesse mit weniger Energie betrieben, fahren Züge nicht mit der möglichen Höchstgeschwindigkeit, sind nicht alle Zweigstellen eines Unternehmens von einem einzigen zentralen Großrechner abhängig oder sind die Datenbestände auf mehrere Stellen verteilt, kann sich der zuvor mögliche größte anzunehmende Unfall nicht mehr ereignen. Dürfen Autos in Ortschaften nur 30 km/h und auf Autobahnen nur 100 km/h schnell fahren, könnte auch ohne elektronische Hilfen die Zahl der Verkehrstoten gesenkt und die Abgasbelastung reduziert werden. Jedenfalls ist darauf zu achten, daß Sicherheitsgewinne durch IuK-Technik nicht wieder durch höheren Energieeinsatz, höhere Geschwindigkeiten und komplexere Systeme 'verbraucht' werden.

(2) Techniksysteme, die auf menschlichem Zusammenwirken beruhen und gesellschaftliche Funktionen nur unterstützen, nicht jedoch übernehmen, sind soweit als möglich Automatisierungslösungen vorzuziehen.

So kann etwa das Kommunikationssystem der Briefpost als Ganzes oder in bedeutenden Teilen nicht zerstört werden, weil es auf dem Wissen und dem Können der beschäftigten Menschen und ihrem sehr differenzierten organisatorischen Zusammenhalt beruht. Es könnte allenfalls aufgrund eines bewußten, koordinierten Aktes aller Beteiligten blockiert werden. Soweit IuK-Technik in Flugzeugen, Zügen und Autos die Piloten, Führer und Fahrer in ihrer Tätigkeit unterstützen, ihre Aufmerksamkeit erhöhen oder ihre Reaktionsschnelligkeit verbessern, sind sie sehr hilfreich. Wo sie diese ersetzen, schaffen sie eine unverantwortliche Abhängigkeit vom einwandfreien Funktionieren der Technik. Die Möglichkeit von unvorhergesehenen äußeren Einflüssen, von unbedachten Systemfehlern oder unvollständigen Wirklichkeitsmodellen machen es erforderlich, daß weiterhin Menschen diese Verkehrsmittel lenken und bei einem Versagen der Technik eingreifen können.

(3) Monopolistische Systeme, die mögliche oder bestehende Alternativen verdrängen, sind zu vermeiden, Substitutionsmöglichkeiten zu erhalten.

Ausweichmöglichkeiten zu schaffen oder zu bewahren, ist die beste Vorsorge für einen Ausfall des gefährdeten Systems. Die 'gelbe Post' auch gegen die elektronischen Kommunikationssysteme zu erhalten, hätte etwa den Vorteil, bei einem völligen oder teilweisen Ausfall des ISDN nicht jede Kommunikationsmöglichkeit zu verlieren. Hart- und Papiergeld auch neben einem elektronischen Zahlungsverkehr weiter zu nutzen, könnte bei dessen Zusammenbruch die folgende Katastrophendynamik erheblich mindern. Ist das Büro der Zukunft nicht papierlos, sondern nur papierarm, wären die Auswirkungen weniger verheerend, wenn der Rechner ausfällt oder Dateien verloren gehen.

(4) Soweit dies möglich ist, sind Redundanzen zu schaffen.

Sind Kommunikationsnetze vermascht, arbeiten Rechner parallel, stehen Ersatzrechenzentren bereit, sind alle Dateien und Programme mehrfach kopiert und an unterschiedlichen Orten gesichert oder ist die für den Betrieb der IuK-Systeme notwendige Infrastruktur mehrfach vorhanden, wird das Ausmaß möglicher Schäden gemindert und der Zwang zur Sicherung reduziert. Bleibt der dritte Mann im Cockpit und der Lokführer in seinem Leitstand, werden dadurch Sicherheitsreserven erhalten. Werden Programme von unterschiedlichen Teams entwickelt und vor ihrem Einsatz ausführlich getestet oder werden alle Veränderungen an einem System einer Revision unterworfen, schafft der zusätzliche Aufwand auch zusätzliche Sicherheit.

(5) Soweit möglich, ist eine zeitliche, räumliche, technische und organisatorische Diversifizierung anzustreben. Herstellermonopole sind zu vermeiden.

Die Verwendung unterschiedlicher technischer Prinzipien, Verfahrensweisen, Materialien und Herstellersysteme innerhalb eines komplexen sozio-technischen Systems verhindert, daß der gleiche Fehler, die gleiche Manipulation oder der gleiche Anschlag das gesamte System außer Funktion setzt. So verhindert beispielsweise die Ausstattung der Vermittlungsstellen im künftigen ISDN je zur Hälfte mit Systemen verschiedener Hersteller, daß ein spezifischer Fehler beide Hälften gleichzeitig zerstört. Einen ähnlich positiven Effekt hätten verschiedene Fernmeldenetze für Sprache, Daten und Bilder. Wird ein medizinisches Expertensystem nicht als einziges flächendeckend eingesetzt, sondern neben anderen Systemen genutzt, wirkt sich ein Fehler nur in einem System aus und wird durch den Vergleich mit den anderen erkannt.

(6) IuK-Systeme sind soweit wie möglich zu entkoppeln, linear aufzubauen und dezentral zu nutzen.

Je stärker entkoppelt das System und je dezentraler die Anwendung, desto geringer ist die Reichweite möglicher Schäden. Je stärker vernetzt und in seiner Anwendung zentralisiert ein IuK-System ist, desto weiter kann ein Primärschaden sich auswirken. Je komplexer das System ist, desto größer ist die Wahrscheinlichkeit, daß es zu unvorhersehbaren Interaktionen von Fehlern und Ausfällen kommt. In keinem System sind Fehler und Mißbrauchsaktionen zu vermeiden. Ist das System nur lose gekoppelt, bestehen im Schadensfall - verglichen mit einem eng gekoppelten System - mehr Möglichkeiten helfend einzugreifen und Puffer, Redundanzen oder Substitutionsmöglichkeiten zu finden, um die Schadensdynamik zu begrenzen. Werden Systeme weniger komplex aufgebaut, sind sie übersichtlicher, fehlerärmer und leichter beherrschbar. Jede lineare Anordnung

von Komponenten reduziert die Gefahr, daß Fehler in ihrem Zusammenwirken einen großen Schaden verursachen. Werden kleinere und selbständige organisatorische Einheiten geschaffen, vermindert sich nicht nur das größtmögliche Schadensausmaß, sondern auch der Schutzbedarf. Denn Systeme mit vermindertem Schadenspotential üben einen geringeren Anreiz aus, sie anzugreifen oder zu stören, da die Wirkung eines Mißbrauchs begrenzt ist.

(7) Systeme sollten möglichst bei Fehlfunktionen oder Ausfällen von Komponenten in einen energieminimalen, schadensarmen und stabilen Zustand übergehen.

Als Vorbild könnten die 'fail-safe'-Schaltungen bei der Bahn dienen: Bei einem technischen Defekt, einem Bedienungsfehler oder Ausfall des Lokführers wird der Zug automatisch abgebremst. Systeme, die nach einem Defekt an wichtigen Sicherungssystemen weiterarbeiten oder gar Leistungsexkursionen ermöglichen, sind zu vermeiden. Konstruktive Vorkehrungen, die bewirken, daß sie immer nur auf die 'sichere Seite' ausfallen können, sollten auch bei Autos, medizinischen Geräten oder Anlagen zur Prozeßsteuerung vorgesehen werden.

(8) Für alle die Allgemeinheit betreffenden Schadensmöglichkeiten ist eine systematische Notfallplanung zu betreiben und einzuüben.

Während bisher die Verletzlichkeit der Gesellschaft durch den Mißbrauch oder ein Versagen der IuK-Technik verdrängt wurde, würden durch Notfallplanungen und -übungen das Sicherheitsbewußtsein geschärft und die notwendigsten Maßnahmen zur Schadensbegrenzung und -beseitigung eingeübt.

(9) Die Gestaltung der Technik und der Sicherungssysteme ist an der Zustimmung der Betroffenen und der Öffentlichkeit zu orientieren.

Die Ausrichtung von Planungen am Konsens und nicht nur an Partikularinteressen verhindert nicht alle, aber einige negative Effekte der Informatisierung und ihrer Sicherung und vermeidet zumindest eine Reihe zusätzlicher Motive für einen Mißbrauch der IuK-Technik. Hierzu gehört auch, die Betroffenen an den Gestaltungsentscheidungen zu beteiligen sowie die sozialunverträglichen Effekte der Informatisierung zu begrenzen und - etwa durch eine gerechte Verteilung der verbleibenden Arbeit - aufzufangen.

(10) Auf ökonomische Vorteile und Komfortgewinn durch die IuK-Technik ist zu verzichten, wenn diese nur mit einem hohem Schadenspotential erkauft werden können.

Das Risiko von Hochgeschwindigkeitszügen ist beispielsweise durch den geringen Zeitgewinn nicht zu rechtfertigen. Ebensowenig kann eine bessere Kapazitätsauslastung von Flughäfen oder die Bequemlichkeit und Umweltfreundlichkeit von Auto-Konvois das durch sie hervorgerufene Risiko legitimieren. Selbst wenn die computerintegrierte und zeitgenaue Produktion gegenüber weniger vernetzten und zentralgesteuerten Produktionskonzepten wirtschaftliche Vorteile bieten, ist zu fragen, ob diese das Risiko wert sein können, das mit einem Produktionsausfall verbunden ist.

20. Politischer Handlungsbedarf

Um die genannten Prinzipien in wirtschaftlichen und politischen Abwägungsvorgängen möglichst weitgehend zur Geltung zu bringen und damit die Verletzlichkeit der Gesellschaft zu reduzieren, sollten Rahmenbedingungen für die politische Technikssteuerung geschaffen werden:

Risikovermeidung

Die Verletzlichkeit der Gesellschaft als bloße Möglichkeit von Schadensereignissen ist unsichtbar. Sie entzieht sich der alltäglichen Erfahrung und wird erst in der wissenschaftlichen Analyse bewußt. Die bloß gewußte Verletzlichkeit konkurriert ständig mit handfesten ökonomischen Interessen, organisatorischen Verfestigungen, individuellen Bequemlichkeiten und bürokratischem Machtbewußtsein. Die ungreifbare Gesellschaftsgefährdung steht daher immer wieder in der Gefahr, verdrängt zu werden. Unter diesen Bedingungen ist es schwer, Verletzlichkeitsrisiken überhaupt zu erkennen und bewußt zu machen oder gar Strategien zur Bekämpfung und Vermeidung dieser Risiken durchzusetzen. Die Mißachtung der sowieso nicht wahrnehmbaren Risiken, die in 'wirtschaftlichem Wachstum', 'Weltmarktkonkurrenz' oder dem 'technischen Fortschritt' ihre Rechtfertigung findet, ist jedoch der "kulturelle und politische Boden, auf dem Risiken und Gefährdungen blühen, wachsen und gedeihen".[1]

Obwohl ein Allgemeininteresse hohen Rangs, wird sich die Verringerung der Verletzlichkeit nicht von selbst gegen die vielen Partikularinteressen durchsetzen, die von der beschriebenen Entwicklung in die 'Informationsgesellschaft' echte oder vermeintliche Vorteile haben. Auf Selbsteinsicht und spontane Interessenvertretung zu vertrauen, ist angesichts des Tempos der ökonomisch-technischen Entwicklung, der Irreversibilität mancher Strukturentscheidungen und der Gefährdungsdimensionen zu riskant. Gegen die Dominanz ökonomischer Interessen und das Verdrängen der Risiken muß dieses Interesse institutionell verselbständigt und verfahrensmäßig verankert werden.

Durch die Förderung wissenschaftlicher Projekte und spezifischer Techniken und durch die Vernachlässigung und Unterdrückung anderer wissenschaftlicher Ansätze und Techniken, wurden auch bisher schon technische Veränderungen gesteuert. Zum Schutz vor unverantwortbaren Gefährdungen kommt es darauf an, das Gestaltungskriterium der Verletzlichkeit bereits im Stadium der Technikerforschung und -entwicklung zur Geltung zu bringen. Dies sollte mindestens auf drei Ebenen vorgesehen werden: auf der Ebene der Gesetzgebung, der technischen Normung und der Zulassung technischer Systeme.

---

1 Beck 59.

Gesetzgebung

Welche Verletzlichkeitsrisiken unsere Gesellschaft eingehen und mit welchen Mitteln sie Risiken bekämpfen soll, sind sowohl Entscheidungen "im Bereich der Grundrechtsausübung"[2] als auch "Leit- und Richtungsentscheidungen für das politische Leben und die staatliche und gesellschaftliche Ordnung".[3] In Ausfüllung des Wesentlichkeitsgrundsatzes[4] sollte daher das Parlament die wichtigen Fragen der Technikzulassung und Technikgestaltung selbst regeln. Es hätte dabei neben anderen Kriterien sozialverträglicher Technikgestaltung auch das Kriterium der Verletzlichkeit ausreichend zu berücksichtigen. Die Verfahrens- und Entscheidungsformen des Gesetzgebers sind jedoch zu überdenken und problemadäquat weiterzuentwickeln.

In einem dynamischen, komplexen und von Ungewißheit geprägten Handlungsfeld wie der Entwicklung der IuK-Technik kann nur unter einem sehr hohen Risiko normiert werden. Unter diesen Bedingungen kann Gesetzgebung nicht mehr auf eine abgeschlossene Kodifikation eines allgemeinen Verhaltensmodells zielen und sich in einer einmaligen gesetzgeberischen Entscheidung sowie gelegentlichen Novellierungen erschöpfen. Insbesondere im Technikrecht wurde diese Form der Gesetzgebung mit einer sehr geringen Regelungsdichte erkauft. Die generalklauselartigen Gesetzesvorgaben überlassen die eigentliche Entscheidung über das von der Technik Geforderte den konkretisierenden (privaten) Regeln der Technik selbst.[5] Der Dynamik und Komplexität der Entwicklung in die 'Informationsgesellschaft' entsprechen jedoch nur solche Entscheidungsmodelle, die nicht zu punktuell reduzierten Entscheidungen führen, sondern einen der Entscheidungsmaterie ähnlich komplexen und dynamischen Entscheidungsprozeß organisieren.

Die notwendige Lernfähigkeit des Gesetzgebers[6] muß allerdings systematisch gesichert und institutionalisiert werden, da soziale Erfahrungsbildung bei so komplexen und in die Zukunft reichenden Auswirkungen 'spontan' nicht mehr ausreichend möglich ist. Der Prozeß eines "Nachfassens" des Gesetzgebers[7], also die Reflexivität der Gesetzgebung, bedarf der organisatorischen Unterstützung, indem in den gesetzgeberischen Prozeß der Technikgestaltung systematisch Rückkopplungsmechanismen eingebaut werden.[8] Gesetzgebung zu Hochtechnologien muß also als ein offener, auf Selbstkorrektur angewiesener Prozeß gestaltet werden, der gesellschaftliche Erfahrungen mit der Technik, Konflikte um die Technik und das jeweils vorhandene Wissen über künftige Technikauswirkungen möglichst weitgehend aufnimmt.

---

2 BVerfGE 49, 89 (126) mwN.

3 Böckenförde 383.

4 S. hierzu näher Roßnagel 1987b, 24 ff. mwN.

5 S. hierzu näher Roßnagel UPR 1986, 46 ff.

6 S. hierzu BVerfGE 49, 89 (132); s. hierzu auch Bull RuP 1987, 131; Roßnagel RuP 1987, 4 ff.

7 S. hierzu näher Roßnagel 1987b, 37 ff.

8 S. hierzu Ladeur ZfG 1987, 150; Scherer DBW 1987, 636.

Um die Zukunftsoffenheit gesellschaftlicher Lernprozesse sicherzustellen, ist der Typ des 'Jahrhundertgesetzes' zu ersetzen durch Sequenznormen, die die Entwicklung technischer Systeme zeitlich strukturieren. Sie sind zeitlich befristet und binden die einzelnen Entwicklungsschritte an jeweils vorangegangene Folgenanalysen und Sicherungen gegen ungewollte Folgen. Diese legislatorische Vorgehensweise ermöglicht, Fehlentwicklungen relativ schnell zu korrigieren und technische wie systemare Alternativen länger offenzuhalten. Dadurch würde zwar der Bestandsschutz riskanter Technikentwicklungen auf den Geltungszeitraum des Gesetzes beschränkt, dafür aber die politische Lern- und Handlungsfähigkeit erheblich erhöht. Nur so kann verhindert werden, daß technische Systeme ausschließlich nach privaten oder beschränkten öffentlichen Interessen entwickelt werden. Die sozialen Risiken würden nicht mehr allein auf die Allgemeinheit oder bestimmte Bürgergruppen abgewälzt, sondern auch von denen getragen, die die Sozialverträglichkeit ihrer Entwicklung behaupten.

