Die Infrastruktur der Informationsgesellschaft

Zwei getrennte Fernmeldenetze beibehalten oder ein wirklich datengeschütztes errichten?

Andreas Pfitzmann

Abstrakt: Seit 1984 kritisieren Herbert Kubicek et al. die Pläne der Deutschen Bundespost zur Errichtung eines zunächst schmalbandigen, später breitbandigen diensteintegrierenden Digitalnetzes unter den Aspekten Rationalisierungsfolgen, Datenschutzprobleme und Medienpolitik und schlagen vor, das im Teilnehmeranschlußbereich **analoge** Telefonnetz (im wesentlichen unverändert) beizubehalten und neu entstehende Dienste (wie bisher) in einem getrennten **digitalen** Datennetz zu vermitteln. Seit 1983 schlage ich die Errichtung **eines** überprüfbar datengeschützten **digitalen** Fernmeldenetzes vor, da die Pläne der Deutschen Bundespost notwendige technische Datenschutzmaßnahmen nicht vorsehen, sie sogar teilweise verhindern und damit dem Bürger unnötigerweise das „Recht auf informationelle Selbstbestimmung" nicht gewähren, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Ein Vergleich der beiden unabhängig entwickelten und technisch gegensätzlichen Vorschläge unter den Aspekten Rationalisierungsfolgen und Datenschutz ergibt, daß der Einfluß der Netzgestaltung auf die Rationalisierung gering, auf den erreichbaren Datenschutz jedoch groß ist. Der Vorschlag von Kubicek et al. ist bezüglich Datenschutz ungenügend, da die Weiterentwicklung der Technik ein Unterlaufen seines Datenschutzes in wenigen Jahren erlaubt.

Überprüfbarer Datenschutz in Fernmeldenetzen ist also nicht durch **Beibehaltung** des jetzigen technischen Zustands erreichbar, sondern nur durch seine gezielte **Weiterentwicklung** oder die (nicht realisierbare) weltweite Verhinderung jeglicher Weiterentwicklung der Technik.

1 Der Vorschlag von Herbert Kubicek et al.

In [KuRo_86, Kubi_85, Kubi_86] beschreiben Herbert Kubicek und Arno Rolf sehr umfassend die Gefahren, welche die Verwirklichung der Pläne der Deutschen Bundespost zur Errichtung eines breitbandigen, vermittelnden, **alle** Dienste integrierenden Digitalnetzes (IBFN, vgl. [ScSc_84, ScS1_84, ScSc_86]) hervorbrächte:

- Rationalisierungsfolgen für Arbeitsbedingungen und Arbeitsmarkt,
- Datenschutzprobleme in Betrieb und Gesellschaft,
- Auswirkungen von Fernsehen, Videofilmen und Computerspielen auf Kinder und Familien und
- Medienpolitische Unwägbarkeiten bezüglich des Privatfernsehens, Meinungsmonopolen und des Fortbestandes des gegenwärtigen öffentlich-rechtlichen Rundfunks.

Zur Begrenzung dieser Gefahren machen sie folgenden **Diskussionsvorschlag:**

Es werden **nicht** alle Dienste über ein Netz angeboten, sondern

- das analoge Telefonnetz bleibt im wesentlichen unverändert erhalten, insbesondere seine analoge Übertragungstechnik im Teilnehmeranschlußbereich und seine einfache und festverschaltete Vermittlungstechnik. Die Vermittlungszentralen enthalten so gut wie keinen Schreib-/Lesespeicher, damit kontrollierbar bleibt bzw. wieder wird, daß sie nicht zusätzlich Unerlaubtes bzw. Unerwünschtes tun, z.B. die Kommunikation der Teilnehmer auswerten.
- das integrierte digitale Text- und Datennetz (IDN) wird dem Bedarf entsprechend ausgebaut. Es integriert vor allem sämtliche Formen der Grundstücksgrenzen überschreitenden Bürokommunikation und erlaubt durch Einsatz von flexibel programmierbaren Rechnern als Vermittlungszentralen beliebige Protokollierung zur Erhöhung der Sicherheit (und damit auch der Überwachung).

Ich möchte diesen Diskussionsvorschlag der Beibehaltung zweier getrennter Fernmeldenetze im folgenden unter den von Kubicek und Rolf selbst gesetzten Aspekten **Rationalisierungsfolgen** und **Datenschutz** behandeln und dabei insbesondere aus technischer Sicht auf Plausibilität prüfen sowie mit den lediglich unter dem Aspekt Datenschutz entwickelten Alternativen vergleichen.

Zu den Auswirkungen von Fernsehen und medienpolitischen Unwägbarkeiten ist aus technischer Sicht nur anzumerken, daß jedes Fernmeldenetz, das qualitativ gutes Bildfernsprechen ermöglicht, auch die Übertragung von Privatfernsehen und Videofilmen erlaubt. Aus meiner subjektiven Sicht ist Bildfernsprechen eine sehr wünschenswerte Verbesserung des Fernsprechens, kann kommerzielles Privatfernsehen Meinungsmonopole stärken, schwächt als Hobby produziertes Privatfernsehen sie und ist Jugendschutz im Zeitalter der Videorecorder durch die Gestaltung von Fernmeldenetzen kaum beeinflußbar. Bevor ich mich den einer objektiven technischen Argumentation zumindest teilweise zugänglichen Aspekten zuwende, sei noch ein weiterer erwähnt: ob die Beibehaltung zweier getrennter Fernmeldenetze die Tendenzen zur Privatisierung der Fernmeldenetze fördere und ob dies ggf. wünschenswert sei, wird in [Kubi_85, WeSo_85, Kubi_86, KuRo_86 Seite 327] diskutiert.

2 Einfluß der Netzgestaltung auf Rationalisierung

Der Diskussionsvorschlag wurde von Kubicek und Rolf bezüglich Rationalisierungsfolgen folgendermaßen begründet:

> Durch die Integration aller Dienste in ein digitales Netz wird Datenfernverarbeitung und Textübertragung stark verbilligt, da kurzfristig alle Investitionen statt auf nur relativ wenige Nutzer des IDN technisch plausibel auf alle Nutzer des Telefonnetzes mit umge-

legt werden können und langfristig die erforderlichen Investitionen und Betriebskosten erheblich niedriger sind. Durch diese Verbilligung wird die bisher auf innerbetriebliche Prozesse beschränkte Rationalisierung auf Transaktionen zwischen Betrieben ausgeweitet, wodurch neue Formen technisch-organisatorischer Einheiten entstehen.

