7. Buckower Mediengespräche 2003: Das Vertrauen in die Medien - Orientierung im Wandel.
Kopaed 2004. S. 23-32. ISBN 3935686773

Günther Schatter

Elektronisch vermittelte Individual-Kommunikation und Vertrauen.

Elemente, Paradoxien und Bildungsfragen

Invention ist Intervention

Die Stichworte Medien und Vertrauen stehen zusammen meist für eine glaubwürdige Auswahl von Mitteilungen und ihrer massenmedialen Formung zu Sinngebilden.[1, 2] Die technische Seite der interpersonell genutzten elektronischen Medien – d. h. deren Substratfunktion [3] – wird im Zusammenhang mit dem Begriff des Vertrauens kaum betrachtet. Durch die technische Fokussierung geht es nicht mehr um publizistische, psychologische oder ethische Bewertungen der Mitteilungen, sondern um den Aspekt, der den eigenständigen Symbolhaushalt und den Werkzeugcharakter des Verbreitungsmediums betrifft.

Der Gebrauch von Kommunikationstechnologien vollzieht sich heute mit einer erstaunlichen Selbstverständlichkeit; das voraus gesetzte Vertrauen schwindet erst in Momenten von Fehlfunktionen und Enttäuschungen. Das im vergangenen Jahrzehnt eingeübte unbekümmerte Benutzen neuer Kommunikationsformen – wie die mit Sorglosigkeit verbundene Nutzung des Mobilfunks und des Internets – kann jedoch nicht länger als uneingeschränkt gegeben erwartet werden. Es zeigt sich, dass die Störanfälligkeit und Verwundbarkeit vieler Systeme im Zusammenhang mit der wachsenden Unzugänglichkeit der Technologie und halbkrimineller Geschäfts- und Nutzungspraktiken Dritter [4] die Grundeinstellung der Menschen heftig erschüttern und Skepsis hervorrufen kann. Vertrauen kann nicht verlangt werden, es muss geschenkt und genommen werden. Wenn um Vertrauen geworben wird, stellt sich sofort Verdacht ein – Überzeugungsversuche sind meist ungeeignet, das Reden darüber untergräbt Vertrauen nachhaltig. Zahlreiche Entwicklungen der Technologie, z. B. ihre überbordende Komplexität, haben zu Nachdenklichkeit und zur Einsicht geführt, dass nicht alle Produkte zwangsläufig zu Optimallösungen hinsichtlich wachsender Lebensqualität führen. In diesem Sinne orientiert sich die Forschungsförderung im Sinne von Sicherheit und Vertrauen teilweise auch neu. [5]

Technik geht aus vielen menschlichen Teilentscheidungen hervor. Sie erscheint dem Einzelnen im wachsendem Maße als unzugängliches Spezialwissen, als Wollen, Wissen und Können fremder Experten. Paradox ist daran, dass es einerseits aus Komfortgründen gern delegiert wird, andererseits will sich dem niemand schutzlos ausgeliefert sehen. In der hoch arbeitsteiligen Gesellschaft wird das Ideal selbstbestimmter Individuen durch die Forderung nach schier grenzenlosem Vertrauen, d.h. durch das Erbringen vielfältiger riskanter Vorleistungen, abgelöst. [6] Diese schwindende Vertrauensbasis innerhalb der kontinuierlichen Verstrickung in Expertensysteme wird in der Soziologie auch als "Entbettung" (disembeddedness) charakterisiert. [7] Die Benutzer durchschauen immer weniger das, von dem sie immer stärker in Abhängigkeit geraten. Das zuversichtliche Darauf-Bauen, dass Erwartungen nicht enttäuscht werden, scheint immer weniger Grund zu haben. Dies umso mehr, da es keinen Determinismus gibt, dass sich technische Neuerungen mit immanenter Folgerichtigkeit entwickeln und gesetzmäßig einen Weg wählen, zu dem es keine Alternative gibt. Jede

technische Lösung ist gleichzeitig eine kontingenter Eingriff in Natur und ein Präparieren neuer kultureller Handlungsmuster. "Jede Invention ist eine Intervention". [8]