Der Gesetzgeber sollte für den jeweiligen Bewertungs- und Entscheidungsprozeß zumindest vier Prüfungsschritte vorsehen und deren jeweils spezifische organisatorische Voraussetzungen gewährleisten[9]:

(1) Alternativen entwickeln

Eine normative Steuerung der Technikentwicklung ist nur möglich, wenn zwischen der Nutzung und der Nichtnutzung einer bestimmten Technik oder zwischen funktionaläquivalenten Alternativen gewählt werden kann. Zu einer geplanten Entscheidung müßten daher immer auch mögliche Alternativen dargestellt werden. Als Voraussetzung hierzu hätte der Gesetzgeber unstrukturierte Handlungszusammenhänge und die durch die Technologie ausgelösten Veränderungsprozesse systematisch zu strukturieren und durch Bündelung von Informationen und Optionen beobachtbar und evaluationsfähig zu machen. Entscheidungsmöglichkeiten erhält sich der Gesetzgeber nur dann, wenn er bestehende sozio-technische Verzweigungssituationen identifiziert und offenhält oder mögliche erkennt und herzustellen versucht. Diesen Entscheidungsspielraum kann er jedoch nur erhalten oder sogar ausweiten, wenn er sich nicht auf ein Technik-System fixiert und sich von diesem abhängig macht, sondern technologiepolitisch neutral möglichst viele technische Alternativen fördert.

(2) Implikationsanalysen erstellen

Für diese Alternativen sind die sozialen, rechtlichen, wirtschaftlichen und ökologischen Folgen abzuschätzen. Da die wissenschaftliche Kapazität zur Durchführung der erforderlichen zukunftsorientierten Implikationsanalysen weitgehend fehlt, ist sie durch entspre-

9 S. hierzu Ueberhorst 245f.; Roßnagel 1986, 364 ff.; Roßnagel/Wedde DVBL 1988, 570 ff.

chende Nachfrage und den dauerhaften Aufbau von Forschungsmöglichkeiten zu schaffen. Folgeabschätzungen dieser Art sind die Voraussetzungen jeder normativen Steuerung des technischen Wandels nach sozialen Kriterien. Sie sollten auch dazu beitragen, daß sich die betroffenen gesellschaftlichen Gruppen möglichst frühzeitig mit den technischen Veränderungen auseinandersetzen.

(3) Folgen bewerten

In einem dritten Schritt sind die Implikationen der technischen Alternativen nach allen relevanten Beurteilungskriterien zu bewerten. Die in einer demokratischen Gesellschaft notwendig offenen Bewertungsprozesse erfordern eine hinreichend diskursive Erörterung der verschiedenen Alternativen in der Öffentlichkeit und in den gesetzgebenden Körperschaften. Nur wenn alle kontroversen Argumente aufgenommen und bearbeitet werden, sind die Bewertungen intersubjektiv vermittelbar, konsensfähig und demokratisch legitimierbar.

(4) Regelungsprogramme entwickeln

Aus der Bewertung sind schließlich rechtspolitische Schlußfolgerungen für die konkurrierenden Alternativen zu ziehen. Um die gesellschaftliche Lernfähigkeit im Umgang mit riskanten Technik-Systemen zu erhalten, sind die Entscheidungen zu befristen und vom weiteren gesellschaftlichen Lernprozeß im Umgang mit der Technik abhängig zu machen.

Technische Normung

Die Aufgabe der Techniksteuerung darf das Parlament nicht überlasten und andere Entscheidungsprozesse blockieren. Es genügt, wenn das Parlament zwar die wesentlichen Entscheidungen trifft, sich aber auch auf die wesentlichen Entwicklungslinien und Grundsatzentscheidungen beschränkt. Das Parlament wäre auch nicht in der Lage, alle erforderlichen Detailregelungen selbst zu treffen. Wie im Technikrecht üblich[10], wird der Gesetzgeber auch für die IuK-Technik die Konkretisierung seiner allgemeinen Vorgaben den Trägern der überbetrieblichen technischen Normung überlassen. In den Normen dieser meist privaten Vereine wie DIN, VDI oder VDE werden der Stand der jeweiligen Technik festgehalten und konkrete Anforderungen an die Beschaffenheit technischer Produkte gestellt. Die technische Normung beeinflußt daher sehr stark die konkrete Ausgestaltung von Technik-Systemen.

10 S. hierzu näher Roßnagel UPR 1986, 46 ff.

In noch viel stärkerem Maße gilt dies für die Normung der IuK-Technik. Denn sie unterscheidet sich von der Normung anderer Techniksysteme in zwei wichtigen Aspekten: Sie erfolgt zum einen bereits heute überwiegend auf europäischer Ebene. Mit der Gründung des Europäischen Instituts für Telekommunikationsnormen im März 1988 wurde eine wichtige Voraussetzung geschaffen, rasch europaweit geltende Telekommunikationsspezifikationen zu schaffen. Zum anderen gilt für die IuK-Technik, daß nicht nur - wie in in den meisten anderen Bereichen technischer Normung - der bereits erreichte Stand der Technik nachvollzogen wird, sondern im Gewand technischer Spezifikationen entwicklungssteuernd, zumindest entwicklungsbegleitend zentrale Eckwerte für neue Techniksysteme gesetzt werden.

Auf diese Normung sollte zumindest in zweierlei Hinsicht Einfluß genommen werden: Der Beschluß des Europäischen Rats "über die Normung auf dem Gebiet der Informationstechnik und Telekommunikation" vom Dezember 1986 nennt als Ziele für die künftigen Normungsaktivitäten zwar die Verbesserung der internationalen Wettbewerbsfähigkeit, die Schaffung eines europäischen Binnenmarktes, die Erleichterung eines gemeinschaftsweiten Informationsaustauschs, die Sicherstellung von Anwenderbedürfnissen und gleiche Konkurrenzbedingungen bei der Vergabe öffentlicher Aufträge. Kein Ziel der Normung ist jedoch, die Verletzlichkeit der Gesellschaft zu verringern. Wegen der Bedeutung der Normung darf diese jedoch nicht nur an Effizienz und Wettbewerbsfähigkeit ausgerichtet werden, sondern muß auch Sicherheitsziele berücksichtigen.

Insoweit könnten die Normungen von Sicherheitsklassen für Computer in den 'Trusted Computer System Evaluation Criteria' des amerikanischen Verteidigungsministeriums und für Computernetzwerke in den 'Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria' des amerikanischen National Computer Security Centers vielleicht ein Beispiel sein. Nach einem 1987 im US-Kongreß eingereichten Gesetzentwurf soll das National Bureau of Standards Verwaltungsvorschriften, Richtlinien, Bewertungsverfahren und Ausbildungsregeln erlassen, um einen Mindeststandard an Sicherheit und Vertraulichkeit sensitiver Informationen in Systemen der Bundesverwaltung sicherzustellen.[11]

Außerdem ist das Verfahren der Normung nach den Mindestkriterien demokratischer Entscheidung zu gestalten. Derartig weitreichende Entscheidungen dürfen nicht im geschlossenen Kreis der marktbeherrschenden Herstellerindustrien und der organisierten Großanwender getroffen werden. Die Zusammensetzung der Normungsgremien ist zumindest um Vertreter betroffener Arbeitnehmer und Benutzer zu erweitern und das Normungsverfahren selbst öffentlich durchzuführen.

11 Der Gesetzentwurf ist abgedruckt in DuD 1987, 544 ff.

Zulassungsverfahren

Die Gestaltungsentscheidungen auf den beiden vorhergehenden Ebenen müssen gegen widerstrebende Interessen organisatorisch durchgesetzt und in ihrem Vollzug kontrolliert werden. Auch wenn die Anwendungsbedingungen etwa durch ein neues Haftungsrecht so verändert würden, daß ein stärkeres Eigeninteresse an der Sicherheit von IuK-Technik entsteht, dürfte diese Aufgabe doch ohne institutionelle Verfestigungen und geordnete Verfahren nicht zu erfüllen sein. Hierbei wäre zum einen etwa an einen parlamentarischen Ausschuß zu denken, der die Abhängigkeit der Gesellschaft von IuK-Systemen überwacht und allen involvierten gesellschaftlichen und staatlichen Instanzen Vorschläge macht, einer zunehmenden Verletzlichkeit gegenzusteuern. Zum anderen müßte wohl eine Validierungsstelle dafür sorgen, daß in Zulassungsverfahren für IuK-Systeme der jeweils festzulegende Mindeststandard an Sicherung und Schadensvorsorge gewährleistet ist.

So radikal, wie der Vorschlag klingt, ist er gar nicht. Andere Techniksysteme - etwa Kraftfahrzeuge - dürfen auch nur genutzt werden, wenn sie zuvor auf ihre Sicherheit hin überprüft und zugelassen wurden. Alle Telekommunikationsendgeräte bedürfen einer Zulassung des Fernmeldetechnischen Zentralamts, und die Einhaltung der Datensicherheit wird schon seit über einem Jahrzehnt von den Beauftragten für den Datenschutz bzw. den Aufsichtsbehörden kontrolliert. Für das Technikrecht ist es sogar eher ungewöhnlich, daß gesellschaftlich so riskante Systeme nicht längst einer präventiven staatlichen Kontrolle unterliegen. Auch IuK-Systeme einem Zulassungsverfahren zu unterwerfen, wäre also nur systemgerecht. Es gibt auch bereits entsprechende Vorbilder im Ausland:

Um die Hersteller und Anwender zu einer an der gesellschaftlichen Verletzlichkeit orientierten Technik- und Aufgabenplanung zu bewegen, schlug die SARK-Studie des schwedischen Verteidigungsministeriums[12] mehrere Alternativen vor:

- eine Institution, die Ratgeber und Wegweiser in Verwundbarkeitsfragen sein soll,
- ein umfassendes Konzessionsverfahren für IuK-Anlagen oder
- eine Aufsichtsbehörde mit weitgehenden Eingriffsrechten.

Das Verwundbarkeitskomitee (SARK) als Untersuchungsgremium wurde 1981 vom Verwundbarkeitsausschuß (SARB) abgelöst. Dieser hat die eher praktische Aufgabe, die Verletzlichkeit der Gesellschaft zu mindern, indem er Anwender informiert und berät sowie Methoden und Hilfsmittel zur Sicherung der Informationsverarbeitung entwickelt. Zusammen mit staatlichen Behörden, Gemeinden, Banken, Versicherungen und Industrieunternehmen hat SARB eine Methode zur Verletzlichkeitsanalyse konkreter Technik-

12 S. SARK 268 f.

anwendungen hervorgebracht, die - nach eigener Einschätzung - mit Erfolg Anwendung findet.[13]

Eine spezielle Institution für die Belange der IuK-Sicherheit ist sicher ein organisatorischer Fortschritt. Ob ihre Beratungs- und Informationskompetenzen jedoch genügen, um den künftigen Verletzlichkeitsproblemen gerecht zu werden, darf bezweifelt werden. In den USA müssen Hersteller von medizinischen Geräten in Sicherheitsstudien deren Zuverlässigkeit nachweisen, und die amerikanische Arzneimittelbehörde FDA will künftig von ihnen sogar die Zusicherung, daß keine Softwarefehler zu Verletzungen des Patienten führen können.[14] Ohne ein Zulassungsverfahren zumindest für kritische Anwendungen in Wirtschaft und Staat wird eine Reduzierung der Verletzlichkeit wohl nicht zu erreichen sein.[15]

Kritische Diskurse

Die Beurteilung der Risiken und die Bewertung von Schutzmaßnahmen ist weitgehend von subjektiven Wertungen abhängig. Gerade deshalb ist es erforderlich, den Gefahren möglicher einseitiger Bewertungen durch institutionalisierte kritische Diskurse zu begegnen. Sie sollten für jede der drei genannten Gestaltungsebenen initiiert werden, indem sowohl das gesamte Spektrum der Wissenschaft als auch die Öffentlichkeit beteiligt werden. Diese Diskurse sollten eine kontroverse Reflexion über die Verletzlichkeit der Gesellschaft in Gang bringen. Sie sollten jedoch nicht auf einen vorschnellen Konsens zielen, sondern vielmehr einer kritischen Aufarbeitung der Verletzlichkeitsprobleme dienen. Dazu könnten sie den sozialen Akteuren ein neues Interaktionsfeld eröffnen, in dem die bestehenden Konfliktbeziehungen selbstverständlich weiterexistieren.[16]

Soweit Parlament, Normungsgremien und Zulassungsstellen auf wissenschaftliche Zuarbeit angewiesen sind, sollten sie vermeiden, von einer Seite der wissenschaftlichen Kontroverse abhängig zu sein und dadurch möglicherweise relevante Gesichtspunkte zu vernachlässigen. Durch Parallelforschung, Reviewstudien und institutionelle Absicherung kritischer Diskursprozesse sollten jeweils die ungesicherten Behauptungen und impliziten Vorurteile des Gegenstandpunkts herausgearbeitet werden. Durch die institutionalisierte gegenseitige Kritik könnte auch die Attitüde der Irrtumslosigkeit in der (Risiko-)Wissenschaft aufgehoben werden. Die Gutachtenaufträge sollten nicht eindeutige Aussagen über Risikobereiche verlangen, wo allenfalls Näherungswissen möglich ist. Als Anstoß kritischer Diskussionen müßten sie vielmehr verlangen, daß jedes Gutachten jeweils ein Spektrum von Alternativen, die Unsicherheitsbereiche, die Nachteile und Gefahren einer

13 S. hierzu z.B. Eriksson 113 ff.

14 S. Schuh, Zeit 17/1988, 86.

15 So auch Lutterbeck 1985, 37.

16 S. hierzu Lagadec 190.

jeden Alternative angibt. Die Gutachten sollten die Debatte also eröffnen, nicht abschließen.[17] Jedenfalls hätten Parlament, Normungsgremien und Zulassungsstellen zu gewährleisten, daß konkurrierender Sachverstand zur Verfügung steht und der Zugriff auf alle wissenschaftlichen Kenntnisse und Anschauungen sichergestellt ist.

Lernprozesse der Gesellschaft im Umgang mit riskanter Technik setzen Bürger voraus, die in der Lage sind, sich selbst ein Urteil zu bilden und sich zu engagieren. Bürgerinitiativen waren die ersten, die auf Risiken der Atomenergie und der Umweltverschmutzung aufmerksam gemacht haben. Ohne den starken Druck der Öffentlichkeit hätte das Allgemeininteresse an Umweltschutz und sicherer Energieversorgung keine Chancen, sich gegen die mächtigen Partikularinteressen durchzusetzen. Ebenso wie in der Ökologiedebatte ist die Sensibilität und politische Kraft engagierter Bürger notwendig, um Verletzlichkeitsrisiken durch IuK-Technik zu erkennen und ins öffentliche Bewußtsein zu heben. Nur durch eine kritische Öffentlichkeit sind Risikominderungen gegen Widerstände durchzusetzen. Die Informations-, Organisations- und Artikulationsmöglichkeiten von Bürgergruppen zu verbessern, muß daher ein überlebenswichtiges Anliegen einer verletzlichen Gesellschaft sein.

Eine Beteiligung der gefährdeten Bürger an den Entscheidungen der Normungsgremien und Zulassungsstellen ist aber nicht nur politisch notwendig, sondern auch rechtlich geboten. Techniksteuerung verteilt nämlich Risiken und gestaltet Grundrechtsbeziehungen. Die Schutzpflicht des Staates kann es gebieten, den betroffenen Bürgern Gelegenheit zu geben, in einem vorverlagerten Rechtsschutzverfahren befürchtete Beeinträchtigungen ihrer Grundrechte geltend zu machen. "Für einen effektiven Grundrechtsschutz der potentiell Gefährdeten ist angesichts des Ausmaßes denkbarer Gefahren entscheidend, daß bereits das behördliche Verfahren geeignet ist, im konkreten Fall zu 'richtigen' sicherheitsrelevanten Entscheidungen zu führen. Wahrscheinlich läßt sich nur über das Verfahrensrecht verhindern, daß der Bereich zwischen Recht und Technik zum juristischen Niemandsland wird."[18]

Sowohl für das Zulassungsverfahren als auch für die technische Normung ist zu prüfen, wie die Öffentlichkeit beteiligt werden kann. Zumindest müßte auf allen Ebenen der Technikgestaltung eine ausführliche Information der Öffentlichkeit über die anstehenden Entscheidungen erfolgen. Dabei müssen die Bürger nicht über jedes Detail unterrichtet werden. Aber sie sollten wissen, was auf dem Spiel steht; sie sollten um die Zwänge, die möglichen Alternativen und deren Kosten, das einzugehende Risiko und die Unsicherheiten seiner Abschätzung wissen. Nur so können die Menschen überhaupt entscheiden, große Risiken um ihrer Vorteile willen in Kauf zu nehmen.[19] Die Information der Öffentlichkeit müßte dazu jeweils in einen öffentlichen Diskurs einmünden, der finanziell, zeitlich und organisatorisch abgesichert ist. Die Interessen nichtorganisationsfähiger Gruppen

17 S. hierzu auch Lagadec 223.

18 BVerfGE 53, 31 (76) - Minderheitsvotum, s. aber auch das Mehrheitsvotum (61f.).

19 S. hierzu auch Lagadec 222.

sollten dabei durch Repräsentanten wahrgenommen werden. Unter noch näher zu diskutierenden Voraussetzungen wäre auch zu ermöglichen, daß nicht hochorganisierte gesellschaftliche Vereinigungen ebenfalls in die Lage versetzt werden, einen Alternativvorschlag auszuarbeiten und darzustellen. Ziel solcher Organisations- und Verfahrensregelungen wäre, eine möglichst weitgehende Verzahnung der institutionellen Techniksteuerung mit den Gestaltungsvorstellungen von unten zu gewährleisten.