Die Auslagerung von Arbeitsplätzen in den privaten Bereich (Telearbeit in der Form von Heimarbeit und Werkverträgen) bzw. Vernichtung von Arbeitsplätzen durch „elektronische Kundenfernselbstbedienung" wird durch den Ausbau (Leistungssteigerung und Kostensenkung der Datenübertragung durch Digitalisierung und Diensteintegration) des fast alle Privathaushalte verbindenden Telefonnetzes für Unternehmen finanziell sehr lukrativ.

Diese neuen Formen technisch-organisatorischer Einheiten sowie diese Form von Telearbeit sind gesellschaftspolitisch aber nicht beherrschbar, da sie die bestehenden juristischen und sozialen Regelungsmechanismen (betriebliche Mitbestimmung, Arbeitnehmerschutzgesetze, Streikrecht) untergraben „und neue weder von den Inhalten noch von den Durchsetzungsmöglichkeiten her in Sicht sind" [KuRo_86 Seite 294], und unerwünscht, da sie menschliche Kontakte vermindern bzw. technisch einengen. Deshalb muß der von der Deutschen Bundespost geplante Ausbau des Telefonnetzes verhindert werden.

Im folgenden werde ich nicht diskutieren, daß meiner Meinung nach neue Formen technisch-organisatorischer Einheiten nach Weiterentwicklung des Rechts (z. B. überbetriebliche Mitbestimmung) und Telearbeit innerhalb eines „normalen" Arbeitsverhältnisses durchaus gesellschaftlich sinnvoll sein können und diese Fälle durch eine Verhinderung des Fernmeldenetzausbaus ebenfalls betroffen wären, sondern ich werde Kubiceks und Rolfs Begründung als Diskussionshypothese annehmen.

Meiner Meinung nach verkennen Kubicek und Rolf bei ihrem Diskussionsvorschlag, daß die Firmen gar nicht das (in ihrem Vorschlag durch Verhinderung von Diensteintegration teurere) IDN in die Wohnungen ihrer Mitarbeiter legen lassen müßten, sondern auch das sowieso vorhandene analoge Telefonnetz für Datenübertragung benutzen können: Über das analoge Telefonnetz können mit Hilfe synchroner Modems mindestens 4800 bit/s übertragen werden (vgl. [KuRo_86 Seite 94, Tane_81 Seite 95, 96]), so daß zum Übertragen einer DIN A4 Seite Text etwa 3 Sekunden nötig sind. Ist das Teilnehmerendgerät ein leistungsfähiger Mikrorechner mit Floppy disk und Bildschirmgerät sowie evtl. einem Drucker, so kann der Teilnehmer daran praktisch alle für Telearbeit zur Diskussion stehenden Arbeiten erledigen, indem die benötigten Daten entweder in seinen Mikrorechner geladen, lokal bearbeitet und nur die Ergebnisse zurückübertragen werden oder indem sein Mikrorechner als Terminal eingesetzt wird. Dann können beliebig große Datenmengen bei allerdings etwas längerer Antwortzeit und höheren Datenübertragungskosten (maximal 13,80 DM pro Tag bei 8 Stunden Arbeitszeit und einer Telefoneinheit zu je 0,23 DM alle 8 Minuten) im Dialog bearbeitet werden.

Die Hauptursache für die Ermöglichung von Telearbeit liegt also nicht in der billiger werdenden Übertragung, sondern den billiger und besser werdenden Heimcomputern.

Tendenziell gelten obige Überlegungen auch für Transaktionen zwischen Betrieben, wobei dabei die begrenzte Übertragungsgeschwindigkeit des analogen Telefonnetzes (praktische Grenze zur Zeit etwa bei 9600 bit/s, theoretische Grenze etwa bei 30000 bit/s [Tane_81 Seite 95, 96]) etwas störender ist, jedoch durch gleichzeitige Nutzung mehrerer Telefonkanäle, die von allen Mitarbeitern der jeweiligen Betriebe je nach Bedarf schnell wechselnd genutzt werden können, preiswerter umgangen werden kann.

Es ergibt sich als **Schlußfolgerung bezüglich der Rationalisierungsfolgen:**

Neue Formen technisch-organisatorischer Einheiten, Heimarbeit und Werkverträge lassen sich durch Verhinderung des **Ausbaus** der Fernmeldenetze nicht verhindern, sondern nur durch deren **Abbau**, da leistungsfähige Mikrorechner immer billiger werden.

Da meiner Meinung nach der Abbau des Telefonnetzes (oder seiner Dienste durch erhebliche Verteuerung oder gar ein Verbot von Modems) weder wünschenswert noch gesellschaftspolitisch durchsetzbar ist und auch der Verkauf billiger und leistungsfähiger Mikrorechner weder verhindert werden sollte noch kann, sehe ich keine **technische** Möglichkeit zur Verhinderung neuer Formen technisch-organisatorischer Einheiten, von Heimarbeit und Werkverträgen.

Entsprechendes gilt für die Fernmeldegebühren: da die Übertragung von Sprache genauso aufwendig wie Datentransfer mäßiger Geschwindigkeit ist, kann man Telearbeit nicht durch die Verhinderung von Gebührensenkungen, sondern nur über drastische Gebührenerhöhungen unrentabel machen, es sei denn, man verbietet nicht nur Modems, sondern auch Akustokoppler und installiert Überwachungsgeräte zur Unterscheidung von Sprache und Daten. Beides halte ich weder für empfehlenswert noch für gesellschaftspolitisch durchsetzbar.

Zur Verhinderung von negativen Rationalisierungsfolgen bleiben also nur juristische oder politische Mittel (Arbeitsrecht, vgl. [Müll_85], Besteuerung von beruflich genutzten Rechenanlagen bzw. Modems o. ä.).

3 Einfluß der Netzgestaltung auf den Datenschutz

Im Gegensatz zu Heimarbeit und Werkverträgen sind mißbräuchliche Erfassung, Speicherung und Verarbeitung personenbezogener Daten mit juristischen und polizeilichen Mitteln allein nicht einmal feststellbar, also auch nicht zu verhindern, so daß für den Datenschutz vorbeugende technische Maßnahmen unumgänglich sind [Pfit_83, PfPW_86]. Deswegen ist von größter Bedeutung, inwieweit der Diskussionsvorschlag von Kubicek und Rolf Datenmißbrauch be- oder verhindert.