Die stetig wachsende Komplexität der Alltagstechnik und ihre Einbindung in fest gekoppelte Großsysteme muss dennoch laufend reduziert werden, um für eine problemlose Anwendung immer wieder erneut anschlussfähig zu sein. Dies setzt auch stabiles Vertrauen in Kommunikationstechnik voraus, um vielfältige Handlungs-Potenziale zu erhalten; ein Leben mit einem Dauergefühl des Ausgeliefertseins und einem Übermaß an Ungewissheit ist auch gesellschaftlich gesehen keinesfalls wünschenswert. Dieses Vertrauen zweiter Ordnung als Konvention – neben einem "ontologischen Urvertrauen" [6] – ist beim Beispiel Technologie umso stabiler, je gründlicher das Wissen um ihre Möglichkeiten und Grenzen als auch von deren Risiken gegeben ist. Diese entstehen, wenn ein unerwartetes Ergebnis einer bewussten Entscheidung nicht auszuschließen ist. Durch Vernetzung wird die moderne alltägliche Kommunikationstechnik zu einer höchst komplexen Großtechnik. Auch dieses Großsystem erfordert Vertrauen als Bedingung. [9, 10]

Irren Maschinen?

Technische Individualkommunikation vollzieht sich inzwischen durchgehend digital; so sind alle Geräte mehr oder minder gut verpackte Computermaschinen der digitalen Signalverarbeitung geworden. Viele Probleme der Zuverlässigkeit sind von der Komplexität der verwendeten Software unmittelbar abhängig. Das Vertrauen in anonyme Technik wird über den Umweg Geräteentwickler letztlich aber zum personalen Vertrauen. Nicht Technik versagt, sondern die Unzulänglichkeit ihrer Entwicklung. Scheinbar ist kein anderes Industrieprodukt wie Software so anfällig gegen Fehlfunktionen, d.h. Nichterfüllen von Aufgaben, Verweigerung von Diensten, Missbrauch durch Dritte etc.

Die Ursachen hierfür sind überaus komplex:
- enormer Druck in Unternehmen, um in schneller Folge Systeme mit neuen Funktionen – damit oft unreif – auf den Markt zu bringen,
- sinkende Möglichkeiten zur Überschaubarkeit der Entwicklung von Großprojekten,
- stetig reduzierte Hardwarepreise, womit Speichervolumen scheinbar grenzenlos bereit steht,
- wachsende Vielzahl und Verschiedenartigkeit von Fehlerursachen, Nebenwirkungen und Seiteneffekten,
- überproportional steigende Kosten für Testverfahren,
- fehlende wissenschaftliche Methoden zur kompletten formalen Validierung insbesondere von Software,
- mangelhafte Produktspezifikationen – paradox, aber fehlerfreie Software muss nicht korrekt sein,
- ungenügender Einsatz von bewährten Methoden des Software Engineering, Programmierung wird gelegentlich als Kunst missverstanden etc. [11]

Der Aufwand zur Beherrschung komplexer Systeme durch Sicherheitsmaßnahmen und Tests, d. h. der Einsatz von Technik zur Kompensation von Technik, kann den Aufwand des Kernsystems weit übersteigen, vgl. Containments für Atomkraftwerke. Nur scheinbar paradox wirkt, dass Techniken zur Sicherung von Technologien wiederum Umsatz auf neuen Geschäftsfeldern versprechen. Für Verschwörungstheorien ist hier mancher Anlass gegeben. Die mathematische Komplexitätstheorie macht zwar für ausgewählte Aufgaben Aussagen über den algorithmischen Aufwand, die Eigenschaft Softwarekomplexität ist im Prinzip aber nicht messbar. Dieser Aufwand wird oft fälschlich mit dem

Codieraufwand (Anzahl Codezeilen bzw. Speichervolumen) gleich gesetzt. Er ergibt dennoch mangels Alternativen grobe Möglichkeiten zur Orientierung.