Keinesfalls jedoch darf die Diskussion über konkrete Sicherungsmaßnahmen allein den Sicherungsfachleuten überlassen werden. Vielmehr sind die politischen Implikationen sicherungsimmanenter Zielkonflikte in einer demokratischen Diskussion zu thematisieren:

- Die Verschlüsselung von Nachrichten, Dateien und Programmen ermöglicht jedem - auch dem, der sich gesellschaftsschädigend verhält, - sich vor Ausspähungen oder Manipulationen zu schützen. Sollen die Interessen der Sicherung und des Datenschutzes vorgehen oder die Interessen der für die innere Sicherheit zuständigen Behörden, jede Kommunikation überwachen und jedes Dokument lesen zu können?
- Zugangs- und Zugriffskontrollsysteme schützen IuK-Systeme vor unbefugtem Eindringen, erfordern aber eine eindeutige Selbstidentifizierung. Sollen hier Sicherungsinteressen höher bewertet werden als das datenschutzrechtliche Interesse an Anonymität?
- Personenkontrollen, Arbeitsüberwachung und Einstellungsüberprüfungen können dazu beitragen, daß Mißbrauchsaktionen weniger leicht möglich sind. Ist im konkreten Fall Freiheitsrechten oder Sicherungsaspekten der Vorzug einzuräumen?
- Präventionsstrategien können möglicherweise Angriffe auf die IuK-Technik verhindern, führen aber zu einem Machtzuwachs bei staatlichen und betrieblichen Sicherungsorganen. Können die ungewissen Vorteile für die gesellschaftliche Stabilität die möglichen Risiken für eine demokratische Politik und einen freien Lebensstil aufwiegen?

Verschärfung des Haftungsrechts

Oft bewirken schon kleinste Veränderungen in den Rahmenbedingungen von Technikanwendungen mehr als Gebote und Verbote. Es ist daher auch zu prüfen, wie durch solche Maßnahmen das Risikobewußtsein und die Bereitschaft, Sicherungsmaßnahmen durchzuführen und zu finanzieren, gesteigert werden können.

Eine solche Möglichkeit wäre die Verschärfung des Haftungsrechts. Bisher haftet, wer ein IuK-System für seine Zwecke einsetzt, nur dann einem Geschädigten, wenn nachzuweisen ist, daß der Schaden auch tatsächlich von dem IuK-System herrührt und er diesen auch verschuldet hat. Nach dem neuen Produkthaftungsgesetz haftet der Hersteller zumindest für Produktfehler unabhängig von seinem Verschulden. Er muß jedoch dann keinen Ersatz leisten, wenn "der Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in der (er) das betreffende Produkt in den Verkehr brachte, noch nicht

bekannt werden konnte".[20] Das Entwicklungsrisiko wird also auch in Zukunft voll auf den Verbraucher abgewälzt.

Müßte dagegen jeder, der ein IuK-System einsetzt, nicht nur bei nachweisbarem Verschulden, sondern wie ein Autohalter auch ohne eigenes Verschulden für jeden Schaden haften, den sein gefährliches Technik-System verursacht, dann würden viele riskante Systeme wohl nicht entwickelt und vorhandene Anwendungen besser gesichert. Würden außerdem immaterielle Schäden durch ein hohes Schmerzensgeld ausgeglichen und der Nachweis, daß der Schaden kausal durch das IuK-System verursacht wurde, wie bei der Produkthaftung durch eine Umkehr der Beweislast erleichtert, müßten zumindest nicht die Geschädigten die Risikofreude des Technikanwenders 'ausbaden'.

Der würde zwar versuchen, seine Haftpflicht zu versichern. Doch dadurch wäre das Problem nur verschoben, denn die Versicherungen werden entweder riskante Anwendungen gar nicht oder nur unter hohen Sicherungsauflagen versichern. Sie würden also weitgehend die Aufgaben wahrnehmen, die sonst einem Zulassungsverfahren zugedacht sind. Dennoch kann eine Verschärfung des Haftungsrechts nicht die staatliche Kontrolle der Technikanwendung ersetzen. Schließlich werden die privaten gewinnorientierten Versicherungen nicht die gleichen Gestaltungsziele einer schadensmindernden Sicherheitspolitik vertreten wie beispielsweise Behörden, die dem Interesse einer sozialverträglichen Technikgestaltung verpflichtet sind.

Bewahrung von Steuerungsmöglichkeiten

Als Grundvoraussetzung jeder Technikgestaltung dürfen bestehende Steuerungsmöglichkeiten in keinem Fall aus der Hand gegeben werden. Daher spricht beispielsweise der Aspekt der Verletzlichkeit grundsätzlich für eine Erhaltung des Fernmeldemonopols und gegen seine Deregulierung. Nur eine der Allgemeinheit verpflichtete Institution ist in der Lage - jenseits kurzfristiger wirtschaftlicher Interessen - die notwendigen Sicherungsmaßnahmen durchzusetzen. Der Regierungsentwurf zur Neustrukturierung der Bundespost will diese jedoch in drei organisatorisch und wirtschaftlich weitgehend verselbständigte öffentliche Unternehmen aufspalten und private Anbieter zu Telekommunikationsdiensten zulassen.[21] Die damit eingeleitete Politik der Deregulierung vertraut darauf, daß gerade die Konkurrenz dezentraler Marktkräfte positive Auswirkungen für das Allgemeinwohl haben wird. Sie sieht jedoch keine Instanz vor, die mögliche Risiken für die Allgemeinheit oder einzelne, die von der künftigen Telekommunikationstechnik und ihren Anwendungen ausgehen können, rechtzeitig erkennt und ihnen durch Technikgestaltung präventiv begegnet. Trotz der Ungewißheit über die positiven und negativen Entwicklungen gibt der Regierungsentwurf durch seine Maßnahmen zur Privatisierung von Tele-

20 § 1 Abs. 2 Ziff. 5 Produkthaftungsgesetz.

21 S. Bundesregierung, BT-DrS 11/2854..; s. hierzu auch Roßnagel/Wedde DVBl 1988, 562 ff.

kommunikationsdiensten und sein Zurückdrängen des politischen Einflusses auf die Deutsche Bundespost bestehende Gestaltungschancen zum Schutz der Grundrechte aus der Hand.

Eine demokratische Gestaltung der Technik setzt jedoch voraus, daß die Möglichkeiten zur Einflußnahme auf Technikentwicklungen und Technikfolgen nicht privatisiert, sondern demokratisiert werden. Die Entwicklung der Telekommunikation wird sozial nur dann beherrschbar bleiben, wenn die Entscheidungen über technische Neuerungen nicht insoweit verselbständigten öffentlichen Unternehmen oder privaten Investoren überlassen werden, sondern die bestehenden Instrumente politischer Einflußnahme auf die Technikgestaltung erhalten und ausgebaut werden. Auch um die notwendige Lernfähigkeit der Gesellschaft zu gewährleisten, ist nicht eine Deregulierung, sondern eine Demokratisierung der Bundespost geboten.[22]

Die Zukunft offen halten

Kurzfristig gilt es vor allem, Zeit zu gewinnen für eine breite öffentliche Erörterung der Verletzlichkeit im Rahmen einer umfassenden Sozialverträglichkeitsdiskussion. Zu diesem Zweck muß verhindert werden, daß ein unreflektierter Technikoptimismus vollendete Tatsachen schafft, die später zu bereuen wären. Solange schwerwiegende Probleme der Verletzlichkeit nicht gelöst sind, ist es besonders wichtig, alternative Entwicklungsmöglichkeiten möglichst lange offenzuhalten. Reversibilität und Korrigierbarkeit der technischen Entwicklung müssen in angemessenen Zeitfristen möglich bleiben. Riskante Systeme sollten daher erst eine zeitlich bemessene 'Versuchs- und Irrtumsphase' durchlaufen, bevor sie im vollen Umfang installiert und genutzt werden. Die Verletzlichkeit der Gesellschaft dürfte bei problembewußter und vorsichtiger Herangehensweise auf ein akzeptables Niveau zu senken sein. Hierauf müßten sich alle Beteiligten eigentlich verständigen können. Denn eine sinkende Verletzlichkeit unserer Gesellschaft kommt schließlich nicht zuletzt der Sozialverträglichkeit der IuK-Technik zugute.

22 S. hierzu näher Roßnagel/Wedde DVBl 1988, 569 ff.

Expertisen, Expertengespräche, Workshops und unterstützende Kritik

Expertisen

Für unser Projekt haben wir folgende Expertisen erhalten:

Dipl. Ing. Manfred Gottschlich:
Der Mensch an den Grenzen der Technik. Die Zukunft der Prozeßtechnik und ihre Zuverlässigkeit bei wachsendem IuK-Anteil, Hannover, Juni 1988.

Dr. Dirk-Michael Harmsen / Dr. Gerd Weiß: Aspekte der Datensicherheit und der Verletzlichkeit der Informationssysteme im Bankensektor, Fraunhofer-Institut für Systemtechnik und Innovationsforschung (ISI), Karlsruhe, Juli 1988.

Dipl-Sozialwirt Jürgen Wengel / Ing. (grad.) Dipl. Psych. Robert Schneider: Schadenspotentiale einer künftig vernetzten Produktion (CIM) am Beispiel des Maschinenbaus, Fraunhofer-Institut für Systemtechnik und Innovationsforschung (ISI), Karlsruhe, Juli 1988.

Expertengespräche

Für die Erstellung des Zukunftsbilds und die Untersuchung der 'Informationsgesellschaft' haben wir folgende Expertengespräche durchgeführt:

1986

25. 8.	Dipl.Ing. H. Thomas, FTZ, Darmstadt
3. 9.	Dipl.Ing. B. Schmitt, FTZ, Darmstadt
6.10.	H. Busch, Dr. F. Werkentin, Bürgerrechte und Polizei, Berlin
7.10.	Dr. H. Garstka, Senatsrat beim Beauftragten für den Datenschutz, Berlin
28.10.	Prof. Dr. B. Lutterbeck, TU Berlin
29.10.	Dr. J. Seetzen, Heinrich-Hertz-Institut, Berlin
10.11.	Prof. Dr. J. Siekmann, Universität Kaiserslautern
24.11.	Prof. Dr. K. Lenk, Universität Oldenburg
24.11.	Prof. Dr. W. Steinmüller, Universität Bremen

1987

27. 1. Dipl.Ing. Benisch, Dipl.Ing. Effenberger, Fernmeldeamt Darmstadt
16. 2. Dipl.Inform. K.H. Hug, TH Darmstadt
6-9.3. Industriekontakte auf der Cebit-Messe, Hannover
9. 3. Dipl.Ing. M. Wolf, FTZ, Darmstadt
10. 3. J. Schalla, Hannover
12. 3. J. Grosch, Leiter Produktionsbereich Roboter, Reis GmbH, Obernburg
14. 3. H. Holland-Moritz, Chaos Computer Club, Hamburg
9. 4. Dipl.Ing.s Schlesinger, Schubert, Schulz, Christiansen, Dyballa, Fernmeldeamt Düsseldorf
13. 5. Dipl.Ing. K. Storck, FTZ, Darmstadt
20. 5. Dr. H. Redeker, Dr. H. Burkert, GMD, Bonn
20. 5. Dipl.Ing. H. Quinke, GMD, Bonn
20. 5. Dr. E.-J. Büsse, GMD, Bonn
22. 5. Dr. G. Wurch, GMD, Bonn
25. 5. Dipl.Ing. Bittner, Fernmeldeamt Darmstadt
26. 5. H. Kraft, Fernmeldeamt Darmstadt
9. 6. Dipl.Inform. P. Höller, SOVT, Darmstadt
15. 6. Dipl.Ing. R. Brodbeck, Dipl.Ing. C. Rathgeber, Fernmeldeamt Darmstadt
15. 6. Dr. K. H. Vöge, Nixdorf, Berlin
15. 6. Frau Br. Lebrun, Leiterin des RZ, D. Stahnke, M. Auch-Schwelk, Be. Lebrun, Bundeszentralregister, Berlin
16. 6. Dipl.Wilng. B. Schmidt, Dipl.Ing. O. Baireuther, FTZ-PDI, Darmstadt
16. 6. Dr. Below, Leiter des RZ, BfA, Berlin
21. 6. Dipl.Ing. S. Herda, GMD, Bonn
21. 6. Dr. P. Mambrey, GMD, Bonn
22. 6. Dr. W. Langenheder, GMD, Bonn
22. 6. Ch. Jung, Leiter der Zentralbibliothek der Landbauwissenschaften, Bonn
20. 7. Dr. B. Freisleben, TH Darmstadt
12. 8. D. Herbert, K. H. Atzbach, Fernmeldeamt Darmstadt
20.11. Dr. K. Franken, W. Lehmler, Dr. A. Kirchgässner, J. Benz, Universität Konstanz
2.12. Dr. P. Rau, H. W. Hoffmann, Hochschulbibliothekszentrum NRW, Köln

1988

8. 1. E. Wetzel, J. Scheller, Gesellschaft für Information und Dokumentation, Frankfurt
9. 2. Prof. Dr. J. Siekmann, Universität Kaiserslautern

18. 2. Dr. M. Brundke, Dipl. Landwirt H. Staudte, Kuratorium für Technik und Bauwesen in der Landwirtschaft, Darmstadt
7. 3. Dipl.Soz. U. Riehm, Abteilung für Angewandte Systemanalyse, Kernforschungszentrum Karlsruhe
10. 3. Prof. Dr. J. Becker, KomTech, Frankfurt
11. 3. L. Nefiodow, GMD, Leiter der Programmkommission Zukunftskonzept 'Informationstechnik 2000' der Bundesregierung, St. Augustin
22. 3. D. Klumpp, Leiter der Stabsstelle Mensch und Technik, SEL, Stuttgart
22. 3. Ltd. MinR Dr. Handrock, Finanzministerium NRW, Düsseldorf
25. 3. Prof. Dr. K. Haefner, Universität Bremen
13. 4. Prof. Dr. L. Reiner, TU Weihenstephan
15. 4. H. Heist, Leiter der
20. 4. Dipl. Ing. K. van de Castel, Dipl.Ing. O. Schenk, Zentrale der Deutschen Bundesbahn, Frankfurt
21. 4. M.A. P. Zoche, Dipl.Ing. D. Saage, Fraunhofer-Institut für Systemtechnik und Innovationsforschung
9. 5. E. Fortenbacher, Werksdirektor, Heidelberger Druckmaschinen, Amstetten
19. 5. A. Liss, IBM, Bonn
19. 5. Dr. P. Mambrey, GMD, St. Augustin
19. 5. C. Riedel, GMD Bonn
29. 5. H. Busch, Bürgerrechte und Polizei, Berlin
3. 6. Bundeskriminalamt, fünf Herrn der Abteilungen Datenverarbeitung sowie Ermittlung und Auswertung und des kriminalistischen Instituts
6. 6. Dr. Ch. Hüttig, Fb Politikwissenschaft, TH Darmstadt
11. 6. Dipl.Soz. W. Dombrowski, Universität Kiel
12. 6. Prof. Dr. D. Viefhues, Hochschule Bremerhaven
14. 6. v. Machui, Daimler Benz AG, Werk Bremen
15. 6. Prof. Dr. J. Haas, TÜV Rheinland, Köln
16. 6. J. Barth, stellv. Geschäftsführer, AOK, Dortmund
22. 6. Reg.Dir. G. Kaufhold, Th. Ewald, Stabsstelle für Information und Kommunikation des Staatsministeriums Baden-Württemberg
23. 6. W. Dorschel, Leiter der Niederlassung, F.-J. Schwarz, INFO AG, Stuttgart
8. 7. MinR D. Affeld, Ministerium für Arbeit, Gesundheit und Soziales, Düsseldorf
25. 7. K. H. Steinberg, Leiter des RZ, P. Gabor, Sparkasse Wuppertal
28. 7. L. Rausch, Öko-Institut, Kassel
1. 8. Dipl.Kaufm. W. Papst, Direktor der Volksbank Wiesbaden
1. 8. B. Fix, H. Holland-Moritz, M. Sentz, Chaos Computer Club, Heidelberg
11. 8. Dipl.Ing. H. Winkler, Dr. Möller, Siemens, München
15. 8. Dr. Joseph Falke, Zentrum für Europäische Rechtspolitik (ZERP), Bremen
19. 8. Prof. Dr. Kuhlen, Universität Konstanz