Die in einem üblichen Fernmeldenetz anfallenden (personenbezogenen) Daten können in zwei Klassen, die eigentlichen Nutzdaten und die Vermittlungsdaten (z. B. Ziel- und Herkunftsadresse, Datenumfang und Zeit) eingeteilt werden [PfPW_86].

Wie Paul Baran schon 1964 erklärte, können die Nutzdaten (Sprache, Text, ...) durch Ende-zu-Ende-Verschlüsselung sehr gut geschützt werden, was kostengünstig jedoch nur in

einem digitalen Netz möglich ist [Bara_64]. Die Bandbreite eines analogen Netzes wird durch Digitalisierung sehr schlecht ausgenutzt, z. B. ist das Übertragen von digitalisierter Sprache auf einem analogen Fernsprechkanal nicht oder nur unter großen Qualitätseinbußen möglich. Außerdem sind pro Teilnehmeranschluß je ein zusätzlicher Analog-/Digital- und Digital-/Analogwandler nötig.

Das in analogen Netzen übliche Zerhacken (scrambling) der Signale erreicht bei weitem nicht den Schutz der Verschlüsselung und ist zudem erheblich teurer [DiHe_79 Seite 412].

Entsprechendes gilt bezüglich der Verbindungs-Verschlüsselung, die alle Daten (Nutz- und Vermittlungsdaten) des Fernmeldenetzes vor netzexternen Angreifern schützt [Bara_64, Denn_82, DaPr_84].

Auch fremde Geheimdienste sowie technisch fähige Amateure werden in der Lage sein, die Leitungen des analogen Fernsprechnetzes abzuhören. Neben den Gesprächsinhalten, die durch Menschen oder in Zukunft auch in größeren Mengen durch automatische Spracherkennung ausgewertet werden können, erfahren sie dabei die mitübertragenen Zieladressen, und sie können entweder über die Gesprächsinhalte oder über automatische Erkennung des Sprechers oder über die eindeutige Zuordnung von Leitungen oder Kanälen zu Teilnehmerendgeräten den Sender bestimmen.

Betreibt man, wie in Bild 1 dargestellt, das Fernnetz digital und benutzt man wenigstens in ihm Verbindungs-Verschlüsselung, so wird Massenüberwachung durch Abhören der Fernleitungen für fremde Geheimdienste und Amateure zwar unmöglich, aber umfangreiche Individual- und Gruppenüberwachung bleiben durch die leicht abhörbaren analogen Teilnehmeranschlußleitungen weiterhin möglich.

Die analogen Teilnehmeranschlußleitungen be- bzw. verhindern nicht nur sichere Verschlüsselung, sondern auch die in den letzten Jahren von David Chaum und mir entwickelten Maßnahmen zum Schutz der Vermittlungsdaten. Diese Maßnahmen schützen sowohl vor dem Netzbetreiber als auch vor den Urhebern (Herstellern von Hardware, Firmware, Systemsoftware und Anwendungssoftware sowie fremden Geheimdiensten mit Einflußmöglichkeiten auf diese Hersteller) von „Trojanischen Pferden" in den Vermittlungszentralen, die die Vermittlungsdaten an ihre Urheber weitergeben [PfPW_86]. Der Schutz durch diese Maßnahmen ist sogar vom Teilnehmer überprüfbar, so daß er nicht mehr darauf angewiesen ist, sich allein auf die Fürsorge eines Datenschutzbeauftragten zu verlassen, dessen Bestellung er nicht beeinflussen und dessen Verschwiegenheit er nicht überprüfen kann.

Wie in [PfPW_86, Chau_81, Chau_85, Pfi1_83, Pfit_84, Pfi1_85] beschrieben, setzen alle diese Maßnahmen ein digitales und, bis auf das MIX-Netz, ein zudem im Teilnehmeranschlußbereich sehr breitbandiges Fernmeldenetz voraus.

In Kapitel 3 von [PfPW_86] wurde die Gestaltung eines Datenschutz durch Anonymität garantierenden **breitbandigen** diensteintegrierenden Digitalnetzes, also eines möglichen **Endzieles** der Netzentwicklung, beschrieben. Hier soll zusätzlich skizziert werden, wie die getätigten Netzinvestitionen der Deutschen Bundespost (DBP) in Form der vorhandenen Gebäude, Kabelkanäle, Kabel, Verstärker und Vermittlungsstellen der heutigen Netze in einem **etappenweisen Ausbau** des Fernmeldenetzes genutzt werden können. Die Einführung der verschiedenen Dienste kann dabei etwa so schnell erfolgen wie von der DBP geplant, und es wird stets mehr Datenschutz garantiert als sowohl in der Alternative der Beibehaltung des analogen Fernsprechnetzes als auch bei der Realisierung der Pläne der DBP. Hierbei entsteht durch alternative Anwendung der Grundverfahren von Kapitel 2 von [PfPW_86] zunächst nur ein **schmalbandiges,** aber auch datengeschütztes Netz, dessen Nutzübertragungsleistung und Datenschutz mit jeder Ausbauetappe wächst.

Ein **schmalbandiges ISDN mit Schutz der Kommunikationsbeziehung durch MIX-Kaskaden** (MIXe mit fester Durchlauf-

