Informationssicherheit der Global Information Infrastructure (GII)[1]

– Einige Bemerkungen zu Problemen, Anforderungen und Entwicklungen –

Hartmut Pohl

0 Einführung

Die Global Information Infrastructure (GII) - auch als Datenautobahn o.ä. bezeichnet - zielt auf die schnelle Übertragung großer Datenmengen zwischen allen Interessierten wie Privaten, Regierungen, Behörden, Institutionen und Unternehmen mit Hilfe von Computern. Übertragen werden können heutzutage numerische Daten, Zeichen, Texte, Tabellen, Grafiken, Animationen, Standbilder, Bewegtbilder (Video) und Film sowie akustische Signale, Sprache und Musik: Multimedia. Auf der Vorläuferstruktur Internet ist dies bereits heute weitgehend möglich. In Zukunft können wohl auch taktile Reize (Bewegungen) sowie weitere Medien wie Gerüche und Geschmack übertragen werden.

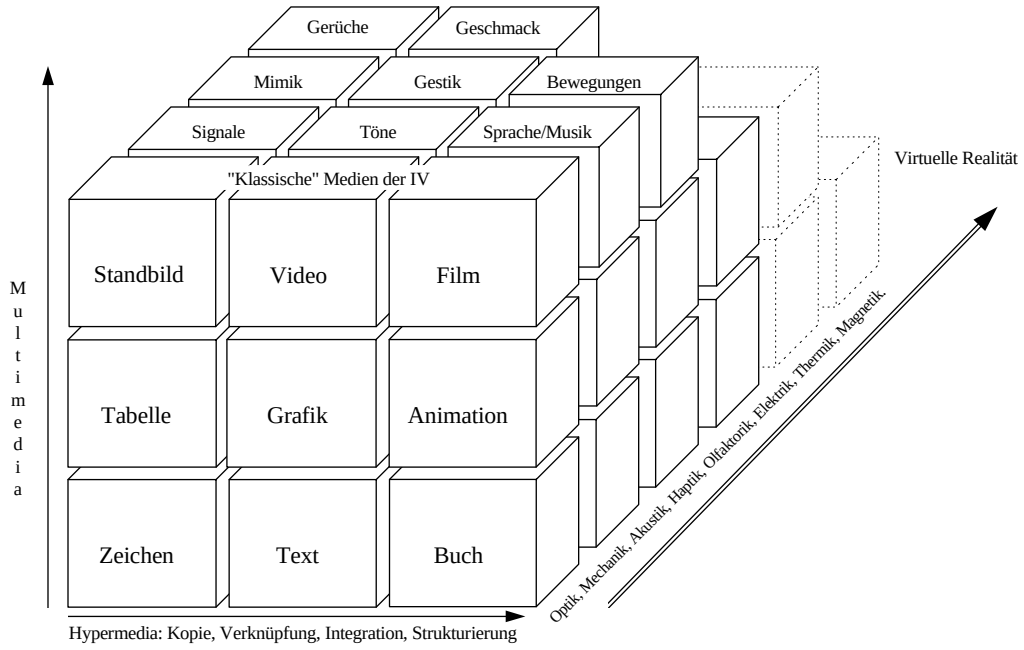

Abbildung 1: Multimedia-Hypermedia-System.

Die gleichzeitige Nutzung dieser Medien wird zusammenfassend als virtuelle Realität bezeichnet. Unter globaler Informationsinfrastruktur wird die integrale Verknüpfung von Daten verarbeitenden (speichernden und verarbeitenden) Computern und deren Vernetzung verstanden - unabhängig von der Art der Nutzung: Klassisches Telefon, Fernsehen oder breitbandige Datenübertragung. Notwendiger Bestandteil sind außerdem Dienste, Dienstleister und Anbieter. Zur kurzen Darstellung der Möglichkeiten der virtuellen Realität und der zu erwartenden Sicherheitsprobleme soll hier ein Szenario eingefügt werden.