In den vergangenen zehn Jahren sind Anwendungsprogramme und Betriebssysteme bei oft wenig gesteigertem Funktionsumfang etwa um den Faktor 10 umfangreicher geworden. Ein bewährtes Entwickler-Motto "keep it small and simple" wird oft ohne Not zugunsten der Opulenz geopfert. So erfordert die Software eines Mobiltelefons heute etwa 200 000 Zeilen Quellcode, ein Standardbetriebssystem benötigt mehr als 10 Millionen Codezeilen. Erfahrungswerte zeigen: Für durchschnittliche Software gilt, dass sie 2,5 % Fehler enthält. Gute Programme, die aufwändiger getestet wurden, erreichen eine Fehlerquote von 0,1 ... 0,3 %. Für besonders hochwertige Software liegen die Fehler eine Größenordnung darunter. Ein Programmierer kann pro Woche ca. 100 Zeilen programmieren und elementar testen. Das bedeutet, dass diese Berufsgruppe sich in einem Vierteljahr nur ein bis zwei Fehler leisten darf, wenn gute Software erzeugt werden soll. So ist es nicht erstaunlich, dass der Hersteller des Systems Windows 2000 unmittelbar vor Markteinführung geschätzt hat, dass das Produkt noch ca. 63 000 Fehler enthält. [12] Die Schere einerseits zwischen Gerätekomfort (insbesondere der Mensch-Maschine-Schnittstelle) sowie der funktionellen Attraktivität und andererseits komplexitätsbedingter Unzuverlässigkeit öffnet sich weiter.

Die Software der Zukunft soll sich selbst reparieren können. Generatorprogramme werden aus Ablauftafeln Code erstellen, der einfach zu modifizieren sein soll. [13] Neue Paradigmen zum fehlerarmen Betrieb vor allem für Betriebssysteme von Mobiltelefonen wurden bereits eingeführt. Dennoch: Absolute Fehlerfreiheit wird noch lange Zeit ein unerfüllter Wunsch bleiben. Offenbar muss die Gesellschaft mit Fehlern bei High-Tech-Massengütern und den damit verbundenen Risiken langfristig leben lernen. In bestimmten Grenzen scheint Vertrauensverlust unausweichlich, der durch sorglosen Umgang aber keinesfalls vergrößert werden darf, um das gesellschaftliche Klima nicht weiter zu schädigen. Immerhin sind verschiedene Werte und Güter wie die Zusicherung der Privatsphäre und des Eigentums hier eng angeschlossen, wobei der Bedeutungsgewinn "unkörperlicher Sachen" wie Rechte, Geheimnisse, Know-how und elektronischer Gelder stetig wächst. [14] Gerde auf diesem Feld der Verunsicherung entdecken viele Unternehmen immer neue Geschäftsmöglichkeiten.

Vertrauensbrüche

Ein Ordnungsversuch geht hier von der Unterscheidung aus, ob
- Vertrauen zur technologischen Basis der Kommunikation entwickelt werden kann (a),
- Vertrauen zu weiteren individuellen Akteuren im Kommunikationssystem möglich ist (b) und
- das soziale Umfeld Vertrauen gegenüber dem Individuum aufbringt (c).

Mit diesen Fragen sind vielfältige Probleme der Achtung der Privatsphäre, der Persönlichkeits- und Eigentumsrechte und der informationellen Selbstbestimmung verbunden, die unter dem Stichwort Informationsschutz neu diskutiert werden. [15] Zur Eindämmung des Vertrauensverlustes verschiedener Art sind insbesondere Gegenstrategien zu verfolgen.

(a) Der Funktionsaspekt birgt zunächst kaum Besonderheiten, da sich Vertrauen hier überwiegend auf Gerätezuverlässigkeit reduziert, die kein spezifisches Problem der Kommunikationstechnik ist, allenfalls

Besonderheiten durch vergleichsweise enorme Komplexität aufweist. Skeptisches Verhalten, insbesondere für early adaptors, empfiehlt sich. Das Vertrauen zu drahtlosen Technologien ist jedoch getrübt, da bislang auch international noch keine belastbaren wissenschaftlichen Antworten zu gesundheitlichen Gefährdungen athermischer Art vorliegen. [16] Die Kritik an der Mobilfunknutzung durch Kinder verstärkt sich und es regt sich in der Bevölkerung zunehmender Widerstand gegen die Aufstellung neuer Sendemasten. [5] Forschung, Aufklärung und ggf. auch Warnung sind hier erforderliche vertrauensbildende Maßnahmen. Bürgerinitiativen, individuelle Verweigerung und symbolische Proteste sind als wesentliche Gegenstrategien verbreitet. [17, 18]