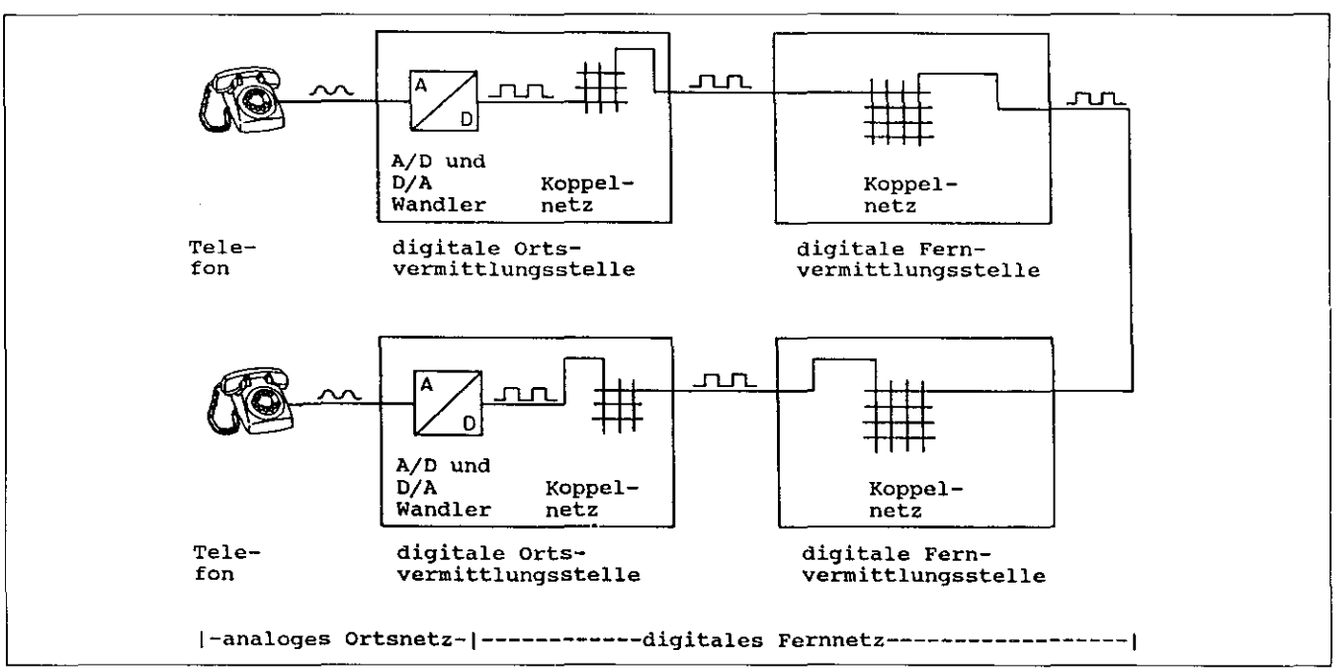

Bild 1 Hybrides Fernsprechnetz: Analoge Leitungen sind abhörbar, digitale bei Verschlüsselung nicht

reihenfolge) stellt die am schnellsten und vermutlich auch am preiswertesten flächendeckend vorzunehmende Modifikation des heutigen beziehungsweise für die nächste Zukunft von der DBP geplanten ISDN dar. Die bereits verlegten schmalbandigen Kupferdoppeladern werden wie von der DBP geplant nach Austausch der Verstärker etc. digital betrieben. Die Vermittlungszentralen können beliebig modernisiert werden, aber ergänzend zu der Datenschutz vernachlässigenden Postplanung werden MIXe eingerichtet.

Damit die Nachrichten nicht mehrmals oder auf Umwegen durch das öffentliche Netz laufen müssen, sollte dies entweder bei allen Fernvermittlungsstellen oder bei der weitaus größeren Menge aller Ortsvermittlungsstellen geschehen. Um diese MIXe einfacher realisieren und nutzen zu können, sollte es sich bei jeder der gewählten Vermittlungsstellen um eine Gruppe von MIXen handeln, für die eine feste Durchlaufreihenfolge festgelegt ist, sogenannte MIX-Kaskaden, und jede Nachricht sollte nur eine (im Fall der Fernvermittlungsstellen) bzw. zwei (im Fall der Ortsvermittlungsstellen) solcher Kaskaden durchlaufen (Bild 2).

Bei der Wahl der Länge der einzelnen Kaskaden hat man zwischen Datenschutz und Praktikabilitätsgesichtspunkten abzuwägen. Um etwa Telefon als Dienst mit Realzeitanforderungen ohne spürbare Verzögerung abwickeln zu können, dürfen (selbst bei Schalten anonymer Kanäle [Pfi1_85 Seite 25]) allerhöchstens 320 MIXe durchlaufen werden [Pfi1_85]. Je weiter man von dieser Grenze entfernt bleibt, desto geringer dürften wegen der größeren zulässigen Verzögerungszeit pro MIX die Kosten jedes MIXes sein, und natürlich verringert eine geringere Zahl an MIXen sowieso die Gesamtkosten, die über die normalen Fernmeldegebühren auf alle Netzteilnehmer umgelegt werden sollten. Auch die Teilnehmerstationen können bei der Verwendung von weniger MIXen billiger werden, da sie vor dem Senden nicht so oft verschlüsseln müssen. Daneben erlaubt es eine geringe Zahl von MIXen pro Kaskade am ehesten, diese auf separaten Grundstücken von verschiedenen Betreibern (z. B. Parteien, Kirchen, Datenschutzbüros, ...) auf verschiedenen Rechensystemen betreiben zu lassen, wie sich das für MIXe gehört. Vom Datenschutz her könnte z. B. die Verwendung von 5 bis 10 MIXen pro Nachricht reichen.

Werden die MIX-Kaskaden bei den Fernvermittlungsstellen errichtet, um mit einer möglichst geringen Anzahl und damit minimalen Kosten sowie einer möglichst kurzen Einführungszeit bis zu einer effizienten flächendeckenden Datenschutzversorgung auszukommen, müssen aus Datenschutzgründen auch Ortsgespräche zumindest über eine Fernvermittlungsstelle geführt werden.

Werden die MIX-Kaskaden, um eine Belastung des Fernnetzes durch Ortsgespräche zu vermeiden, bei den Ortsvermittlungsstellen errichtet, so sind erheblich mehr erforderlich. Dafür könnten in diesem Fall die Teilnehmerstationen, um ihr Senden zu verbergen, ständig bedeutungslose Nachrichten senden, die vom letzten MIX der Kaskade ihres Ortsnetzes weggeworfen werden, so daß es zu keiner Belastung der Netzteile kommt, die nur für anteilige Benutzung durch die einzelnen Teilnehmer ausgelegt sind. Es kann sogar nötig sein, künstlich Verkehr im Netz zu erzeugen, da die MIX-Kaskade bei Ortsvermittlungsstellen in kleineren Ortsnetzen sonst zu wenig Verkehr haben könnte, um Verkehrsbeziehungen zu verbergen.

Wo ein **schmalbandiges ISDN** vorhanden ist oder errichtet werden soll und die DBP mit dem **Koaxialkabelbaumnetz** zu ganz anderen Zwecken (Verteilung zusätzlicher Fernsehprogramme) im Teilnehmeranschlußbereich bereits ein breitbandiges Netz errichtet hat, kann dieses genutzt werden, um auch andere Datenschutzmaßnahmen als MIXe anzuwenden.