Workshop: Zukunftsbild

Die erste Fassung des Zukunftsbilds war Gegenstand eines Workshops am 22. 10. 1987 in Darmstadt. An ihm haben teilgenommen:

Prof. Dr. U. v. Alemann, Rhein-Ruhr-Institut für Sozialforschung und Politikberatung (RISP)
J. Bogumil, Fernuniversität Hagen
A. Gorres, Sozietät für Beratung und Planung
P. Hogsche, Sozietät für Beratung und Planung
H.J. Lange, Fernuniversität Hagen
Dr. W. Rammert, Universität Bielefeld
J. Schaffner, Institut für Angewandte Systemforschung und Prognose, Hannover
R. Schleicher, Projekt Regionale Technologiepolitik, Wuppertal
P. Sacher, Gesamthochschule Kassel
A. Solle, Zukunftswerkstätten Ratingen

Kritik: Zukunftsbild

Eine Kritik der ersten Fassung des Zukunftsbildes erhielten wir schriftlich oder im Rahmen eines Expertengespräches von

E. Becker-Töpfer, Gewerkschaft Handel, Banken und Versicherungen, Düsseldorf
Dr. M. Brundke, Kuratorium für Technik und Bauwesen in der Landwirtschaft, Darmstadt
U. Erb, Die Grünen im Bundestag, Bonn
Prof. Dr. K. Haefner, Universität Bremen
Ch. Jahl, Industrie- und Anlagenbau Gesellschaft mbH, München
Prof. Dr. F. Kaderali, Fernuniversität Hagen
Prof. Dr. H. Kubicek, Universität Trier
A. H. Liss, IBM, Bonn
L. A. Nefiodow, GMD, Leiter der Programmkommission Zukunftskonzept 'Informationstechnik 2000' der Bundesregierung, St. Augustin
B. Pagalies, Hamburg- Mannheimer Versicherung, Hamburg
A. Pfitzmann, Universität Karlsruhe
Prof. Dr. L. Reiner, TU Weihenstephan
Prof. Dr. J. Siekmann, Universität Kaiserslautern
Dipl. Landwirt H. Staudte, Kuratorium für Technik und Bauwesen in der Landwirtschaft, Darmstadt
G. K. Storck, FTZ, Darmstadt

Prof. Dt. D. Viefhues, Hochschule Bremerhaven
dem Arbeitskreis 'Zukunft der Arbeit', Heidelberg
einer Gruppe Bremer Bürger

Workshop: Verletzlichkeit

An unserem Workshop "Die Verletzlichkeit einer künftigen Informationssgesellchaft" am 13. und 14. 10. 1987 in der Evangelischen Akademie Iserlohn haben teilgenommen:

Prof. Dr. U. v. Alemann, Rhein-Ruhr-Institut für Sozialforschung und Politikberatung, Duisburg
Prof. Dr. K. Brunnstein, Universität Hamburg
Prof. Dr. G. Ebbrecht, Evangelische Akademie Iserlohn
Bernd Fix, Heidelberg
Dr. H. Garstka, Senatsrat beim Berliner Datenschutzbauftragten, Berlin
Dipl.Ing. S. Herda, GMD, St. Augustin
W. Hill, FTZ, Darmstadt
Dipl.Inform. P. Höller, SOVT, Darmstadt
W. Hölzer, Kooperationsstelle des DGB, Dortmund
Ch. Jahl, Industrie- und Anlagenbau Gesellschaft mbH, München
Dr. W. Mende, Fernuniversität Hagen
B. Pagalies, Hamburg-Mannheimer Versicherung, Hamburg
A. Pfitzmann, Universität Karlsruhe
Jochen Rieß, Universität Bremen
H. R. Schuchmann, Siemens AG, München
Prof. Dr. W. Steinmüller, Universität Bremen
Th. Vogler, Bayrische Hackerpost, München
Prof. Dr. B. Walke, Fernuniversität Hagen
K.-T. Weise, Volkswagen AG, Wolfsburg

Arbeitspapiere der
Projektgruppe Verfassungsverträgliche Technikgestaltung - provet
Darmstadt

AP 1 Alexander Roßnagel: Die Verfassungsverträglichkeit von Technik-Systemen - am Beispiel der Informations- und Kommunikationstechnik, Oktober 1986, 18 S. (veröffentlicht in: Recht und Politik, Heft 1/1987, S. 4 ff.)
AP 2 Alexander Roßnagel/Peter Wedde: Planungsverfahren von unten für Infrastrukturmaßnahmen und Länderkompetenzen bei Postplanungen, November 1986, 16 S.
AP 3 Peter Wedde: Zwischenbericht zur Verletzlichkeit der Datenverarbeitung in der öffentlichen Verwaltung, Dezember 1986, 89 S. AP 4 Volker Hammer: Technik-Szenario, August 1987, 22 S.
AP 5 Alexander Roßnagel/Volker Hammer/Ulrich Pordesch/Peter Wedde: Trendszenario einer Informationsgesellschaft, August 1987, 47 S.
AP 6 Ulrich Pordesch: Der Beitrag der Telekommunikation zur Verletzlichkeit der Gesellschaft, September 1987, 142 S.
AP 7 Peter Wedde: Die künftige Bedrohung der Informationsgesellschaft. Überlegungen zu Angriffsmotiven, Angriffsformen und Angriffsfolgen, September 1987, 94 S.
AP 8 Volker Hammer: Technische Aspekte der künftigen Verwundbarkeit der EDV, September 1987, 33 S.
AP 9 Peter Wedde: Die Verwundbarkeit der Datenverarbeitung in der Verwaltung, September 1987, 107 S.
AP 10 Alexander Roßnagel/Volker Hammer/Ulrich Pordesch/Peter Wedde: Thesen zur Verletzlichkeit einer künftigen Informationsgesellschaft, August 1987, 30 S.
AP 11 Alexander Roßnagel: Sie Sozialverträglichkeit von Techniksystemen, Juli 1987, 4 S. (veröffentlicht in: SoTech-Rundbrief Nr. 5 / September 1988), S. 22 ff.).
AP 12 Alexander Roßnagel: Sozialverträglichkeit von Computern - rechtlich gesehen, Dezember 1987, 27 S. (erscheint in: Bechmann/Rammert (Hrsg.), Technik und Gesellschaft, Jahrbuchs, 1989).
AP 13 Alexander Roßnagel/Volker Hammer/Ulrich Pordesch/Peter Wedde: Skizze zur Verfassungsverträglichkeit künftiger Informations- und Kommunikationstechniken, Januar 1988, 93 S..
AP 14 Volker Hammer/Alexander Roßnagel: Informationstechnische Vernetzung - Techniksicherheit und Demokratieverträglichkeit - ein lösbarer oder unlösbarer Widerspruch?, März 1988,17 S. (veröffentlicht in: Forum für interdisziplinäre Forschung 2/1988, 39 ff.).

AP 15 Alexander Roßnagel: Möglichkeiten verfassungsverträglicher Technikgestaltung, September 1988, 16 S. (veröffentlicht in: Alexander Roßnagel (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, 177 ff.).
AP 16 Ulrich Pordesch: Das Problem der Verletzlichkeit in den Bereichen Landwirtschaft, Bundesbahn, Polizei, Juni 1988, 43 S.
AP 17 Volker Hammer: TeleTrusT: Verletzlichkeit und Verfassungsverträglichkeit eines Konzepts für rechtssichere Transaktionen in der Informationsgesellschaft, Juni 1988, 30 S. (veröffentlicht in: Datenschutz und Datensicherung 8/1988, 391 ff.).
AP 18 Alexander Roßnagel: Verfassungsverträglichkeit künftiger Informations- und Kommunikationstechniken, April 1988, 17 S. (gekürzt veröffentlicht in: Universitas 2/1989).
AP 19 Volker Hammer/Alexander Roßnagel: Die künftige Informatisierung der Gesundheitsvorsorge und ihr Einfluß auf die Verwirklichung von Grundrechten, Mai 1988, 35 S. (gekürzte Fassung in: Alexander Roßnagel (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft und Grundgesetz, Stuttgart 1989, S. 121 ff.).
AP 20 Alexander Roßnagel/Peter Wedde: Die Reform der Deutschen Bundespost im Licht des Demokratieprinzips, Mai 1988, 22 S. (veröffentlicht in: Deutsches Verwaltungsblatt 1988, S. 562 ff.).
AP 21 Peter Wedde: Der Einsatz der Datenverarbeitung in der Steuerverwaltung und im Einwohner- und Meldewesen - Überlegungen zum Ausbau und zur Verletzlichkeit in der Informations- ung Kommunikationstechnik in ausgewählten Bereichen der öffentlichen Verwaltung, Juni 1988, 56 S.
AP 22 Ulrich Pordesch/Peter Wedde: Die zukünftige Verletzlichkeit der Informationsgesellschaft, Januar 1988, 16 S.
AP 23 Alexander Roßnagel: Technik und Recht - wer beeinflußt wen?, Mai 1988, 15 S. (veröffentlicht in: Alexander Roßnagel (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, S. 9 ff.).
AP 24 Volker Hammer: Die künftige Informationsgesellschaft und das Grundrecht auf Information, Juli 1988, 37 S. (veröffentlicht in: Alexander Roßnagel (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, S. 49 ff.).
AP 25 Ulrich Pordesch: Auswirkungen der Computerisierung auf Polizei und Grundrechte, Juli 1988, 33 S. (gekürzt veröffentlicht in: Alexander Roßnagel (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, 87 ff.).
AP 26 Peter Wedde: Verwaltungsautomation und Verfassungsrecht, Juni 1988, 40 S. (gekürzt veröffentlicht in: Alexander Roßnagel (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, S. 67 ff.).
AP 27 Volker Hammer/Ulrich Pordesch: Beherrschbarkeit von Informationssystemen, Juli 1988, 22 S.
AP 28 Alexander Roßnagel: Eine Datenabgabe als Instrument zur Dateneinsparung, Mai 1988,19 S. (erscheint in: Computer und Recht 3/1989).

Abschlußberichte

Alexander Roßnagel/Peter Wedde/Volker Hammer/Ulrich Pordesch: Die Verletzlichkeit der Informationsgesellschaft, Studie im Auftrag des Ministers für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen, August 1988, 295 S.

Alexander Roßnagel/Peter Wedde/Volker Hammer/Ulrich Pordesch: Die Verfassungsverträglichkeit künftiger Informations- und Kommunikationstechniken, Studie im Auftrag des Ministers für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen, November 1988, 380 S.

Literatur

Abel, H.: HICOM und seine Sicherungsmaßnahmen, DuD 1987, 445 ff.

ders.: Auswirkungen neuer Entwicklungen der Informationstechnik auf Datenschutz und Datensicherung in Unternehmen, RDV 1988, 73 ff.

ders./Schmölz W.: Datensicherung für Betriebe und Verwaltung, München 1986

Adam-Schwaetzer, I.: Chancen des Binnenmarktes für Wirtschaft und Handel, Bulletin des Presse- und Informationsamts der Bundesregierung 1988, 537 ff.

Afheldt, H. (Hrsg.): Auf neuen Wegen in die Zukunft. Stuttgart u.a. 1986.

Albers, F.: Risiken beim Einsatz von Personalcomputern, DuD 1985, 201 ff.

Alemann U.V.: Sozialverträglichkeit neuer Technologien: Grundrecht oder Grundwert? in: Roßnagel, A. (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, S. 21 ff.

ders./Schatz, H. (Hrsg.): Mensch und Technik. Grundlagen und Perspektiven einer sozialverträglichen Technikgestaltung, Opladen 1986.

Altvater, E. u.a.: Arbeit 2000, Hamburg 1985.

Andow, P.: Failure of Process Plant Monitoring Systems, in: Wise, J. A./Debons, A. (Eds.), Information Systems: Failure Analysis, NATO ASI Series F 32, Berlin 1987, 233 ff.

Arbeitskreis Rationalisierung Bonn (Hrsg.): Verdatet, Verdrahtet, Verkauft, Stuttgart 1984.

Arndt, G./Rothamel, HJ.: Kommunikationsdienste im ISDN, Telcom Report 8, Sonderheft 'Diensteintegrierendes Digitalnetz ISDN', Februar 1985,10 ff.

Arnold, F.: Die künftige Entwicklung der öffentlichen Fernmeldenetze in der Bundesrepublik und ihre Auswirkungen auf den Benutzer, Hamburg 1984.

ders./Kranz, U. u.a.: Studie für einen 'Telekommunikationsentwicklungsplan" für das Land Nordrhein-Westfalen, hrsg. v. Landespresse- und -informationsamt des Landes Nordrhein-Westfalen, Düsseldorf 1984.

Balkhausen, D.: Die elektronische Revolution, Düsseldorf 1985.

Bangemann, M.: Strategien für die Weltinformationsgesellschaft, Bulletin des Presse- und Informationsamts der Bundesregierung 1987, 777 ff.

Barnaby, F.: Computer und Militär, in: Duve, F. (Hrsg.), Schöne elektronische Welt, Reinbek 1982, 146 ff.

Bäumler, A.: Sicherheitsüberlegungen in Bürokommunikationssystemen, DSB 8/1987, 1 ff.

Baumgartner, T./Borries, V.v./Frosch, A./Harmsen, A./Mettler, P.H.: NRW 2020, Mikroelektronik, Arbeitsmarkt und Gestaltungsmöglichkeiten, Werkstattbericht 35, MAGS, Düsseldorf 1988.

Beck, U.: Risikogesellschaft, Frankfurt 1986.

Beck, T./Wendeling-Schröder, U.: Der Arbeitnehmer als Risikofaktor?, WSI-Mitteilungen 1985, 754 ff.

Becker, J.: Zugangssperren bei US-amerikanischen Datenbanken, NfD 1988, 21 ff.

Bequai, A.: Computer Crime, Lexington 1978.

Berger, J. J./Koch, E. R.: Vorbereitet war so gut wie nichts, in;: Koch, E./Vahrenholt, F. (Hrsg.), Im Ernstfall hilflos, Köln 1980.

Berger, P./Kühn, M./Kubicek, H./Mettler-Meibom, B./Voogd, G.: Optionen der Telekommunikation, Düsseldorf 1988.

Bickenbach, J./Keil-Slawik, R./Löwe, M./Wilhelm, R. (Hrsg.): Militarisierte Informatik, Marburg 1985.

Bilinski, A.: System Failure Models äs a Result of Design Inadequancy, in: Wise, J. A./Debons, A. (Eds.), Information Systems: Failure Analysis, NATO ASI Series F 32, Berlin 1987, 21 ff.

Bläsius, K. H./Siekmann, J. H.: Computergestützte Frühwarn- und Entscheidungssysteme, Informatik Spektrum 10/1987, 24 ff.
Blankenburg, E.: Politik der inneren Sicherheit, Frankfurt 1980.
Böckenförde, E.-W.: Gesetz und gesetzgebende Gewalt, 2. Aufl. Berlin 1981.
Böge, H.: Perspektiven der Verbrechensbekämpfung aus der Sicht des Bundeskriminalamts, KR 1982, 240 ff.
Bossel, H./Simon, K.-H. (Hrsg.): Computer und Ökologie, Karlsruhe 1986.
Breuer, R.: Computer-Schutz durch Sicherung und Versicherung, 2. Aufl., Neubiberg 1984.
Briefs, U.: Informationstechnologien und Zukunft der Arbeit, Köln 1984.
Brinkmann, H.: Das Verkehrsinformationssystem ZEVIS als Beispiel technischer Determinierung von Recht und Verwaltung, DÖV 1985, 889 ff.
Brödner, P.: Fabrik 2000. Alternative Entwicklungspfade in die Zukunft der Fabrik, 3. Aufl. Berlin 1986.
Brödner, P./Krüger, D./Senf, B.: Der programmierte Kopf, Berlin 1981.
Brunnstein, K.: Über Viren, Würmer und anderes seltsames Getier in Computer-Systemen: ein kleines "Infor-matik-Bestiarium", Angewandte Informatik 1987, 397 ff.
ders.: Gefahr von Viren, Wanzen und Würmern, CW v. 8.4.1988,12f.
ders.: Blindes Vertrauen in den Computer: Unterschätztes Risiko, BdW 2/1988, 8 ff.
Bruns, W.: Automatisierung im Kraftfahrtzulassungswesen, ÖVD-Online 11/1985, 85 ff.
Bschorr, Ch. K.: Computerkriminaltität - Gefahr und Abwehr, Düsseldorf, 1987.
Bull, H. P.: Datenschutz oder die Angst vor dem Computer, München 1984.
ders.: Wie können Juristen zur Technikfolgenabschätzung beitragen? RuP 1987, 131 ff.
Bundesbeauftragter für den Datenschutz: Dritter Tätigkeitsbericht, Bonn 1981.
ders.: Fünfter Tätigkeitsbericht, Bonn 1983.
Bundesminister für Forschung und Technologie: Informationstechnik. Konzeption der Bundesregierung zur Förderung der Entwicklung der Mikroelektronik, der Informations- und Kommunikationstechniken, Bonn 1984.
Bundesminister für das Post- und Fernmeldewesen (Hrsg.): Konzept der Deutschen Bundespost zur Weiterentwicklung der Fernmeldeinfrastruktur, Bonn 1984.
ders.: ISDN - die Antwort der Deutschen Bundespost auf die Anforderungen der Telekommunikation von morgen, Bonn 1984.
ders.: Mittelfristiges Programm für den Ausbau der technischen Kommunikationssysteme, Bonn 1986.
ders.: Chance und Herausforderung der Telekommunikation in den 90er Jahren, Bonn 1986.
Bundesregierung: Informationstechnik, Bonn 1984.
dies.: Regierungsbericht "Informationstechnik", 1. Fortschrittsbericht, Bonn 1985.
Bundesverband der Deutschen Industrie e.V. (BDI): Politische Weichenstellungen für den Informations- und Kommunikationsbereich, Köln 1988.
Bungers, D.: Expertensysteme in der GMD, Der GMD-Spiegel 3-4/86, 59 ff.
Burger, R.: Das große Computer-Viren Buch, 2. Aufl., Düsseldorf 1988.
Burkert, H.: OSIS und das Recht, GMD-Spiegel 1/86, 43 ff.
Busch, H./Funk,A./Narr, W. D./Werkentin, F.: Die Polizei in der Bundesrepublik, Frankfurt 1985.
Butti, W.: Insider-Delikte, IC-Management Zeitschrift 57,1988,121 ff.
Cerny, D.: Die US-Güteprüfung als Beispiel für Sicherheitsstandards, in: Gliss, H./Hentschel, B./Wronka, G. (Hrsg.), Datenschutzmanagement und Datensicherheit, Tagungsband der 9. DAFTA, Köln 1985(a), 255.