(b) Die Besonderheit der immanent soziotechnischen Kommunikationsgeräte liegt im Gegensatz zur Alltagstechnologie nicht einfach in deren Versagensmöglichkeiten, sondern in ihrer dramatischen Verletzlichkeit, im Mangel an Widerstandskraft gegen entfernte Attacken, im Potenzial ihrer missbräuchlicher Benutzung durch Dritte.

Die Bandbreite von Angriffen auf informationelle Rechte ist außerordentlich groß. Computerkriminalität, so der offizielle Begriff, beruht meist auf technisch bedingten Sicherheitslücken in Verbindung mit Sorglosigkeit beim Zugang und zeigt sich in Computerbetrug, Missbrauch von Kommunikationsdiensten und elektronischen Konten, Leistungserschleichung, Datenmanipulation, Computersabotage, Produktpiraterie, Fälschung und Täuschung im Zusammenhang mit Daten etc.. Die Methoden gründen meist auf dem Einschleusen von Softwarepartikeln, die in Symbiose oder parasitär existieren und mehr und mehr dazu in der Lage sind, sich zu modifizieren als auch zu vermehren, Strategien zu ändern und klandestin zu handeln, um damit ihr Aufspüren und Eliminieren zu erschweren. Auch die Benennung erinnert an autonomes Leben: Viren, Würmer, Wanzen, Käfer, Pferde... Hinzu kommt ein Arsenal von Belästigungen mit unerbetener Werbung (Spam) oder mit verunsichernden paranoiden Botschaften (Hoax). [19] Die Statistik weist für Computerkriminalität in den vergangenen Jahren ein exponentielles Wachstum aus, wobei vor allem in der Wirtschaft mit einer sehr hohen Dunkelziffer gerechnet wird, da die Strafverfolgung aus Furcht vor Ansehensverlust oft nicht eingeleitet wird. [20] Die Motive sind ebenso vielfältig wie die Attacken: Sie reichen von Neugier, über Suche nach Selbstbestätigung, Erfolg und Zerstörungslust bis zu Piraterie, Bereicherungssucht, Wirtschaftskriminalität und Spionage. Eine Beruhigung der Situation ist nicht in Sicht, da neue Gefahren durch die Verschmelzung von Internet, Mobiltelefonie (UMTS) und drahtlose Netze drohen. So gelten alle Sicherheitsmassnahmen des W-LAN-Standards 802.11 als überwindbar und bieten keinen verlässlichen Schutz für sensible Informationen. [21] Die Skepsis der Europäer gegen Internethandel speist sich aus solchen Quellen. [22] Im Umfeld der Ausforschung sind manipulierte Mobiltelefone bekannt geworden, wobei z. Z. noch kein Prüfwerkzeug existiert, mit dem die Firmware von Mobiltelefonen auf Manipulationen hin überprüft werden kann. [23]

Oft wird unter dem Vorwand der Aufklärung von der Medienindustrie über Computerkriminalität reißerisch berichtet oder im spielerischen Gewand auch unterschwellig nahezu Handlungsanleitung gegeben. [24, 25] Eine interessante Frage stellt sich, ob hier nicht über harmlose Neugier ein Weg zur Nachahmung führt:

> "Bei HACKER werden die Spieler als Softwehr-lngenöre von Konkurrenzunternehmen bei EiBiäM eingeschleust. Jeder will als erster an die brandneuen EiBiäM-Entwicklungen rankommen, die sicher in den Datenbanken des Großrechners liegen. Dazu muss natürlich erst einmal der Geheimcode geknackt werden. In jeder Abteilung liegt eine Geheimzahl. Kein Problem für einen Profi-Hacker." [26]