Am einfachsten zu realisieren ist dabei **Verteilung zum Schutz des Empfängers.** Dazu muß man nur einen kleinen Teil der Bandbreite digitalisieren. Mit 32 Mbit/s können etwa 500 Teilnehmer gleichzeitig 64 kbit/s empfangen (z. B. beim Telefonieren), so daß selbst bei Verdopplung der

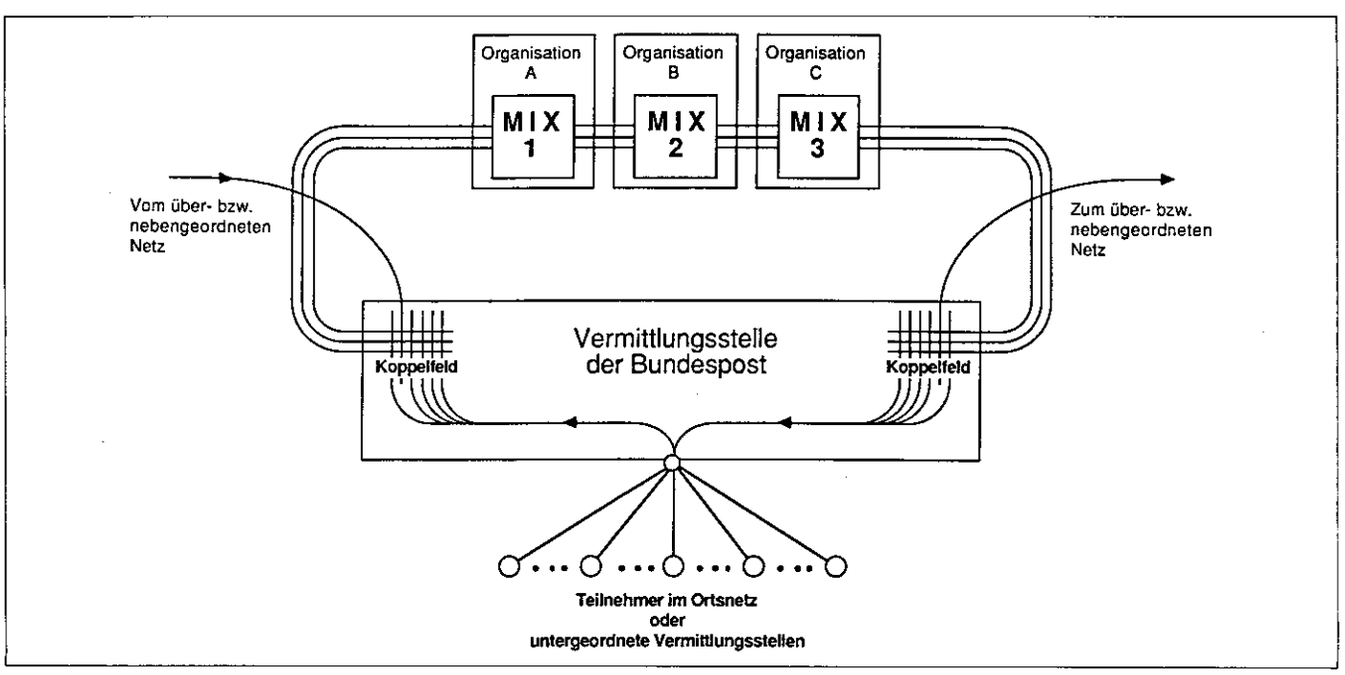

Bild 2 Vermittlungsstelle mit MIX-Kaskade

„Telefon"-nutzung auf maximal 20 % gleichzeitig die Information für je 2500 Teilnehmer über ein Koaxialkabelbaumnetz verteilt werden kann. Zur Adressierung und Geheimhaltung vor den zusätzlichen Empfängern siehe [PfPW_86]. Bei dieser Maßnahme müssen die Teilnehmerstationen weniger schnell verschlüsseln können als bei der Verwendung von MIXen. Können sie dies aber doch, so ergänzt sich diese Maßnahme auch gut mit evtl. vorhandenen MIXen in der Ortsvermittlungsstelle des Senders oder in einer Fernvermittlungsstelle.

Will man auch das **Senden** statt auf dem üblichen schmalbandigen ISDN **geschützt auf dem Koaxialkabelbaumnetz** durchführen, so hat man die Wahl zwischen einer dem RING-Netz nachempfundenen einfach zu realisierenden Maßnahme und der sehr wirkungsvollen des überlagernden Sendens (s.u.). In beiden Fällen entsteht damit in beschränkten Netzteilen ein **schmalbandiges Vermittlungs-/Verteilnetz,** das aber zumindest bei Realisierung der ersten Möglichkeit bei Diensten mit besonders geringen Leistungsanforderungen (z.B. elektronische Post) durch MIXe im Fernnetz ergänzt werden sollte. Hierzu muß wieder ein kleiner Teil der Bandbreite der Koaxialkabelbaumnetze digitalisiert werden, und die Verstärker müssen zur Verstärkung in beiden Richtungen erweitert oder ausgetauscht werden. Beides ist im Bereich „Lokaler Netze" seit langem üblich (vgl. WANGNET [Czaa_82, Elek_82]). Digitalisiert man 16 Mbit/s (wie bei WANGNET) in beiden Richtungen, so können selbst bei 20 % Nutzung gleichzeitig (s.o.) 1250 Teilnehmer über ein teildigitalisiertes Koaxialkabelbaumnetz mit schmalbandigen Diensten versorgt werden. Da jede Teilnehmerstation potentiell auf jeden der (Telefon-) Kanäle zugreifen kann und im Durchschnitt erheblich weniger als 20 % der Teilnehmer gleichzeitig „telefonieren", können den größten Teil des Tages sogar etliche Teilnehmer je einige 64 kbit/s Kanäle gleichzeitig nutzen.

Die weniger aufwendige Möglichkeit sind die dem RING-Netz nachempfundenen **Kollisionen verhindernden digitalen Baumnetze,** die aber wegen der nur beschränkten Eignung der Baumtopologie für Schutz durch physikalische Unbeobachtbarkeit der Leitungen nur geringeren Schutz bieten.

Die inneren Knoten des Baumnetzes werden mit Kollisionen verhindernden Schaltern [Alba_83, SuSY_84] ausgerüstet. Ein Kollisionen verhindernder Schalter schaltet einen aus Richtung der Blätter kommenden Informationsstrom nur dann in Richtung der Wurzel durch, wenn der Übertragungskanal in Richtung Wurzel frei ist. Bewerben sich mehrere Informationsströme aus Richtung der Blätter gleichzeitig um den freien Übertragungskanal in Richtung Wurzel, wählt der Kollisionen verhindernde Schalter genau einen zufällig aus und ignoriert die anderen.