ders.: Vertrauenswürdige DV-Systeme. Das Berwertungsverfahren des US-Verteidigungsministeriums, in: Spies, P. P. (Hrsg.), Datenschutz und Datensicherung im Wandel der Informationstechnologien, Berlin 1985(b), 171 ff.
Charlier, M.: Ost-West-Handel unter CoCom-Bedingungen, CM 7/8/1987, 18 ff.
Chaos Computer Club: Die Hackerbibel, Hamburg 1986.
Chaum, D.: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, CACM 24 (1981), 84 ff.
ders.: Sicherheit ohne Identifizierung, DuD 1988, 26 ff.
Christaller, Th.: Künstliche Intelligenz - eine zukunftsorientierte Forschungsperspektive in der Informatik, GMD-Spiegel 3-4/86, 45 ff.
Clausen, L: Übergang zum Untergang, in: ders./Dombrowski, W.R. (Hrsg.); Einführung in die Soziologie der Katastrophen, Bonn 1983, 43 ff.
ders./Dombrowski, W. R.: Warnpraxis und Warnlogik, Zeitschrift für Soziologie 1984, 293 ff.
Cohen, F.: Computer Viruses - Theorie and Experiments, Proceedings of the 7th DoD/NBS Computer Security Conference, 31.8.1984, 240 ff.
Computer Security Service GmbH: SBA-Security by Analysis, Essen, o.J.
Coughran, E. H.: Computer Abuse and Criminal Law, La Yolla 1976.
Coy, W.: Geheime Schriften - Geheime Dienste, Kursbuch 66 (1981), 83 ff.
Dahmen, H.: Sicherheit für das Rechenzentrum, ÖVD-Online, 5/1985, 46 ff.
Dämmert, B.: Das Sabotagerisiko im Unternehmen wächst!, IO-Management Zeitschrift 57, 1988,128 ff.
ders.: Vorsicht: Wirtschaftsspione gehen um! IO-Management-Zeitschrift 57,1988, 287 ff.
Debons, A.: System Issues in Information System Failure, in: Wise, J. A./Debons, A. (Eds.), Information Systems: Failure Analysis, NATO ASI Series F 32, Berlin 1987,15 ff.
Denning, D. E.: Cryptography and Data Security, Reading 1982.
Dewdey, A. K.: Computer Recreations, A Core War Bestiary of Virus, Worms and other Threats to Computer Memories, Scientific America 252 (märz 1985), 14 ff.
258
Dhillon, B. S.: Human Reliabillty in Information Systems, in: Wise, J.A./Debons, A. (Eds.), Information Systems: Failure Analysis, NATO ASI Series F 32, Berlin 1987,183 ff.
Diebold/Dornier/Ikoss: Erstellung eines Landessystemkonzeptes, Stuttgart 1984.
Dierstein, R.: Computerviren, in: Gliss, H./Hentschel, B./Wronka, G. (Hrsg.), Datenschutzmanagement und Datensicherheit, Tagungsband der 9. DAFTA, Köln 1985(a), 87 ff. = KES 1985, 77 ff., 125 ff.
ders.: Computer Viruses, A New Threat to Computers and Computing, Vortrag auf der First European Conference on Computer Audit, Control and Security' in Oslo v. 15. bis 19.9.1986.
Dombrowski, W. R.: Soziologische Katastrophenforschung im Aufriß, in: Clausen/ders. (Hrsg.), Einführung in die Soziologie der Katastrophen, Bonn 1983,11 ff.
Dreyfuss, H. L/Dreyfuss, S. E.: Künstliche Intelligenz, Reinbek 1987.
Dropmann, H.: Datenvermittlungssystem Nordrhein-Westfalen, hrsg. v. Landesamt für Datenverarbeitung und Statistik, 6. Aufl. Düsseldorf 1987.
Droux, R.: Physische EDV-Sicherheit, in: Zimmerli, E./Liebl, K (Hrsg), Computermißbrauch - Computersicherheit, Ingelheim 1984,195 ff.
Dumitriu, P.: Die neuen Medien, Heidelberg 1985.
Dvorak, T.J.: Elektromagnetische Verträglichkeit - Eine Wachstumsgrenze der Funktechnik, NTZ 1987, 432 ff.

Ebbinghaus, K.: Das Turmbau-zu-Babel-Syndrom - Kommunikationsprobleme in der Durchführbarkeit von Großprojekten, in: Meyer-Abich, K. M./Ueberhorst, R. (Hrsg.), AUSgebrütet - Argumente zur Brutreaktorpolitik, Basel 1985, 232 ff.
Effelsberg, W./Fleischmann, A.: Das ISO-Referenzmodell für offene Systeme und seine 7 Schichten, Informatik Spektrum 9/86, 280 ff.
EG-Kommission: Grünbuch über die Entwicklung des Gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsendgeräte - KOM(87)290endg. (1987) - BT-DrS 11/930.
EG-Wirtschafts- und Sozialausschuß (Hrsg.): Europa und die neuen Technologien, Brüssel 1986.
Egli, H.: Grundformen der Wirtschaftskriminalität, Heidelberg 1985.
Eidenmüller, K.: Aufbau des Datenbestandes bei der Datenstelle der deutschen Rentenversicherung, Deutsche Rentenversicherung 1975, 224 ff.
Elling, A.v./Wunder, M.: Krebsregister. Erfassung als Politik, Hamburg 1986.
Enquete-Kommission "Künftige Kernenergie-Politik": Künftige Kernenergie-Politik, Zur Sache 1/80 und 2/80.
Enquete-Kommission "Neue Informations- und Kommunikationstechniken": Zwischenbericht, BT-DrS 9/2442 vom 28.3.1983.
Enquete-Kommission 'Technikfolgenabschätzung": Zur Institutionalisierung einer Beratungskapazität für Technikfolgen-Abschätzung und -Bewertung beim Deutschen Bundestag, BT-DrS 10/5844.
Erriksson, A.: SBA - eine Methode zur Verletz!ichkeitsanalyse, in: Gliss, H./Hentschel, B./Wronka, “G. (Hrsg.), Datenschutzmanagement und Datensicherheit, Tagungsband der 9. DAFTA, Köln 1985, 113 ff.
Evens, M./Orr, J.: Management Awareness of Computer Risks. A European Survey, o.O 1987.
Feigenbaum, E.A./McCorduck, P.: Die fünfte Computer-Generation, Stuttgart 1984.
Fetscher, I.: Terrorismus und Reaktion, Reinbek 1981.
Friedrichs, G./Schaff, A. (Hrsg.): Auf Gedeih und Verderb. Mikroelektronik und Gesellschaft, Reinbek 1984.
Fischer, K.: Telekommunikation, Raumordnung und regionale Strukturpolitik, Köln u.a. 1984.
Fölsing, A.: Die hohe Schule der Kryptographie, Kursbuch 66 (1981), 92 ff.
Gaede, E./Hammer, V./ Podesch, U.: Der Software-Life-Cycle, Darmstadt 1986.
Garstka, H./Schneider, J./Wiegand, K.-H.: Verwaltungsinformatik, Darmstad 1980.
Gergely, S.: Mikroelektronik, 3. Aufl. München 1985.
Gesellschaft für Reaktorsicherheit: Deutsche Risikostudie Kernkraftwerke, Hauptband, Köln 1979.
Gleich, A.v./Lucas, R./Schleicher, R.: Blickwende, Werkstattbericht Nr. 33, MAGS, Düsseldorf 1988.
Goebel, J.: Rechtliche Rahmenbedingungen für Zertifizierungsinstanzen in der elektronischen Kommunikation, GMD-SpiegeM/1988, 54 ff.
Goldberg, A.: President's Letter: Reliability of Computer Systems and Risks to the Public, CACM 28 (1985), 131.
Goos, G.: Perspektiven der Informations- und Kommunikationstechnik, GMD-Spiegel 3-4/86, 26 ff.
Gottschlich, M.: Der Mensch an den Grenzen der Technik, Gutachten für das Forschungsprojekt "Informatisie-rung der Gesellschaft: Verfassungsverträglichkeit und Verletzlichkeit des sozialen und politischen Systems", Hannover 1988.
Grobstudie: Führungs- und Einsatzmittel zur Kommunikation bei der Polizei, erstellt von der Polizetführungs-

akademie Münster, 1985.
Grupp, H./Hohmeyer, O./Kollert, R./Legler, H.: Technometrie, Köln 1987.
Guenther, F./Lehmann, H.: Verarbeitung natürlicher Sprache - ein Überblick, Informatik-Spektrum 9/86,162 ff. Guggenberger, B.: Das Menschenrecht auf Irrtum, München 1987.
Häfele, W.: Hypotheticality and the New Challanges: The Pathfinder Role of Nuclear Energy, Minerva 1974, 303 ff.
Haefner, K.: Die neue Bildungskrise. Lernen im Computerzeitalter, Reinbek 1985.
ders.: Mensch und Computer im Jahr 2000. Ökonomie und Politik für eine human computerisierte Gesellschaft, Basel u.a. 1984.
ders.: Grundrechtsentfaltung durch Nutzung der Informationstechnik, in: Roßnagel, A. (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft1 und Grundgesetz, Stuttgart 1989, S. 31 ff.
Hahn, U.: Expertensysteme als intelligente Informationssysteme. Konzepte für die funktionale Erweiterung des Information Retrieval, NfD 1985, 2 ff.
Haussier, R.: CoCom: Das Mißtrauen wächst, CM 9/1986,1.
Hammer, V.: TeleTrusT: Verletzlichkeit und Verfassungsverträglichkeit eines Konzepts für rechtssichere Transaktionen in der Informationsgesellschaft, DuD 8/1988, S. 391 ff.
ders.: Die künftige Informationsinfrastruktur und das Grundrecht auf Information, in: Roßnagel, A. (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, S. 49 ff.
ders./Roßnagel, A.: Die Informatisierung der Gesundheitsversorgung, in: Roßnagel, A. (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, S. 121 ff.
Harmsen, D.-M./Weiß, G.: Aspekte der Datensicherheit und der Informationssysteme im Bankensektor, Karlsruhe 1988.
Hase, F.: Das Recht auf "informationelle Selbstbestimmung", DuR 1984, 39 ff.
Hausmann, H.: Projekt Prometheus vereint Europas Automobilindustrie, Das Parlament v. 30.5.1987, 15.
Health and Safety Executive: Canvey: An Investigation of Potential Hazards from Operations in the Canvey Is-land/Turrock Area, London 1978.
Heidinger, J. L/Andrich, R.: Datensicherung im Unternehmen, Landsberg 1987.
Heilmann, W./Reusch.G.: Datensicherheit und Datenschutz, Wiesbaden 1984.
Heine, W.: Die Hacker, Reinbek 1984.
Henckel, D./Nopper, E./Rauch, N.: Informationstechnologie und Stadtentwicklung, Stuttgart u.a. 1984.
Hennings, R.-D./Müller, W.: Wie sicher sind Computer?, ÖVD-Online 3/1985, 75 ff.
Henns, K./Mikos, L: Personalinformationssysteme. Der große Bruder im Betrieb, Berlin 1984.
Herda, S.: Sicherheitsaspekte in OSIS, GMD-Spiegel 1/86,17 ff.
ders.: Authenticy, Anonymity and Security in OSIS, An Open System for Information Services, in: Spieß, P. P. (Hrsg.), Datenschutz und Datensicherung im Wandel der Informationstechnologien, Berlin 1985, 35 ff.
ders./Ryska, N.: Kryptographische Verfahren in der Datenverarbeitung, Berlin 1980.
Hofmann, K.: Die externe Revision als Teil der Abwehrmaßnahmen, in: Zimmerli, E./Liebl, K. (Hrsg.), Computermißbrauch - Computersicherheit, Ingelheim 1984, 307 ff.
Holl, F./Keil-Slawik, R.: Informationstechnologie und Militär am Beispiel von SDI, in: Internationale Bildstörung, Materialien zum gleichnamigen Forum vom 30.8. bis 8.9.1985 in Berlin.
Hondrich, K. O.: Zukunftsvisionen für die Industriegesellschaft, FAZ v. 30.4.1988.

Honnacker, H.: Polizeiliche Informationssysteme im Spannungsfeld von Datenschutz und wirksamer Strafverfolgung, DuD 1987, 218 ff.
Huber, J.: Telearbeit. Ein Zukunftsbild als Politikum, Opladen 1987.
Hug, K. H.: Es überlebe der Computer, Initiative für Abrüstung, TH Darmstadt 1985.
Husseiny, A. A./Sabri, Z. A.: Analysis of Human Factor in Operation of Nuclear Power Plants, Atomkerner-gie/Kerntechnik 1980,115 ff.
Informationstechnik 2000: Berichte der Arbeitskreise Industrieelektronik, Informationsverarbeitung, Mikroelektronik und Technische Kommunikation/Unterhaltungselektronik, o.O., 10.6.1987.
Innenminister des Landes Nordrhein-Westfalen: Bilanz und Perspektiven: Einsatz der Informationstechnik in der Landesverwaltung Nordrhein-Westfalen, Düsseldorf 1986.
ders.: Koordiniertes Programm für den Einsatz von Informationstechnik in der Landesverwaltung Nordrhein-Westfalen von 1987 bis 1990 - Aktionsprogramm Informationstechnik 1990, Düsseldorf 1987.
Innenminister des Landes Schleswig-Holstein: Schnee- und Hochwasserkatastrophen zum Jahreswechsel 1978/79 und im Februar 1979, Erfahrungsbericht der Landesregierung des Landes Schleswig-Holstein, Kiel 1979.
Jacobsen, H.-D.: Legitime Sicherheitsbedürfnisse weit überzogen, Blätter für deutsche und internationale Politik 1988,359 f.
Jahl, Gh.: SW-Engineering - eine notwendige Voraussetzung für DV-Sicherheit, in: Gliss, H./Hentschel, B./Wronka, G. (Hrsg.), Datenschutzmanagement und Datensicherheit, Tagungsband der 9. DAFTA, Köln 1985, 247 ff.
Jenkins, B. M.: New Modes of Conflict, Rand Corporation, R-3009-DNA, Santa Monica, 1983.
ders./Rubin, A.: New Vulnerabilities and the Aquisition of New Weapons by Nongovernment Groups, in: Evans, A./Murphy, J. (Eds.), Legal Aspects of International Terrorism, Lexington, Mass., 1978, 221 ff.
Jorissen, H.D./Kämpfer, S./Schulte, H. J.: Die neue Fabrik. Chance und Risiko industrieller Automatisierung, Düsseldorf 1986.
Jueterbock, D.: Zehn Jahre S.W.I.F.T.-Netzwerk - ein Meilenstein der Automation?, Die Bank 1988, 269 ff.
ders.: S.W.I.F.T. II für die 90er Jahre, Die Bank 1988, 329 ff.
Kabel, R./Strätling, Th.: Kommunikation per Satellit, Berlin 1985.
Kern, H./Schumann, M.: Das Ende der Arbeitsteilung? Rationalisierung in der industriellen Produktion, München 1984.
KES: KES-Sicherheits-Enquete, KES 1988, 148 ff.
Klebe, T./Roth, S.: Informationen ohne Grenzen, Hamburg 1987.
Klotz, U./Meyer-Degenhart, K.: Personalinformationssysteme. Reinbek 1984.
Koch, E./Vahrenholt, F.: Sebeso ist überall, aktualisierte Ausgabe, Frankfurt 1980.
Koenen, H.: Gefahr: Abstrahlung, KES 1985, 60 ff.
Kohl, H.: Europas Zukunft - Vollendung des Binnenmarktes 1992, Bulletin des Presse- und Informationsamts der Bundesregierung 1988, 333 ff.
Kommission "Zukunftsperspektiven gesellschaftlicher Entwicklung": Bericht, erstellt im Auftrag der Landesregierung Baden-Württemberg, Stuttgart 1983.
Krabel, E.: Die Viren kommen, computingtoday4/1987, 108 ff.
Kraus, J.: Selbstreproduzierende Software, Dortmund 1981.
Krückeberg, F./Oltmann, H.P./Ronneberger, F. (Hrsg.): Bürotätigkeit in der öffentlichen Verwaltung und technsicher Wandel, Regensburg 1983.
Kubicek, H.: Kabel im Haus - Satellit überm Dach, Reinbek 1985.
ders.: Soziale Beherrschbarkeit integrierter Fernmeldenetze, CM 10/1986, 28 ff.