Die Rolle der Hacker ist deutlich von halbkriminellen Crackern oder Script Kiddies zu unterscheiden. [19] Hacker verstehen sich als heraus geforderte Avantgarde einer technikbegeisterten Hobby-Szene, die vor allem auf die Verwundbarkeit bzw. den Missbrauch von Informationssystemen hinweisen will. [27] Ihre Funktion als gesellschaftliches Frühwarnsystem ähnelt künstlerischen Strategien und sollte von der Gesellschaft anerkannt und

durchaus auch kritisch gefördert werden, da blindes Vertrauen, falsches Sicherheitsgefühl, Fehler in Standards und Systemen, Sorglosigkeit und Unrechtsbewusstsein in kreativer Form öffentlich gemacht werden. Viele Unternehmen haben das erkannt und stellen solche Aktivisten ein.

(c) Soziales Vertrauen wird durch die Informatisierung, Kommerzialisierung und Internationalisierung des Lebens zunehmend gefährdet. Die illegale Datenweitergabe, Veröffentlichungs- und Äußerungsdelikte, Adresshandel, Überwachung u.v.a.m. sind hier zu nennen. Arbeits-, Lebens-, und Konsumgewohnheiten werden immer umfassender erforscht. Hier findet Kommunikationstechnik Anwendung, die ungefragt zur Beeinträchtigung der Privatsphäre eingesetzt wird.

Im kommerziellen Bereich werden Daten über Personen häufig mit minimalen Versprechen eines Gegenwertes gesammelt, um daraus per data mining Verbraucherprofile für zielgerichtete Werbe- und Absatzstrategien zu erstellen. Die Einführung drahtloser Etiketten [28] (Radio Frequency Identifier RFID) hat Diskussionen und Proteste stark intensiviert. Misstrauen ist auch die Ursache des epidemieartigen Ausbreitens der Videoüberwachung in öffentlichen als auch in privaten Räumen. Personen unter Generalverdacht werden zu Objekten einer vertrauensbrechenden Observation. An Arbeitsplätzen gibt es zahlreiche Versuche und Möglichkeiten, die Computeraktivitäten und Gewohnheiten Abhängiger elektronisch zu kontrollieren [29]; in Institutionen werden universelle Zugangs-, Berechtigungs- und Zahlungssysteme eingeführt, die in einfacher Form Auskunft über individuelle Profile zulassen. Gegen diese Tendenzen wenden sich zunehmend Initiativen mit oft sarkastisch-ironischen Initiativen wie dem Big Brother Award [28] oder auch ambitionierte künstlerische Aktionen (Kartierung von Videoanlagen, Installationen, Inszenierungen etc.). [30]

Vertrauen und Bildung

Sicherheit und Vertrauen bilden einen engen Zusammenhang; aber Sicherheit steht oft im Widerspruch zu anderen vom Markt honorierten Produkteigenschaften wie Komfort, Funktionsreichtum, Benutzerfreundlichkeit, Kostengünstigkeit und Attraktivität. Sie erbringt im Fahrzeugbau oder in der Gebäudeautomatisierung Gewinn, da die materiellen Gefahren glaubhaft vermittelt werden können. Im IT-Bereich ist Sicherheit für Amateure überwiegend ein lästiges Übel; die Risikoreduzierung findet nur geringe Akzeptanz, sie klingt wie Verzicht, erinnert an puritanische Lebensweise. Der Markt hat hier wiederum Grenzen der Selbstregulierung, die an die Situation bei ökologischen Fragen erinnern.

In der öffentlichen Darstellung wird die konsumorientierte Medientechnik meist nicht verstehensorientiert, sondern umsatzfördernd präsentiert. Sie hat bislang zwar längst nicht so heftige Diskussionen wie in der Energie- oder Gentechnik hervorgerufen, dennoch können künftig durchaus komplizierte ethisch-moralische Fragen auf der Tagesordnung stehen, z. B. mit dem Einzug ubiquitärer roboterähnlicher Technik in den Alltag. Vernetzte Gebrauchsgegenstände erfahren eine Aufwertung durch Zuschreibung bzw. Simulation prä-intelligenter Eigenschaften. Technischen Einheiten wird zunehmend die Rolle von Sozialpartnern mit Möglichkeiten zu autonomen Entscheidungen zuwachsen. [31] Damit wandeln sich Situationen vom Systemvertrauen zum Personalvertrauen, ethisches Vorausdenken setzt hier nur zögernd ein. [32, 33] Bestrebungen der relativ neuen Arbeitsgebiete Computerethik und Philosophy of Information gehen überwiegend davon aus, dass neue technische Lösungen auch neue geisteswissenschaftliche