Die Wurzel des Baumes sendet die von ihr durchgeschaltete Information in Richtung der Blätter usw.

Um das Senden einer Teilnehmerstation an den Blättern des Baumnetzes beobachten zu können, muß eine spezielle Leitung beobachtet werden (beim RING-Netz müssen für alle Stationen zwei spezielle Leitungen beobachtet werden); um das Senden einer Teilnehmerstation innerhalb des Baumes beobachten zu können, müssen alle ihre Eingänge und ihr Ausgang beobachtet werden.

Leistungsbewertungen [Alba_83, SuSY_84] attestieren diesen Baumnetzen ein hervorragendes Leistungsverhalten auch bei völlig unkoordiniertem Zugriff.

Aufwendiger, dafür aber von weit größerer Schutzwirkung ist **überlagerndes Senden auf den Koaxialkabelbaumnetzen.** Wie in [PfPW_86, Pfi1_85] beschrieben, ist ein Baumnetz ohnehin eine für überlagerndes Senden geeignete Topologie.

Für die ins Auge gefaßte Bandbreite von etwa 16 Mbit/s kann man zu recht hoffen, Pseudozufallszahlengeneratoren mit guten Sicherheitseigenschaften in wenigen Jahren auf einem Chip implementiert kaufen zu können. Pseudozufallszahlengeneratoren von etwa dieser Geschwindigkeit, allerdings mit umstrittenen Sicherheitseigenschaften, sind schon heute auf einem Chip erhältlich.

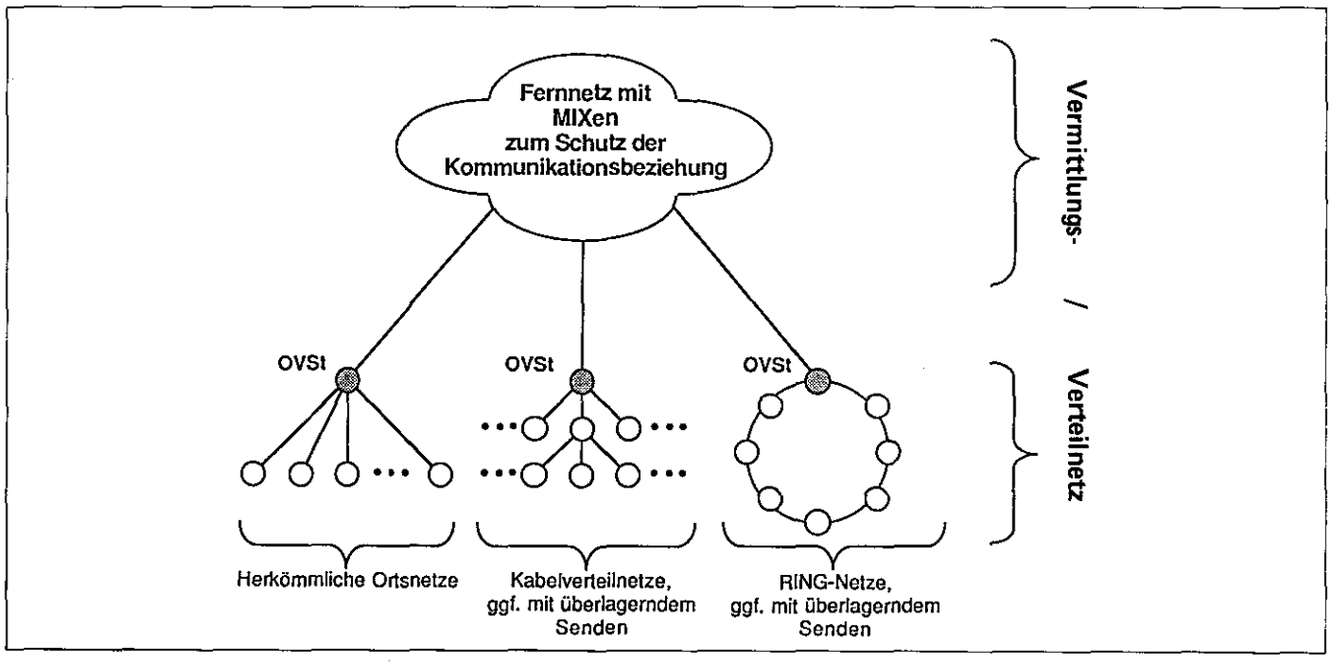

Bild 3 Integration verschiedener Datenschutzmaßnahmen in einem Netz

Der Ausbau dieses schmalbandigen zu einem **breitbandigen Vermittlungs-/Verteilnetz** sollte je nach Erschließungszustand und Besiedelungsstruktur des zu versorgenden Gebietes erfolgen (Bild 3). Sind im zu versorgenden Gebiet schon Kabelkanäle vorhanden oder handelt es sich um ein ländliches Gebiet und sind inzwischen genügend schnelle Pseudozufallszahlengeneratoren mit guten Sicherheitseigenschaften verfügbar, so dürfte es billiger sein, die Verkabelungsstruktur beizubehalten und die Verteilnetze mittels überlagerndem Senden zu realisieren, selbst wenn die Pseudozufallszahlengeneratoren noch teuer und die erforderliche Bandbreite des Verteilnetzes etwas höher ist, als die Verkabelungsstruktur zu ändern und RING-Netze als Verteilnetze einzusetzen. Sind im zu versorgenden Gebiet noch keine Kabelkanäle vorhanden und sind noch keine genügend schnellen Pseudozufallszahlengeneratoren mit guten Sicherheitseigenschaften verfügbar, sollten RING-Netze als Verteilnetze realisiert werden. Trifft keine der obigen Bedingungen zu und besteht unmittelbarer Handlungsbedarf, so sollte trotz erhöhter Kosten ringförmig verkabelt und bei ländlichen Gebieten überlagerndes Senden später nachgerüstet werden.

Im Laufe der Zeit kann der Umfang der durch überlagerndes Senden realisierten Verteilnetze vergrößert werden. Bis die Bundesrepublik vielleicht in sehr ferner Zukunft über ein Verteilnetz mit allen Kommunikationsdiensten versorgt wird, können die in früheren Ausbauetappen errichteten MIX-Kaskaden für schmalbandige Dienste zur Erhöhung des Datenschutzes über das durch die Verteilnetze gegebene Maß hinaus weiterbenutzt werden. Dies und die beschriebenen Etappen sprechen dafür, sie bei den Fernvermittlungsstellen zu errichten, da sie dann nach Errichtung eines Vermittlungs-/Verteilnetzes bequemer weiterbenutzt werden können und das Fernnetz sowieso ausgebaut werden muß.