ders.: Konzeptionelle Herausforderung bei der sozialverträglichen Gestaltung der sogenannten Neuen Infor-mations- und Kommunikationstechniken, in: Rolf, A. (Hrsg.), Neue Techniken Alternativ, Hamburg 1986, 81 ff.
ders.: Telematische Integration: Zurück in die Sozialstrukturen der Früh-Kapitalismus? in: Steinmüller, W. (Hrsg.), Verdatet und vernetzt, Frankfurt 1988, 51 ff.
ders./Rolf, A.: Mikropolis. Mit Computernetzen in die Informationsgesellschaft, 2. Aufl. Hamburg 1986.
Kuß, A.: Scanner-Daten bei der Datenerhebung für die Marktforschung, Thexis 3/1985, 12 ff.
Ladeur, K. H.: Der Vorbehalt des Gesetzes im Telekommunikationsrecht, Das Beispiel ISDN, ZfG 1987, 147 ff.
Lagadec, P.: Das große Risiko. Technische Katastrophen und gesellschaftliche Verantwortung, Nördlingen 1987.
Landesregierung Baden-Württemberg: Bericht der Kommission "Zukunftsperspektiven gesellschaftlicher Entwicklung", Stuttgart 1983.
Landesregierung Nordrhein-Westfalen: Studie für einen Telekommunikationsentwicklungsplan, Düsseldorf 1984.
Lange, P.: Cobol hatte das Pentagon zum Vater, Computerwoche v. 30.5.1986, 66 ff.
ders.: Kleincomputer knacken Codes kostengünstig, CW v. 5.9.1986, 40.
Leicht, A.: Computerspionage - Die "besondere Sicherung gegen unberechtigten Zugang" (§ 202a StGB), iur 1987, 45 ff.
Lenk, K.: Informationstechnik und Gesellschaft, in: Friedrichs, G./Schaff, A. (Hrsg.), Auf Gedeih und Verderb, Mikroelektronik und Gesellschaft, Reinbek 1982, 295 ff.
ders.: Gesellschaftliche Auswirkungen der Informationstechnik, NfD 1982, 200 ff.
Lenckner, Th.: Computerkriminalität und Vermögensdelikte, Karlsruhe 1981.
Levy, H. M.: Capability Based Computer Systems, Bedford, Mass., 1984.
Lewens, A.: A Study in Computer Abuse, Caulfield 1979.
Llebl, K.: Erscheinungsformen und beispielhafte Fälle, in: Zimmerli, E./Liebl, K. (Hrsg.), Computermißbrauch -Computersicherheit, Ingelheim 1984,25 ff.
ders. (Hrsg.): Betriebs-Spionage, Ingelheim 1987.
Lindner, R./Wohag, B ./Zeltwange, H.: Planen, Entscheiden, Herrschen. Vom Rechnen zur elektronischen Datenverarbeitung, Reinbek 1984.
Lischka, Ch./Diederich, J.: Gegenstand und Methode der Kognitionswissenschaft, GMD-Spiegel 2-3/87, 21 ff.
Litzenroth, H.A.: Neue Perspektiven f r die Panelforschung durch hochentwickelte Technologien, Jahrbuch der Absatz- und Verbrauchsforschung 1986, 212 ff.
Luhmann, N.: Ökologische Kommunikation, Opladen 1986.
ders.: Soziale Systeme, Taschenbuchausgabe, Frankfurt 1987.
Lutterbeck, B.: Sind Großsysteme der Informationstechnologien beherrschbar? in: Dey, G. (Hrsg.), Beherrschung der Informationstechnik - Verantwortung der Wissenschaft, Oldenburg 1985, 17 ff.
ders.: Das Restrisikoder Informationstechnologie: Gefahr für Freiheit und Demokratie?, in: Löwe, M./Schmidt, G./Wilhelm, R. (Hrsg.), Umdenken in der Informatik, Berlin 1987, 43 ff.
MANTO (Forschungsprojekt): Chancen und Risiken der Telekommunikation für Verkehr und Siedlung in der Schweiz (Leitung M. Rotach), Zürich 1986.
Marshall, E.: The Scourge of Computer Viruses, Science 240 (1988), 133f.
McLellan, V.: Computer Systems Under Siege, The New York Times v. 31.1.1988, 8.
McRobbie, M. A./Siekmann, J. H.: Artificial Intelligence: Persperctives and Predictions, Ms. Kaiserslautern 1987.
Meier, Gh.: Wirtschaftsdelikte im Bankengewerbe, Bern 1986.

Meyer-Tasch, P. C.: Der Weg vom Rechtsstaat zum Atomstaat wird gepflastert, in: Roßnagel, A. (Hrsg.), Recht und Technik im Stannungsfeld der Kernernegiekontroverse, Opladen 1984, 67 ff.
Mettler-Meibom, B.: Breitbandtechnologie. Über die Chancen sozialer Vernunft in technologipolitischen Ent-scheigungsprozessen, Opladen 1986.
dies.: Soziale Kosten der Informationsgesellschaft, Frankfurt 1986.
Meyer-Abich, K. M./Steger, U.: Mikroelektronik und Dezentralisierung, Berlin 1982.
Meyer-Abich, K. M./Schefold, B.: Die Grenzen der Atomwirtschaft, München 1986.
Mitsubishi Electronic Corporation: Mitsubishi Optical Disc Drive, München 1986.
Moreitz, M./Landwehr, R.: Der Sprung in die Zukunft. Zur Bedeutung der Informations- und Kommunikationstechnologie für die soziale Entwicklung, Weinheim 1985.
von zur Mühlen, R.: Computerkriminalität - Gefahr und Abwehrmaßnahmen, Neuwied 1973.
ders.: Integrierte Sicherheitskonzepte, in: Gliss, H./Hentschel, B./Wronka, G. (Hrsg.), Datenschutzmanagement und Datensicherheit, Tagungsband der 9. DAFTA, Köln 1985, 117 ff.
Müller, G.F.; "Computer-Viren" - Neue Gefährdungen der EDV?, DuD 1987, 482 ff.
Müller-Reißmann, K. F./Bohmann, K./Schaffner, J.: Kriterien der Sozialverträglichkeit, Teil D.: Vier Visionen zur Zukunft der Arbiet, ISP Hannover 1988.
Müller-Stoy, P.: Zukünftige Rechnerarchitekturen, in: Schulz, A. (Hrsg.), Die Zukunft der Informationssysteme, Heidelberg 1986,150 ff.
Nefiodow, L A.: Einführung in das Zukunftskonzept "Informationstechnik 2000", CM 3/1988, 20 ff.
Nötzold, J.: Die weitere technologische Spaltung Europas verhindern, Blätter für deutsche und internationale
Politik 1988, 360 ff.
Nora, S./Minc, A.: Die Informatisierung der Gesellschaft, Frankfurt 1979. Norman, A. R. D.: Computer Insecurity, London 1983.
Oberpostdirektion Frankfurt/M. (Hrsg): Leitfaden Telekommunikation, Frankfurt 1986. Opitz, R.: Roboter und künstliche Intelligenz auf dem Gefechtsfeld, Wehrtechnik 3/1986, 76 ff. Ortmann, G.: Derzwingede Blick. Personalinformationssysteme - Architektur der Disziplin, Frankfurt 1984. Otto, P./Sonntag, P.: Wege in die Informationsgesellschaft. Steuerungsprobleme in Wirtschaft und Politik, München 1985.
Pagalies, B.: Akzeptanz und Kontrolle der Datensicherheitsorganisation, in: Heilmann, W./Reusch, G. (Hrsg.), Datensicherheit und Datenschutz, Wiesbaden 1984,187 ff.
ders.: Sicherheit: Motivierte Anwender sind die besten Datenschützer, CW v. 22.8.1986, 7.
Papert, S.: Gedankenblitze, Reinbek 1985.
Parnas, D. L: Warum ich an SDI nicht mitarbeite, Informatik Spektrum 10/1987, 3 ff.
ders./Schouwen, A. J./Kwan, S. P.: Evaluation Standards for Safety Critical Software, Technical Report 88-220, Department of Computing and Information Science, University of Kingston, Ontario 1988.
Paul, W.: Programmsabotage, CR 1985, 52 ff.
Perrow, R. W.: Normale Katastrophen, Frankfurt 1987.
Perry, R. W.: Standhalten oder weichen? in: Clausen, L/Dombrowski, W. R. (Hrsg.), Einführung in die Soziologie der Katastrophen, Bonn 1983,103 ff.
Pfitzmann, A.: Die Infrastruktur der Informationsgesellschaft: Zwei getrennte Fernmeldenetze beibehalten oder ein wirklich datengeschütztes errichten? DuD 1986, 353 ff.
ders./Mann, A.: Technischer Datenschutz und Fehlertoleranz in Kommunikationssystemen, DuD 1987, 393 ff.

ders./Pfitzmann, B./Waidner, M.: Technischer Datenschutz in diensteintegrierten Digitalnetzen - Warum und wie? DuD 1986, 178 ff.
dies.: Weitere Aspekte fernmeldetechnischer Alternativen zum ISDDN, PIK 1988, 5 ff.
dies.: Datenschutz garantiert offene Kommunikationsnetze, Informatik Spektrum 1988,118 ff.
Pfitzmann, B./ Waidner, M./Pfitzmann, A.: Rechtssicherheit trotz Anonymität in offenen Systemen, CR 1987, 712 ff, 796 ff., 898 ff.
Piore, M. J./Sabel, C. F.: Das Ende der Massenproduktion, Berlin 1985.
Poerting, P.: Umfang und Struktur der Computerkriminalität, KR 1986, 595 ff.
Pohl, H.: Krimineller Mißbrauch von Mikrocomputern, DuD 1987, 80 ff.
Pordesch, U.: Informatisierung und neue Polizeistrategien, in: Roßnagel, A. (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, S. 87 ff..
Primio, F. di: Darstellung von "Wissen": Der Computer auf dem Weg zum "aktiven Buch", Der GMD-Spiegel 3-4/86, 55 ff.
Purton, P.: Photon kontra Elektron, Telematik-Magazin 2/86, 30 ff.
Rada, J.: Die Mikroelektronik und ihre Auswirkungen, Berlin 1983.
Radig, B.: Bildverstehen und künstliche Intelligenz, o.J., o.O.
Ratzke, D.: Handbuch der neuen Medien, Stuttgart 1984.
Rauch, G./Mertens, U.: Programmverifikation, CM 5/1986, 56 ff.
Raulefs, P.: Expertensysteme, in: Bibel, W./Siekmann, J. H., Künstliche Intelligenz - Frühjahrsschule Teisen-dorf, Heidelberg 1982, 61 ff.
Rebmann, K.: Sicherheit vor Datenschutz - nicht umgekehrt, KR 1982,153f.
Reese, J./Lange, B.-P.: Die Entwicklung der Informationsgesellschaft aus der Sicht der Bundesrepublik Deutschland, in: Hessische Landesregierung, Informationsgesellschaft oder Überwachungsstaat, Wiesbaden 1984, 13-284.
Reinermann, H./Fiedler, H./Grimmer, K,/Lenk, K. (Hrsg.): Organisation informationstechnik-gestützter öffentlicher Verwaltungen, Berlin u.a. 1981.
Reinermann H./Fiedler, H./Grimmer, K./Lenk, K./Traunmüller, R. (Hrsg.): Neue Informationstechniken - Neue Verwaltungsstrukturen? Heidelberg 1988.
Reusch, G.: Motiviertes Handeln für die Sicherheit der Datenverarbeitung erfordert Problembewußtsein, in: Heilmann, W./Reusch, G. (Hrsg.), Datensicherung und Datenschutz, Wiesbaden 1984, 71 ff.
Riesenhuber, H.: Stimulieren statt steuern, CM 12/1987, 34 ff.
Rihaczek, K.: OSIS - Open Shops for Information Services, GMD-Spiegel 1/86, 13 ff.
ders.: Datensicherheit amerikanisch, DuD 1987, 240 ff.
ders.: Ein Kompromißvorschlag zur Datenverschlüsselung, DuD 1987, 299 ff.
Ritchie, D.: Gehirn und Computer, Stuttgart 1984.
Rivest, R. L/Shamir, A./Adleman, L: A Method for Obtaining Digital Signatures an Public-Key Cryptosystems, CACM21 (1978), 120 ff.
Rolf, A. (Hrsg.): Neue Techniken alternativ. Möglichkeiten und Grenzen sozialverträglicher Technikgestaltung, Hamburg 1986.
Roos, J.: Das zentrale Verkehrs-Informations-System (ZEVIS) des Kraftfahrtbundesamtes, KR 1987, 321 ff.
Rosenberg, J./Abramson, D.: Monads PC - A Capability-Bases Werkstation to Support Software Engeneering, in: Proceedings of the 18th Annual Hawai International Conference on System Science, 1985, 222 ff.
Roßnagel, A.: Bedroht die Kernernergie unsere Freiheit? Das künftige Sicherungssystem kerntechnischer Anlagen, 2. Aufl. München 1983.
ders.: Grundrechtsprobleme des nuklearen Katastrophenschutzes, Zivilverteidigung 4/1983, 23 ff.

ders.: Radioaktiver Zerfall der Grundrechte? Zur Verfassungsverträglichkeit der Kernenergie, München 1984(a).
ders.: Rechtliche Risikosteuerung: Kritik und Alternativen, in: ders. (Hrsg.), Recht und Technik im Spannungsfeld der Kernenergiekontroverse, Opladen 1984(b), 198 ff.
ders.: Die rechtliche Fassung technischer Risiken, UPR 1986, 46 ff.
ders.: Großtechnik und Bürgerfreiheit, Referat zum 6. Rechtspolitischen Kongreß der SPD, Essen 20. -22.6.1986, in: Däubler-Gmelin, H./Adlerstein, W. (Hrsg.), Menschengerecht, Heidelberg 1986, 337 ff.
ders.: Die Verfassungsverträglichkeit von Technik-Systemen - am Beispiel der Informations- und Kommunikationstechnik, RuP 1987, 4 ff.
ders.: 'Verletzlichkeit der Gesellschaft" und "Verfassungsverträglichkeit11 als Maßstab für Techniksysteme, So-Tech-Rundbrief Nr. 5 (1987), 22 ff.
ders.: Die unfriedliche Nutzung der Kernenergie. Gefahren der Plutoniumwirtschaft, Hamburg 1987a.
ders.: Gesetzesvorbehalt für die Wiederaufarbeitung?, in: ders. (Hrsg.),: Rechtsprobleme der Wiederaufarbei-tung, Baden-Baden 1987(b), 17 ff.
ders.: Technik und Recht - wer beeinflußt wen?, in: ders. (Hrsg.): Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, S. 9 ff.
ders./Wedde, P.: Die Reform der Deutschen Bundespost im Lichte des Demokratieprinzips, DVB11988, 562 ff.
ders./Wedde, P./Hammer, V./Pordesch, U.: Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit künftiger Informations- und Kommunikationstechniken, Opladen 1989.
Rothkirch, C. v./Weidig, I.: Die Zukunft der Arbeitslandschaft, Beiträge zur Arbeits- und Berufsforschung 94.1 und 94.2, Nürnberg 1985.
Rügemer, W.: Neue Technik - Alte Gesellschaft, Silicon Valley, Köln 1985.
Rühl, H.-W./Dreissig, D./Kulas, W.: Sprachausgabe - die Aussteuerung von Phonen-Synthetisatoren, ntz-Ar-chiv 6/84, 243 ff.
Ruland, C.: Datenschutz in Kommunikationssystemem, Datacom 1/1987, 78 ff., 4/1987. 98 ff.; 9/1987.172 ff., 1/1988, 92 ff.
SARK: Bericht des Verwundbarkeitskomitees "Datenverarbeitung und die Verwundbarkeit der Gesellschaft", Stockholm 1979 (Deutsche Übersetzung).
Sawade, U./Schomburg, W.: Ausgewählte Probleme des Bundeszentralregisters, NJW 1982, 551 ff.
Schank, R. C./Childers, P. G.: Die Zukunft der künstlichen Intelligenz, Chancen und Risiken, Köln 1986.
Scharioth, J.: Prognosen - mehr als Spekulation, CM 12/1987, 20 ff.
Scheer, A.-W.: CIM. Computer Integrated Manufactoring. Der computergesteuerte Industriebetrieb, Heidelberg 1987.
ders.: Computer Integrated Manufactoring. Einsatz in der mittelständischen Wirtschaft, Berlin 1988.
Scheerer, S.: Gesetzgebung im Belagerungszustand, in: Blankenburg, E. (Hrsg.), Politik der inneren Sicherheit, Frankfurt 1980, 120 ff.
Scherer, J.: Telekommunikationsrecht und Telekommunikationspolitik, Baden-Baden 1985.
ders.: Netzintegration: Verfassungs- und verfahrensrechtliche Aspekte von Nutzungskonzepten und Folgeabschätzung, DBW 1987, 638 ff.
Schlomann, F.-W.: Ost-Spionage: Der Griff auf die Datenverarbeitung DSB 5/1987, 8 ff.
Schmidt, W.: Kompromittierende Abstrahlung, DuD 1987, 276 ff.
Schmidt, W.: Auf dem Risiko leben: Komplexität von MegaStrukturen, CM 3/1987, 22 ff.