Denkansätze erfordern. [34] In der Kunst dominiert die groteske Darstellung unbeherrschbarer autonomer Systeme wie das Beispiel eines chaotisch reagierenden "smart house". [35]

Im Bildungssystem werden bislang Fragen von Unzuverlässigkeit und von Gefahrenpotenzialen der Informationstechnik kaum Aufmerksamkeit geschenkt. Im Vordergrund sowohl der Schul- als auch Hochschulbildung steht zumeist die formale Herausbildung von Bedien- und Programmierkompetenz, die ein "Verstehen" und "Beherrschen" der soziotechnischen Systeme suggerieren. Wissen um die Unvollkommenheit, Verwundbarkeit informationstechnischer Aggregate und den damit verbundenen technischen, juristischen und sozialen Fragen wird nicht erzeugt. Die Vermittlung latenter Gefahren, persönlicher Risiken, die Ausprägung ethisch-moralischer Grundsätze der Techniknutzung sollten unbedingt eine Grundlagenvermittlung der Zuverlässigkeitsthematik ergänzen, um Vertrauen würdigen zu können. Es ist an der Zeit, dass "das naive Verständnis heutiger Schulabgänger abgelöst wird, bei welchem die heutige Verherrlichung des goldenen Kalbs "High-Tech" durch eine risikobewusste Nutzung, z. T. auch Einschränkung oder Vermeidung riskanter Nutzungen abgelöst wird." [36] Dies ist Bedingung für erwachendes Sicherheits- als auch Unrechtsbewusstsein und Schlüssel für die skeptische Akzeptanz und Nutzung entwickelter Techniken, die dem Leben durchaus mehr Komfort und manche kleine Erleichterung sinnvoll verleihen können.

Literatur

1 Kohring, Matthias: Vertrauen in Medien - Vertrauen in Technologie. Akademie für Technikfolgenabschätzung Stuttgart, 2001. ISBN 3934629490.

2 Schweer, Martin: Der Einfluss der Medien. Vertrauen und soziale Verantwortung. Leske + Budrich Opladen, 2001. ISBN 3810030139.

3 Heider, Fritz: Ding und Medium. In: Pias, Claus u. a. (Hrg.): Kursbuch Medienkultur. S. 319-333. DVA Stuttgart, 2003. ISBN 3421053103.

4 Lienhard, Ulrich: Missbräuchliche Internet-Dialer – eine unbestellte Dienstleistung. Neue Juristische Wochenschrift. 56(2003) H. 50, S. 3592-3597.

5 Aktionsprogramm Informationsgesellschaft Deutschland 2006. www.bmbf.de/pub/aktionsprogramm_informationsgesellschaft_2006

6 Böhme, Gernot: Trau, schau, wem! Die Zeit (1998) H. 52.

7 Giddens, Anthony: Konsequenzen der Moderne. Suhrkamp Frankfurt a. M., 1995. ISBN 351858197X.

8 Zimmerli, Walter: Die Glaubwürdigkeit technisch-wissenschaftlicher Informationen. VDI-Verlag Düsseldorf, 1990. ISBN 3184009270.

9 Luhmann, Niklas: Vertrauen. Ein Mechanismus der Reduktion sozialer Komplexität. Enke Stuttgart, 1989. ISBN 343837739.

10 Luhmann, Niklas: Soziologie des Risikos. de Gruyter Berlin, 1991. ISBN 3110129396.

11 Knuth, Donald: The Art of Computer Programming I. Addison-Wesley Reading , 2000. ISBN 0201896834.

12 Windows 2000 betritt das RZ durch die Hintertür. Computerwoche (2000) H. 8 Seite 11 bzw. www.heise.de/newsticker/data/2000/cp-12.02.00-000/

13 Tristram, Claire; Fitzgerald, Michael: Software wird extrem. Technological Review (2003) H. 1, S. 34-45.

14 Beukelmann, Stephan: Prävention von Computerkriminalität. Peter Lang Frankfurt a. M., 2001. ISBN 3631378467.

15 Albers, Marion: Analyse und Neukonzeption des Rechts auf informationelle Selbstbestimmung. Habilitationsschrift Berlin, 2001.