Der in [KuRo_86 Seite 325] vorgeschlagene Datenschutz durch Vermeidung „softwaregesteuerter speicherprogrammierter Systeme" als Vermittlungszentralen stellt zwar eine Verbesserung gegenüber den Plänen der Deutschen Bundespost dar, ist aber bei weitem schlechter als obige Vorschläge, da

- die Teilnehmer den Datenschutz nicht selbst überprüfen können,
- die Gefahr der von Anfang an vorhandenen „Trojanischen Pferde" in den Vermittlungszentralen zwar etwas verringert wird, aber nicht gänzlich ausgeschaltet werden kann und
- Geheimdienste durch Installation von Zusatzgeräten oder Austausch von Festwertspeichern innerhalb der Vermittlungszentralen alle Vermittlungsdaten (und bei Unterlassung von Ende-zu-Ende-Verschlüsselung auch alle Nutzdaten) erfassen können, wenn immer dies eine Gesetzeslücke oder gar die gesetzgebende Mehrheit zur Kontrolle einer Minderheit mit anderen Interessen zuläßt.

Die Vermeidung „softwaregesteuerter speicherprogrammierter Systeme" als Vermittlungszentralen ist zwar als einzige Datenschutzmaßnahme unzureichend, zumal wenn analoge Teilnehmeranschlußleitungen verwendet werden. Sie stellt aber wie MIX-Kaskaden eine sinnvolle und preiswerte Ergänzung zum Konzept des Vermittlungs-/Verteilnetzes [PfPW_86] dar, da aus seinen Vermittlungszentralen alle Authentikations-, Abrechnungs- und Protokollierungsfunktionen in den Netzabschluß bzw. die Teilnehmerstation verlagert werden können, so daß keine laufenden Veränderungen seiner Vermittlungszentralen nötig sind.

Natürlich finden alle ein Fernmeldenetz gestaltenden technischen Datenschutzmaßnahmen ihre Grenze dort, wo es jemand gelingt, ein „Trojanisches Pferd" im Netzabschluß eines Teilnehmers oder seiner Teilnehmerstation unterzubringen oder ihn direkt zu beobachten. Gegen ersteres hilft nur die freie Wahl zwischen verschiedenen Bezugsquellen, deren Produkte nach öffentlichen Entwürfen unter öffentlicher Kontrolle hergestellt werden. Letzteres ist zur Individualüberwachung weniger Personen bei dringendem Tatverdacht sogar wünschenswert.

Es ergibt sich als **Schlußfolgerung bezüglich des Datenschutzes:**

> Die Beibehaltung des analogen Telefonnetzes ist für den Datenschutz besser als die gegenwärtigen Pläne der Post zur Digitalisierung und Diensteintegration, sofern die Teilnehmer so unvorsichtig sind, keine Ende-zu-Ende-Verschlüsselung zu betreiben, oder Ende-zu-Ende-Verschlüsselung durch (bisher) fehlende Standardisierung nur innerhalb geschlossener Benutzergruppen möglich ist und die Post so fahrlässig ist, keine Verbindungs-Verschlüsselung vorzunehmen.
>
> Die Beibehaltung des analogen Telefonnetzes ist aber bezüglich des Datenschutzes weit schlechter als unter Berücksichtigung des Datenschutzes entworfene Digitalnetze, die insbesondere als diensteintegrierendes Netz ein günstiges Preis/(Leistungs+Schutz)-Verhältnis erwarten lassen.
>
> Das Festschreiben des analogen Telefonnetzes schreibt leider nicht einmal dessen jetzigen (aus meiner Sicht sehr mangelhaften) Datenschutz fest, sondern der technische Fortschritt, dessen sich ein Angreifer bedienen kann (z.B. automatische Sprecher- und Spracherkennung), untergräbt ihn von Jahr zu Jahr mehr.

4 Fazit

Will man in Zukunft auf Datenschutz bei Kommunikation nicht verzichten, spitzt sich alles auf zwei Alternativen zu:

- Leben ohne technische Zweiwegkommunikation, d.h. Verzicht auf ein Fernmeldenetz (auch auf das Telefonnetz) bis in die Privatwohnung, oder
- Leben mit sehr stark technisierter, dafür aber überprüfbar datengeschützter Zweiwegkommunikation (vgl. [PfPW_86]).

Da Maßnahmen zur Begrenzung der Datensammelmöglichkeit von Konzernen, Banken und Behörden über Bürger [Chau_85, WaPf_85, PPW_86, BüPf_86] ein datengeschütztes Netz zur anonymen Kommunikation zwischen Bürger und Konzern, Bank bzw. Behörde benötigen und ich auch private technische Kommunikation für nötig halte, empfehle ich die Realisierung der zweiten Alternative.

Für Kritik und fruchtbare Diskussionen danke ich Dr. Klaus Echtle, Prof. Winfried Görke, Prof. Herbert Kubicek, Michael Kühn, Birgit Pfitzmann, Prof. Detlef Schmid und Michael Waidner.

Stichwörter: Telearbeit, Rationalisierungsmöglichkeiten, Technischer Datenschutz, überprüfbarer Datenschutz, (Un-)Beobachtbarkeit, Anonymität, Verhinderung der Datenerfassungsmöglichkeit, Individualüberwachung, Massenüberwachung, Fernmeldenetze, IDN, ISDN, IBFN, Trojanische Pferde, Verkehrsanalyse, Vermittlungssysteme, Nutzdaten, Vermittlungsdaten, Verbindungs-Verschlüsselung, Ende-zu-Ende-Verschlüsselung, MIX-Netz, Verteilung, überlagerndes Senden, RING-Netz, Vermittlungs-/Verteilnetz, Baumnetz

Literatur

[Alba_83] A. Albanese: Star Network With Collision-Avoidance Circuits; The Bell System Technical Journal (BSTJ) Vol. 62, Nu. 3, March 1983, Seite 631 bis 638

[Bara_64] Paul Baran: On Distributed Communications: IX. Security, Secrecy, and Tamper-Free Considerations; Memorandum RM-3765-PR, August 1964, The Rand Corporation, 1700 Main St, Santa Monica, California, 90406; Reprinted in: Lance J. Hoffman (ed.): Security and Privacy in Computer Systems; Melville Publishing Company, Los Angeles, California, 1973, Seite 99 bis 123