Schmoch, U./Grupp, H./Mannsbart, W./Schwitalla, B.: Technikprognosen mit Patentindikatoren, Köln 1988.
Schnarrenberg, E./Büchner, C.: Tatwerkzeug Computer, Berlin 1986.
Schneider, H.: Die Güterabwägung des Bundesverfassungsgerichts bei Grundrechtskonflikten, Baden-Baden 1979.
Schönberg, V.: Organisatorische und softwaregeschützte EDV-Sicherheit, in: Zimmerli, E./Liebl, K. (Hrsg.), Computermißbrauch - Computersicherheit, Ingelheim 1984, 83 ff.
Schöneburg, E.: Computer-Viren - eine aktuelle Bedrohung für Computersysteme, Dornier Post 1/1987, 69 ff.
Schubert, I./Krebsbach-Gnath, C./Rothemund, M./Potthoff, P.: Chancen und Risiken des Einsatzes von Expertensystemen in Produktion, Verwaltung, Handwerk und Medizin, in: Materialien der Enquete-Kommission 'Technikfolgenabschätzung", Band III, Bonn 1987,1 ff.
Schuh, H.: Der programmierte Exitus, Zeit 17/1988, 86.
Schulz, A. (Hrsg.): Die Zukunft der Informationssysteme. Lehren der 80er Jahre, Berlin 1983, 380.
Schwarz-Schilling, Gh.: Die zukünftige Kommunikationsgesellschaft, Der Landkreis 1983, 380.
ders.: Neuordnung der Telekommunikation - Gesamtkonzept und Leitlinien, Bulletin des Presse- und Informationsamtes der Bundesregierung 1987, 781 ff.
Serie Bevölkerungsentwicklung: Die Zeit 1987, Nr. 23 ff.
Shoch, J./Hupp, J. A.: The "Worm" Programms - Early Experiences with Distributed Computation, CACM 3/1982, 172 ff.
Sieber, U.: Computerkriminalität und Straf recht, 2. Aufl. Berlin 1980.
ders.: Computerkriminalität und Strafrecht, Nachtrag zur 1. Aufl. Köln 1980.
ders.: Gefahr und Abwehr von Computerkriminalität, BB 1982,1465 ff.
Sieg, R.: Rechtliche Aspekte des Datenschutzes im Strafverfahrensrecht, in: Vollkommer, M. (Hrsg.), Datenverarbeitung und Persönlichkeitsschutz, Erlangen 1986.
Siekmann, J. H.: Künstliche Intelligenz, Kaiserslautern 1985.
Siemens AG: ISDN im Büro - HICOM, Berlin-München 1985.
dies.: Kommunikationstechnik. Bedeutung und Nutzen für heute und morgen, München o.J.
Simitis, S./Rydzy, W.: Von der betrieblichen Mitbestimmung zur staatlichen Administration, Baden-Baden
1984.
Simon, H./Kucher, E./Sebastian, K. H.: Scanner-Daten in der Marktforschung und Marktentscheidung, Zeitschrift für Betriebswirtschaft 1982, 555 ff.
Sneed, H. M.: Software-Qualitätssicherung, Köln 1983.
Söldner, F.: Neue kriminologische Erscheinungsformen der Betriebskriminalität, KR 1973, 1 ff.
Solarz, A.: Computer Technology and Computer Crime, Stockholm 1981.
Sonntag, P.: Die Zukunft der Informationsgesellschaft, Frankfurt 1983.
Soyka, J.: Computer Kriminalität, München 1986.
Späth, L: Wende in die Zukunft - Die Bundesrepublik auf dem Weg in die Informationsgesellschaft, Reinbek
1985. Spector, A. Z.: Software für Prozeßleittechnik, Spektrum der Wissenschaft, Sonderheft Computer-Software
1985, 88 ff. Spiers, J. D.: Failure of Business Information Systems, in: Wise, J. A./Debons, A. (Eds.), Information Systems:

Failure Analysis, NATO ASI Series F 32, Berlin 1987, 29 ff. Spoerl, J. R.: Stand und Aussichten der Wissensverarbeitung: Der Computer auf dem Wege zum Persönlichen
Assistenten, Der GMD-Spiegel 3-4/86, 68 ff.
Steinbach, W.: Back-up-Systeme für katastrophenbedingte RZ-Ausfälle - Bestandsanalyse, DuD 1985, 159 ff. Steiner, A.: Sicherheit und Revision in der Informatik, I0-Management-Zeitschrift 57 (1988), 50 ff, 100 ff., 118f.
und 192 ff. Steinert, H.: Die Reaktion der Öffentlichkeit auf den Terrorismus, in: Jugend und Terrorismus. Ein Hearign des
Bundesjugendkuratoriums, München 1979, 41 ff.
Steinke, W.: Kriminalität durch Beeinflussung von Rechnerläufen, NStZ 1984, 295 ff. Steinmüller, W.: Die zweite industrielle Revolution hat eben begonnen, Kursbuch 66 (1981), 152 ff. ders.: Soziale Technikgestaltung bei Informationstechnologien, in: Rolf, A. (Hrsg.), Neue Techniken Alternativ,
Hamburg 1986, 71 ff.
ders.: Technologiefolgen"ab"schätzung, CM 12/1987, 56 ff. ders. (Hrsg.): Verdatet und vernetzt, Frankfurt 1988.
Strampp, J. M.: Mehr Sicherheit mit 'Prometheus1, FR-Beilage zum 9.9.1987, 2. Stümper, A.: Die Wandlung der Polizei in Begriff und Aufgaben, KR 1980, 242 ff. ders.: Versuch einer sicherheitsanalytischen Bewertung der inneren Konfliktsituationen unserer Zeit, KR 1981,
76 ff. Szyperski, N./Grochla, E./Richter, U./Weitz, W. P. (Eds.): Assessing the Impacts of Information Technology,
Braunschweig-Wiesbaden 1983.
Toffler, A.: Die dritte Welle, München 1980. Turkle, S.: Die Wunschmaschine, Reinbek 1984.
Ueberhorst, R.: Normativer Diskurs und technologische Entwicklung, in: Roßnagel, A. (Hrsg.), Recht und Technik im Spannungsfeld der Kernenergiekontroverse, Opladen 1984, 245 ff.
Ullrich, 0.: Was spricht gegen Plastikhirne? Ursachen und Folgen der Maschinisierung des Lebens, Ms. Berlin 1988.
Ulrich, O.: Wissen ist Macht, Die Zeit 44/1987,13.
US-Department of Defense: Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, December 1985.
US-National Computer Security Center: Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, NCSC-TG-005, Version 1, July 1987.
Valk, R.: Beherrschbarkeit von Systemen und Verantwortungen des Informatikers, in: Kitzing, R./Linder-Kostka, U./Obermaier, F. (Hrsg.), Schöne neue Computerwelt, Berlin 1988,19 ff.
Vallee, J.: Computernetze. Träume und Alpträume von einer neuen Welt, Reinbek 1984.
Vester, H. G.: Die wiederkehrende Vergänglichkeit von Katastrophen, Universitas 1988, 745 ff.
Vogel, H.: Die Reform des sowjetischen Außenwirtschaftssystems erweitert das Kooperationsspektrum erheblich, Blätter für deutsche und internationale Politik 1988, 362f.
Volesky, K. H./Schölten, H.: Computersabotage, Sabotageprogramme - Computerviren, iur 1987, 280 ff.
Wagner, D.: Datensicherheit: Glaube an den Klapperstorch, ÖVD-Online 1985, 39.
Waidner, M./Pfitzmann, A.: Betrugssicherheit trotz Anonymität, DuD 1986,16 ff.
Waidner, M.//Pfitzmann, B/ Pfitzmann, A.: Über die Notwendigkeit genormter kryptographischer Verfahren, DuD 1987, 293 ff.
Webb, R. E.: The Accident Hazard of Nuclear Power Plants, Amherst, Mass. 1976.
Weck, G.: Datensicherheit, Stuttgart 1984.

Wedde, P.: Telearbeit und Arbeitsrecht, Köln 1986.
ders.: Verwaltungsautomation und Verfassungsrecht, in: Roßnagel, A. (Hrsg.), Freiheit im Griff, 'Informationsgesellschaft' und Grundgesetz, Stuttgart 1989, S. 67 ff.
Weese, E./Lessing, G.: Wie ein EDV-Sicherheits-Konzept im Unternehmen in Gang gesetzt wird - oder welche Hilfen der Datenschutzbeauftragte braucht, DSB 8/1987,17 ff.
dies.: Sicherung gegen Einbruch und Sabotage, KES 1987, 143 ff.
Weise, K. T.: Sicherheit: Motivierte Anwender sind die besten Datenschützer, CW v. 22.8.1986, 7.
Weizsäcker, C. F.: Die offene Zukunft der Kernenergie, in: ders., Diagnosen zur Aktualität, München 1979, 9 ff.
Wengel, J./Schneider, R.: Schadenspotentiale einer künftig vernetzten Produktion (CIM) am Beispiel des Maschinenbaus, Karlsruhe 1988.
Wernery, S.: Jüngste Hacker-Erfolge: Trojanische Pferde via Datenleitung, DSB 9/1987, 1 ff.
Wiener, E. L: Fallible Humans and Vulnerable Systems: Lessons Learned from Aviation, in: Wise, J. A./Debons, A. (Eds.), Information Systems: Failure Analysis, NATO ASI Series F 32, Berlin 1987, 163 ff.
Wiener, O.: Vom dialektischen zum binären Denken, Kursbuch 75 (1984), 12 ff.
Wiesel, G.: Computer-Kriminalität, Tatbestände und ihre strafrechtliche Verfolgung, data report 3/1973, 24 ff.
Wildemann, H.: Einführungsstrategien, Wirtschaftlichkeit und Wettbewerbsbedingungen von Just-In-Time, in: ders (Hrsg.), Just-In-Time, Tagungsberich zum 23./24.9.1987, Böblingen.
Winkler, M.: Sicherheitsmaßnahmen in Datennetzen der IBM Deutschland GmbH, Referat auf dem GDD/Count Symposium, Stuttgart 1985.
Winograd, T.: Software für Sprachverarbeitung, Spektrum der Wissenschaft, Sonderheft Computer-Software 1985, 48 ff.
Witten, I. A.: Computer (In)security: Infiltrating Open Systems, Abacus 4/1987, 7 ff.
Wolfram, S.: Software für Mathematik und Naturwissenschaften, Spektrum der Wissenschaft, Sonderheft Computer-Software 1985, 98 ff.
Wong, K.: Data Security - Watch out for the New Computer Criminals, DuD 1987, 133 ff.
ders.: Overview of Computer Disasters and Business Impact Review, DuD 1987, 352.
ders.: Security in Communication Networks, DuD 1987, 498 ff.
Zerbst, H.-U./Gottschlich, M.: Höhere Zuverlässigkeit für Mikrocomputer, Elektronik, Sonderpublikation
Com&Pro1983, 153 ff.
Zimmerli, E.: Computerkriminalität, KR 1987, 247 ff, 333 ff. ders./Liebl, H.: Computermißbrauch - Computersicherheit, Ingelheim 1984.

Abkürzungen

ACM	Association of the Computing Machinery
AI	Angewandte Informatik (Zeitschrift)
BAG	Bundesarbeitsgericht
BB	Betriebsberater (Zeitschrift)
BDI	Bundesverband der Deutschen Industrie
BdW	Bild der Wissenschaft (Zeitschrift)
BMFT	Bundesminister für Forschungs und Technologie
BMPF	Bundesminister für Post und Fernmeldewesen
BT-DrS	Bundestags-Drucksachen
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
CACM	Communications of the ACM (Zeitschrift)
CM	Computer Magazin
CR	Computer und Recht (Zeitschrift)
CW	Computerwoche (Zeitschrift)
DBP	Deutsche Bundespost
DBW	Die Betriebswirtschaft
DGB	Deutscher Gewerkschaftsbund
DÖV	Die öffentliche Verwaltung (Zeitschrift)
DSB	Datenschutz-Berater (Zeitschrift)
DuD	Datenschutz und Datensicherung (Zeitschrift)
DuR	Demokratie und Recht (Zeitschrift)
DVBl	Deutsches Verwaltungsblatt
DVR	Datenverarbeitung im Recht (Zeitschrift)
FAZ	Frankfurter Allgemeine Zeitung
FR	Frankfurter Rundschau
GG	Grundgesetz
GMD	Gesellschaft für Mathematik und Datenverarbeitung
Hrsg.	Herausgeber
ISDN	Integrated Services Digital Network
IBFN	Integriertes Breitband Fernmelde-Netz
iur	Informatik und Recht (Zeitschrift)
ISP	Institut für angewandte Systemforschung und Prognose
KR	Kriminalistik (Zeitschrift)
MAGS	Ministerium für Arbeit Gesundheit und Soziales NRW
Ms	Manuskript
mwN	mit weiteren Nachweisen

NfD	Nachrichten für Dokumentation
NRW	Nordrhein-Westfalen
RDV	Recht der Datenverarbeitung (Zeitschrift)
RuP	Recht und Politik (Zeitschrift)
SoTech	Programm des MAGS: Sozialverträgliche Technikgestaltung
TAZ	Tageszeitung
UPR	Umwelt- und Planungsrecht (Zeitschrift)
WAZ	Westdeutsche Allgemeine Zeitung
WSI	Wirtschafts- und sozialwissenschaftliches Institut des DGB
ZfG	Zeitschrift für Gesetzgebung

Glossar

Akustikkoppler	Datenübertragungseinrichtung für Fernsprechwege. Der Akustikkoppler übernimmt die Umwandlung von Tönen in digitale Signale und umgekehrt.
Back-Up-Rechenzentrum	Zur Absicherung gegen große Schäden beim Ausfall einer Computeranlage können Ersatz- oder Back-Up-Rechenzentren (BURz) eingerichtet werden. Diese werden unterschieden in: kalte BURz, wenn das Rechenzentrum erst im Notfall in Betrieb genommen wird; warme BURz, wenn das Rechenzentrum ständig betriebsbereit ist und im Notfall lediglich die Programme gestartet werden müssen; und heiße BURz, wenn die Programme ständig mitgerechnet werden bzw. parallel laufen und im Notfall lediglich auf dieses Rechenzentrum umgeschaltet werden muß.
Batch Verarbeitung	Stapelverarbeitung. Klassische Form der elektronischen Datenverarbeitung. Ein Auftrag wird zur Verarbeitung abgegeben, unabhängig vom Auftraggeber auf der Maschine gerechnet und das Ergebnis zurückgeliefert. Die Ergebnisse sind also erst zu einem späteren Zeitpunkt aktualisiert. Veränderungen an der Bearbeitung können nur verzögert vorgenommen werden.
Bildschirmtext (Btx)	Dienst der Deutschen Bundespost, mit dem Teilnehmer Mitteilungen austauschen, von Anbietern Informationen abrufen oder bei diesen Bestellungen aufgeben können.
CAD	Computer Aided Design. Hochentwickelte Form der graphischen Datenverarbeitung. CAD ermöglicht es, am Bildschirm rechnergestützt Arbeiten aus Bereichen wie Entwurf, Konstruktion, Entwicklung usw. durchzuführen.