16 König, Wolfram: Das Deutsche Mobilfunk Forschungsprogramm. 2. BfS-Fachgespräch "Forschungsprojekte zur Wirkung elektromagnetischer Felder des Mobilfunks" Berlin, 25.09.2003. www.bfs.de/elektro/papiere/rede_forschungsprogramm.html

17 Freiburger Appell 9.10.2002. www.elektrosmognews.de/Freiburger_Appell.pdf

18 Strahlenschutzgitter Weilersbach Juni 2003. www.elektrosmognews.de/Fotos/ssgweilersbach.jpg

19 Medosch, Armin; Röttgers, Janko (Hrg.): Netzpiraten. Die Kultur des elektronischen Verbrechens. Heise Hannover, 2001. ISBN 3882291885.

20 Polizeiliche Kriminalstatistik Computerkriminalität BKA Wiesbaden, 2002. www.bka.de/pks/pks2002/p_3_21.pdf

21 Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte. Bundesamt für Sicherheit in der Informationstechnik Bonn, 2003. www.bsi.de/literat/doc/drahtloskom/drahtloskom.pdf

22 Betrug und Fälschung. EU 2003. www.europa.eu.int/comm/internal_market/payments/fraud/index_de.htm#prevention-press

23 Manipulation von Mobiltelefonen. Bundesamt für Sicherheit in der Informationstechnik Bonn, 2003. www.bsi.bund.de/literat/doc/gsm/gsm.pdf

24 Russel, Ryan u. a.: Die Hacker-Bibel. mitp Bonn, 2002. ISBN 3826609263.

25 Vosseberg, Thomas: hackerz book. Franzis' München, 2003. ISBN 3772363466.

26 Hacker. Werbung für ein Spiel. www.fanfor.de/p_hacker.htm

27 Himanen, Pekka: The hacker ethic, and the spirit of the information age. Random House New York, 2001. ISBN 0375505660.

28 BigBrotherAwards. Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.. www.foebud.org/foebud/foebud.html bzw. www.bigbrotherawards.de/

29 Der Chef liest mit. www.heise.de/newsticker/data/jk-28.08.03-005/

30 Baumgärtel, Tilman: Ab heute wird zurückgefilmt. Die Zeit (2003) H. 37.

31 Kittler, Friedrich: Die Evolution hinter unserem Rücken. In: Kaiser, Gert u. a.: Kultur und Technik im 21. Jahrhundert. S. 221-223. Campus Frankfurt Main, 1993. ISBN 3593348055.

32 Christaller, Thomas: Robotik: Perspektiven für menschliches Handeln in der zukünftigen Gesellschaft. Springer Berlin, 2001. ISBN 3540427791.

33 Holeschak, Wolfgang: Vertrauen durch Partizipation. DUV Wiesbaden, 2000. ISBN 3824444267.

34 Floridi, Luciano: Two approaches to the Philosophy of Information. www.wolfson.ox.ac.uk/~floridi/pdf/tattpi.pdf

35 Pollesch, René: Smarthouse. Auszug in: ARCH+ (2001) H. 157, S. 66-71. Siehe auch: Schatter, Günther: Medium Gebaute Welt. In: 6. Buckower Mediengespräche. S. 55-64. Kopaed München, 2003. ISBN 3935686161.

36 Brunnstein, Klaus: Mit IT-Risiken umgehen lernen. In: Keil-Slawik, R.; Magenheim, J.(Hrg.): Informatikunterricht und Medienbildung. GI-Fachtagung 2001. S. 9-12. ISBN 3885793342.

37 Kubicek, Herbert: Die ganz normalen Risiken der Telekommunikationssysteme. In: /31/, S. 148-159.

38 Leiberich, Otto: Bedrohungsarten der Informationstechnologie. In: /31/, S. 160-166.