[BüPf_86] Holger Bürk, Andreas Pfitzmann: Value transfer systems enabling security and unobservability; IFIP/Sec. '86, Proceedings of the Fourth International Conference and Exhibition on Computer Security, Monte Carlo, 2. bis 4. Dezember 1986, A. Grissonnanche (ed.), North-Holland, 1986

[Chau_81] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM Vol. 24, Nu. 2, February 1981, Seite 84 bis 88

[Chau_85] David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM Vol. 28, Nu. 10, October 1985, Seite 1030 bis 1044

[Czaa_82] Franz R. Czaak: Konzepte eines lokalen Netzwerks; Kommunikationstechnologien, Neue Medien in Bildungswesen, Wirtschaft und Verwaltung, Helmut Schauer, Michael J. Tauber (eds.), Schriftenreihe der Österreichischen Computer Gesellschaft Band 17, R. Oldenbourg Wien München 1982, Seite 341 bis 359

[DaPr_84] D. W. Davies, W. L. Price: Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer; John Wiley & Sons, Chichester, New York, 1984

[Denn_82] Dorothy E. Denning: Cryptography and Data Security; Addison-Wesley Publishing Company, Reading, Mass.; 1982

[DiHe_79] Whitfield Diffie, Martin E. Hellman: Privacy and Authentication: An Introduction to Cryptography; Proceedings of the IEEE, Vol. 67, No. 3, March 1979, Seite 397 bis 427

[Elek_82] Elektronik Sonderheft Nr. 50, „Daten-Kommunikation"; 8. Teil Einführung in die Datenfernverarbeitung, Lokale Netzwerke – die Basis für integrierte Informations-Systeme; Franzis-Verlag GmbH, Karlstr. 37–41, 8000 München 2, ISSN 0170–0898, 1982, Seite 69 bis 77

[Kubi_85] Herbert Kubicek: Soziale Beherrschung des technischen Wandels erfordert Technikgestaltung auf allen Ebenen; HFF, Hörfunk, Fernsehen, Film; Zeitschrift der Rundfunk-Fernseh-Film-Union (RFFU) in der Gewerkschaft Kunst (GK) im DGB, 35. Jahrgang, Dezember 1985, 12/85, Seite 10

[Kubi_86] Herbert Kubicek: Für eine andere Technologiepolitik; HFF, Hörfunk, Fernsehen, Film; Zeitschrift der Rundfunk-Fernseh-Film-Union (RFFU) in der Gewerkschaft Kunst (GK) im DGB, 36. Jahrgang, Januar/Februar 1986, 1–2/86, Seite 25 bis 27

[KuRo_86] Herbert Kubicek, Arno Rolf: Mikropolis; Mit Computernetzen in die „Informationsgesellschaft"; 2. Auflage, VSA-Verlag, Hamburg 1986

[Müll_85] Wolfgang Müllner: Arbeitsrechtliche Aspekte der Telearbeit; „Computer und Recht (CuR)", Verlag Dr. Otto Schmidt KG, Köln, 1. Jahrgang, Oktober 1985, Seite 33 bis 39

[Pfit_83] Andreas Pfitzmann: Ein Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes in Bildschirmtext-ähnlichen Neuen Medien; GI '83 13. Jahrestagung der Gesellschaft für Informatik, Oktober 1983, Hamburg, Informatik-Fachberichte Band 73, Springer-Verlag Heidelberg, Seite 411 bis 418

[Pfit_84] Andreas Pfitzmann: A switched/broadcast ISDN to decrease user observability; 1984 International Zurich Seminar on Digital Communications, Applications of Source Coding, Channel Coding and Secrecy Coding, March 6–8, 1984, Zurich, Switzerland, Swiss Federal Institute of Technology, Proceedings IEEE Catalog no. 84CH1998–4, Seite 183 bis 190

[Pfi1_83] Andreas Pfitzmann: Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 18/83, Dezember 1983

[Pfi1_85] Andreas Pfitzmann: How to implement ISDNs without user observability – Some remarks; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 14/85

[PfPW_86] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Technischer Datenschutz in diensteintegrierenden Digitalnetzen – Warum und wie? „DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme", Vieweg & Sohn, Braunschweig, Heft 3, Juni 1986, Seite 178 bis 191

[PPW_86] Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; erscheint in „Computer und Recht (CuR)", Verlag Dr. Otto Schmidt KG

[ScSc_84] Christian Schwarz-Schilling (ed.): Konzept der Deutschen Bundespost zur Weiterentwicklung der Fernmeldeinfrastruktur; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Stab 202, Bonn, 1984

[ScSc_86] Christian Schwarz-Schilling (ed.): Mittelfristiges Programm für den Ausbau der technischen Kommunikationssysteme; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn, 1986

[ScS1_84] Christian Schwarz-Schilling (ed.): ISDN – die Antwort der Deutschen Bundespost auf die Anforderungen der Telekommunikation von morgen; Herausgeber: Der Bundesminister für das Post- und Fernmeldewesen, Bonn, 1984

[SuSY_84] Tatsuya Suda, Mischa Schwartz, Yechiam Yemini: Protocol Architecture of a Tree Network with Collision Avoidance Switches; Links for the Future; Science, Systems & Services for Communications, P. Dewilde and C. A. May (eds.); Proc. of the Intern. Conference on Communications – ICC '84, Amsterdam, The Netherlands, May 14–17, 1984, IEEE, Elsevier Science Publishers B. V. (North-Holland), Seite 423 bis 427

[Tane_81] Andrew S. Tanenbaum: Computer Networks, Prentice-Hall, Englewood Cliffs, N. J., 1981

[WaPf_85] Michael Waidner, Andreas Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; Proc. 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, München, Oktober 1985, P. P. Spies (Hrsg.), Informatik-Fachberichte Band 113, Springer-Verlag Heidelberg 1985, Seite 128 bis 141; Überarbeitung erschien in „DuD, Datenschutz und Datensicherung, Informationsrecht, Kommunikationssysteme", Vieweg & Sohn, Braunschweig, Heft 1, Februar 1986, Seite 16 bis 22

[WeSo_85] Marita Wellmann, Michael Sommer: Gespaltene Kommunikationsnetze – eine falsche Strategie; HFF, Hörfunk, Fernsehen, Film; Zeitschrift der Rundfunk-Fernseh-Film-Union (RFFU) in der Gewerkschaft Kunst (GK) im DGB, 35. Jahrgang, Dezember 1985, 12/85, Seite 11