Capability-Verfahren	In Rechner-Systemen kann ein Benutzer häufig undifferenziert auf eine relativ große Menge von Daten und Programmen (Objekten) zugreifen. Das moderne Konzept der Capabilities sieht für jeden Benutzer einen individuellen "Schlüssel" (Zugangsrechte) für die Nutzung von Objekten vor. Damit verfügt der Benutzer nicht mehr gleichsam über einen Generalschlüssel für jedes Objekt, sondern nur über spezielle Zugriffsbefugnisse für einzelne Dateien oder Programme, für die er zugriffsberechtigt sein soll. Die aufwendige Verwaltung der Zugangsrechte übernimmt der Rechner.
CIM	Computer Integrated Manufacturing. Systemintegration im industriellen Fertigungsbereich. Die einzelnen Bereiche einer Fabrik wie etwa Produktentwicklung, Anlieferung von Einzelteilen, innerbetrieblicher Transport, Planung, Modellbildung oder Simulation von Arbeits- und Prozeßabläufen werden in einheitliche Datenverarbeitungs-Konzepte integriert. CIM soll die umfassende und rationelle Steuerung aller verzahnten betrieblichen Abläufe ermöglichen.
Datei	Eine Datei ist eine Sammlung von Daten oder Programmen, die in einem Computersystemen gespeichert sind. Dateien sind auf Datenträgern magnetisch gespeichert und maschinenlesbar. Datenschutzrechtlich versteht man unter einer Datei eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen erfaßt und geordnet, nach anderen bestimmten Merkmallen umgeordnet und ausgewertet werden kann, ungeachtet der dabei angewendeten Verfahren (§ 2 Abs. 3 BDSG).
Datenbank	Datenbanken dienen zur Speicherung von Massendaten. Die einzelnen Daten werden in einer festen Zuordnung zueinander nach bestimmten Strukturen abgelegt (z.B. Name, Adresse, Religionszugehörigkeit). Aus Datenbanken können Informationen ähnlich wie aus Karteien abgefragt werden, allerdings können die Datensätze maschinell nach jedem beliebigen Kriterium sortiert werden. Beispiele für typische Datenbankanwendungen finden sich z.B. bei den Meldebehörden, bei der Polizei (Fahndung)und beim Statistische Bundesamt (Volkszählung).

Datex-L	Dienst bzw. Netz der Deutschen Bundespost, der Datenübertragung ermöglicht. Das Vermittlungsprinzip des Datex-L entspricht dem Telefonnetz, d.h. es wird nach einer eingegebenen Wahlinformation eine feste Verbindung zwischen rufendem und gerufenem Teilnehmer hergestellt.
Datex-P	Dienst bzw. Netz der Deutschen Bundespost, der Datenübertragung ermöglicht. Die vom Teilnehmer ausgesendeten Daten werden in Einheiten fester Länge ("Pakete") zerlegt und stückweise zusammen mit den Paketen anderer Verbindungen über dieselben Kanäle im Netz geleitet.
Diversifikation	Die (parallele) Nutzung verschiedener Computerfabrikate und/oder Programme für eine Aufgabe oder Anwendung. Im Vergleich zu einheitlichen Anlagen wird der (fertigungs- oder programmbedingte) Ausfall eines diversifizierten Computersystems unwahrscheinlicher.
Duplikate	Kopien von Daten oder Programmen. Wird eine Version vernichtet, kann mit dem Duplikat weitergearbeitet werden. Typischerweise werden Duplikate von Daten und Programmen auf Disketten, Magnetbändern oder Magnetplatten abgespeichert und getrennt von den Originaldatenträgern aufgewahrt.

Expertensystem	Expertensysteme sind eine spezielle Anwendungsforme der ->"Künstlichen Intelligenz". Sie sollen das vielfältige und oft unstrukturierte Wissen von Experten speichern und unabhängig von deren Anwesenheit zugänglich machen. Expertensysteme bestehen aus einer ->Wissensbasis, in der Fakten und Regeln eines Fachgebietes abgelegt sind, einer Inferenzmaschine, die Fakten und Regeln für eine bestimmte Aufgabe interpretieren und verknüpfen kann und einer Erklärungskomponente. Die Erklärungskomponente kann einem Benutzer Schlußfolgerungen zu den unterschiedlichsten Anfragen auf der Basis von Regeln und Fakten darlegen. Ein Expertensystem muß nicht für jede neue Aufgabe speziell programmiert werden, sondern kann sich die Lösungswege mit Hilfe der vorhandenen Regeln selbst erarbeiten. Bisher gibt es funktionierende Expertensysteme allerdings nur für sehr eingeschränkten Aufgabenbereiche, vorwiegend auf dem Gebiet technischer und naturwissenschaftlicher Fragestellungen. Die praktischen Einsatzformen sind derzeit noch sehr begrenzt.
Glasfasertechnik	Bauteile und Verfahren der Signalübertragung mittels Laserlicht, das in lichtleitende Fasern eingegeben wird.
Hacker	Personen, die über Datennetze unautorisiert auf fremde Systeme zugreifen. In der Regel werden für derartige Zugriffe Lücken im Sicherheitssystem genutzt oder fremde Paßwörter verwendet. Hackern liegt dabei nicht daran, Daten oder Systeme zu schädigen. Was zählt, ist zumeist die Fähigkeit, in fremde Rechner eindringen zu können.
Hardware	Die Hardware umfaßt alle "physischen" Komponenten eines Computersystems (z.B. Zentraleinheit, Speichergeräte, Bildschirme, Tastaturen, Drucker). Nicht zur Hardware gehören die Programme, Dateien und Daten (->Software).
IBFN	Integriertes Breitbandiges Fernmeldenetz (auch BIGFON = Breitbandiges Integriertes Glasfaser-Fernmeldeortsnetz genannt). Ein dienstintegriertes Netz, das künftig über eine Glasfasseranschlußleitung und Teilnehmerschnittstellen schmalbandige und breitbandige Kommunikationsdienste wie Fernsehen, Telefon bzw. Bildfernsprechen bereitstellt.

Information Retrieval	Das Heraussuchen bestimmter Informationen aus einer umfangreichen Menge gespeicherter Informationen (z.B. Literaturdokumente).
ISDN	Integrated Services Digital Network oder Integriertes Schmalbandiges Digitales Netz. Das ISDN stellt im Gegensatz zur herkömmlichen elektromechanischen und analogen Vermittlungstechnik computergesteuert digitale Verbindungen zwischen beliebigen Teilnehmern bereit. Über dieses Netz können verschiedene Dienste (Telefon und Datenübertragung) gleichzeitig angeboten und abgewickelt werden.
IuK-Technik	Informations- und Kommunikationstechnik. Dieser Begriff bezeichnet die Gesamtheit der zur Informationsbe- und -verarbeitung zur Verfügung stehenden Geräte und Anlagen, der zur Übermittlung von Daten dienenden Leitungs- und Verbindungsnetze sowie der verschiedenen Übermittlungsdienste.
Kryptoprozessoren	Ein Kryptoprozessor ist ein spezieller Rechner (Chip), der Zeichenfolgen ver- und entschlüsseln kann. Das ->Kryptoverfahren ist in die Hardware integriert, so daß der Verschlüsselungsvorgang sehr schnell abgewickelt werden kann.
Kryptoverfahren	Im Rahmen eines Kryptoverfahrens werden Zeichenfolgen (z.B. Texte) durch mathematische Verfahren und Funktionen so umgewandelt, daß der Sinn und Inhalt der Nachricht nicht mehr erkennbar ist (Verschlüsselung oder Chiffrierung). Dieser Vorgang ist umkehrbar (Entschlüsselung oder Dechiffrierung). Für die Umwandlung im Rahmen eines Kryptoverfahrens wird ein Schlüssel benötigt. Im Rahmen des sog. symmetrischen Verfahrens sind die Schlüssel für beide Vorgänge gleich und im Rahmen des sog. asymmetrischen Verfahrens werden zwei unterschiedliche, aber zusammengehörige Schlüssel verwendet.

Künstliche Intelligenz	Die "Künstliche Intelligenz" bildet ein Fachgebiet innerhalb der Informatik. Es werden Verfahren gesucht, durch die menschliche Fähigkeiten wie das Schlußfolgern von Experten (->Expertensysteme), das mathematische Beweisen, das Erkennen von Bildern, das Verstehen menschlicher Sprache oder das zielgerichtete Optimieren in beliebiger Umgebung auf Computern nachgebildet werden können. Diese Systeme sollen "lernfähig" sein und z.B. einen unbekannten Sachverhalt beim Benutzer abfragen und die dabei gewonnenen Informationen zur Wiederverwendung abspeichern können. Die gespeicherten Programme und Daten können in Form von Regeln dargestellt werden.
LCD-Bildschirm	LCD = Liquid Crystal Display oder Flüssig-Kristall-Anzeigen. Bildschirme auf LCD-Basis ermöglichen die Darstellung von Zeichen und Graphiken. Im Gegensatz zu herkömmlichen Kathodenstrahl-Bildschirmen sind sie extrem flach und energiesparend. Geringe Energiemengen reichen aus, um die Flüssigkristalle zu aktivieren und Bildschirmanzeigen zu erzeugen.
Log-Dateien	In Log-Dateien wird während der Betriebszeit eines Computersystems automatisch aufgezeichnet, wer welche Aufgaben und Aktionen abgewickelt hat. Auf einem separaten Datenträger wird gespeichert, wer wann mit dem System gearbeitet hat, welche Programme dabei aufgerufen, verändert und abgespeichert wurden und welche ->Dateien eingesehen und bearbeitet wurden. Log-Dateien dienen sowohl zur Rekonstruktion der Daten nach Programm- und Systemfehlern und -ausfällen als auch zur Überprüfung mißbräuchlicher Zugriffe und Nutzungen.
Offline-Verarbeitung	->Batch-Verarbeitung. Bei der Offline-Verarbeitung besteht keine direkte Verbindung zwischen dem Benutzer und dem zentralen Computer.

Online-Verarbeitung	Die inzwischen übliche Form der Datenverarbeitung. Der Bildschirmarbeitsplatz ist direkt mit dem zentralen Computer verbunden. Der Benutzer gibt Arbeitsaufträge direkt in das Datenverarbeitungssystem ein und erhält unmittelbar eine Antwort oder ein Ergebnis. Soweit er dazu die Kompetenz hat, kann der Benutzer unmittelbar auf die im System vorhandenen Programme und Daten zugreifen.
Operations-Research	Wissenschaftliche Disziplin, die die Entwicklung und Anwendung mathematischer Verfahren zur Analyse und Lösung komplexer Probleme zum Gegenstand hat (z.B. Optimierung betriebswirtschaftlicher Prozesse).
Optische Speicher	Bisherige Massenspeicher arbeiten auf der Basis von magnetischen Systemen, vergleichbar herkömmlichen Tonbändern. Neuere Entwicklungen führen hin zu optischen Platten, die bei hohem Speichervolumen beliebig oft wiederbeschrieben werden können. Sie sind leistungsfähiger und unempfindlicher als herkömmliche Speichermedien.
Paßwortverfahren	Im Rahmen eines Paßwortverfahrens muß der Benutzer sich gegenüber einem Computersystem zu erkennen geben. Mit Hilfe einer Zeichenfolge oder eines Namens (des Paßwortes) wird von einem Programm geprüft, ob der jeweilige Benutzer eine Zugangsberechtigung hat. Stimmt die eingegebene Zeichenfolge mit der verdeckt gespeicherten überein, wird der Zugang zum System eingeräumt. Anderfalls wird die Verbindung abgebrochen.
Plasma-Display	Mit Edelgase gefüllte Bildschirme, die durch Elektroden zum Leuchten gebracht werden und so die Darstellung von Zeichen und Graphiken ermöglichen. Wie die ->LCD-Bildschirme extrem flach aufgebaut.

Point Of Sale (POS)	Form der (bargeldlosen) Zahlung, die vorwiegend im Handel zum Einsatz kommen soll. Statt mit Bargeld zu bezahlen, muß nur eine Karte und eine persönliche Kennummer in das POS-Terminal eingegeben werden. Der Betrag wird direkt vom Konto des Kunden abgebucht. Beim POS sind sowohl ->Online Konzepte denkbar, die jederzeit eine Kontrolle der Liquidität des Kunden ermöglichen als auch ->Offline Systeme, die ein bestimmtes Kreditlimit des Kunden voraussetzen und auf die Übermittlung der angefallenden Buchungen via Datenaustausch angewiesen sind. Online-Verfahren sind vor allem wegen der anfallenden Leitungskosten relativ teuer.
Realtime-Verarbeitung	Form der Datenverarbeitung, bei der die Ergebnisse eines Verarbeitungsauftrages innerhalb sehr enger Grenzen verfügbar sein müssen. Zum Bereich der Realtime-Verarbeitung zählt z.B. die Prozeßsteuerung, die Maschienensteuerung und Bewegtbild-Computergraphiken.
Redundanz	Zusätzliche Sytem-Komponenten, die als Reserve für technische Störungen bereitgehalten werden. Dabei kann es sich um ->Duplikate von Daten und Programmen, um ->Back-Up-Rechenzentren oder um parallele Kommunikationsverbindungen handeln.
Rückkanal	Leitung oder Teil einer Leitung, über die bei einseitigen Verteildiensten (z.B. Kabelfernsehen) Rückmeldungen erfolgen können. Der Rückkanal kann z.B. genutzt werden, um zur Gebührenberechnung festzuhalten, welches Fernsehprogramm in einem bestimmten Haushalt gesehen wird.
Simulation	Die Abbildung natürlicher Vorgänge aller Art in Computerprogrammen. Ein realer Vorgang (Bevölkerungsentwicklung, Wetterbildung, Flug einer Rakete, Fahrverhalten eines Autos usw.) wird als mathematisches Modell dargestellt und in ein Programm gefaßt. Das Programm zeigt dann den Ablauf des Vorgangs als Modell auf dem Bildschirm oder in Graphiken an. Dabei können Risiken eines realen Vorgangs erkannt und in der Praxis vermieden werden. Durch die Erprobung und Veränderung der Ausgangsparameter (z.B. Richtung des Triebwerksschubs, Anordung der Bauteile einer Schaltung) können die Ergebnisse optimiert werden.

Software	Als Software werden die Programme von Computern oder Computersystemen bezeichnet. Sie bestimmen unabhängig von der ->Hardware die Eigenschaften und Funktionen eines Computers. Auf dem gleichen Computersystem können unter Nutzung verschiedener Programme z.B. Aufgaben der Buchhaltung, der Textverarbeitung oder der Konstruktion abgewickelt werden. Software läßt sich unterteilen in die zur Benutzung des Computers erforderliche Systemsoftware (z.B. das Betriebssystem), die zur Benutzung eines Computers unumgänglich ist und in die Anwendersoftware (z.B. Buchhaltungs- und Textverarbeitungsprogramme).
Software-Engeneering	Disziplin der Informatik, die sich mit der Entwicklung großer Programmsysteme befaßt. Es werden Prinzipien und Verfahren entwickelt, mit denen große Problemstellungen in kleine aufgeteilt werden können. Ziel ist die höhere Qualität und Zuverlässigkeit von Programmen, die verbesserte Prüfbarkeit und Wartbarkeit und ein effizientes Management von Entwicklerteams. Zur Unterstützung des Software-Engeneering werden "Werkzeuge" zur Systementwicklung auf Computern angeboten (CASE = Computer Aided Software Engeneering).
Superuser / Systemherr	Der Superuser/Systemherr ist zuständig für den gesamten Betrieb eines Computersystems. Er verfügt über die höchste Zugangspriorität, steuert das System, räumt neuen Benutzern Zugangsrechte ein und soll in der Lage sein, auftretende Schwierigkeiten sofort zu beheben. Um zu jedem Zeitpunkt eingreifen zu können, verfügt er über weitreichende Möglichkeiten. Er kann im Gegensatz zu anderen Benutzern auf alle Programmebenen zugreifen und bestehende Schutzvorkehrungen umgehen.
Telefax	Fernkopieren. Dienst der Deutschen Bundespost zur Übertragung von Bilddokumenten.
Telex	Dienst der Deutschen Bundespost zur Übertragung von Texten. Telex verfügt nur über einen beschränkten Zeichenvorrat (z.B. nur Kleinschreibung).
Teletext	Dienst der Deutschen Bundespost zur Übertragung von Texten zwischen Speicherschreibmaschinen sowie von und zu Computersystemen und Telexanschlüssen. Teletex verfügt über einen umfassenden Zeichenvorrat.

Textfax	Dienst der Deutschen Bundespost zur Übertragung von Dokumenten, die Texte und Bilder enthalten.
Temex	Fernmeß- und Fernwirkdienst der Deutschen Bundespost.
Virtuelle Maschinen	Simulation eines Computers vom Typ B auf einem Computer vom Typ A. Mit Hilfe der ->Software können auf einem Computer die Eigenschaften anderer Computer nachgeahmt werden. Auf diesem Weg wird es möglich, die Programme anderer Computersysteme auf beliebigen Rechnern zu benutzen.
Wissensbasis	Weiterentwicklung einer ->Datenbank. Auch als "Wissensbank" bezeichnet. Die Wissenbasis ist Grundlage für den Aussagebereich und die Qualität eines ->Expertensystems. Die Daten werden hier jedoch nicht in formaler Weise wie in einer Datenbank abgelegt, sondern in Form von Fakten und Regeln. Mit den Regeln können Beziehungen zwischen Fakten hergestellt oder Zusammenhänge zwischen Ereignissen beschrieben werden. Die Wissensbasis ermöglicht die einfache Darstellung vieler verschiedener Beziehungen zwischen unterschiedlichen Objekten.