Szenario: Ein Urlaub auf Hulateebe

Von einem heimischen Gerät wie Personal Computer (PC), Workstation oder Fernsehapparat und Overhead-Display mit 4 Zoll großen Sichtgeräten unmittelbar vor seinen Augen, 4-Kanal-Ton und an das System angeschlossenen Datenanzug mit Datenhandschuh wählt der Betrachter August Schulze die Internet-Adresse eines Reiseveranstalters und aus dem Menü Urlaub das Zielgebiet Südsee durch Zeigen auf den dreidimensional dargestellten Globus mit dem Datenhandschuh aus - und zwar die kleine Insel Hulateebe. Es läuft ein Video an, das in angenehm weichen aber kontrastreichen Farben insbesondere das einzige Hotel der Insel in gleißender Sonne mit dem weißen Strand im Hintergrund sowie ei-

[1] Erschienen in: Tauss, J. (Hrsg.): Deutschlands Weg in die Informationsgesellschaft. Herausforderungen und Perspektiven für Wirtschaft, Wissenschaft, Recht und Politik. Baden Baden 1996 S. 358 - 390

nigen hörbar musizierenden Hotelangestellten zeigt. Die dreidimensionale Darstellung ist beeindruckend. Durch deutlichen Blick auf den Hoteleingang schaltet sich der Betrachter in die Hotellobby. Hier läuft ein weiteres Video an mit dem Hotelportier und der Empfangsdame, die ein Zimmer anbietet. Nach Anwahl der 7. Etage im Aufzug wird das entsprechende Zimmer gezeigt. Der Betrachter betritt es. Nach kurzem Blick in das Badezimmer wendet er sich - das King-Size-Bett nur streifend - dem Fenster zu und sieht nun die Strandszene mit den hörbar musizierenden Hotelangestellten und auch die gar nicht übervölkerte, eindrucksvoll im Südsee-Stil eingerichtete Freiluftbar am Pool. Sein Blick fällt auf die sanfte Dünung des durchsichtig wirkenden Meeres der bereits tief stehenden Sonne entgegen. August Schulze wendet sich zufrieden vom Panoramafenster dem großen Bett zu. Er legt sich darauf - und spürt durch seinen Datenanzug die bequeme aber feste Matratze. Er ist überzeugt - hier würde ein Urlaub nie langweilig werden. Eindringlich blickt er auf die angebotenen Termine und die Preisliste, wählt drei Wochen aus, wartet noch auf die Buchungsbestätigung und schaltet dann um auf das Unterhaltungsprogramm eines seiner Pay-TV-Sender.

Der Betrachter hatte durch die gleitenden Übergänge zwischen den insgesamt 8 betrachteten Videos die technischen Brüche gar nicht bemerken können. Die Zeit von insgesamt 3 Stunden war ihm wie im Fluge vergangen.

August Schulze zieht die Datenhandschuhe und den Datenanzug aus und setzt das Overhead-Display ab. Dabei sinniert er über den lang dauernden Flug in die Südsee mit Umsteigen. Eigentlich könnte er sich dies alles ersparen, wenn er noch weiter und länger in die vom Reiseveranstalter bereitgestellte virtuelle Realität eintauchen würde.

Als sich der Kunde zum Abflugtermin rechtzeitig mit seinem Gepäck auf dem Flugplatz einfand, mußte er bemerken, daß es keinen Flug nach Hulateebe gab. Nach längeren Diskussion mit Beteiligten und Unbeteiligten fuhr er enttäuscht nach Hause. Recherchen ergaben, daß der angebliche Reiseveranstalter nicht existierte. Die vorgespielte virtuelle Realität war offensichtlich aus Versatzstücken anderer Veranstalter und von Reisebüros und Fremdenverkehrsämtern zusammengestückelt worden. Die Internet-Adresse des Reiseveranstalters war nicht mehr eruierbar. Allerdings war nicht nur der Reisepreis sondern darüberhinaus ein noch größerer nicht weiter spezifizierter Betrag von seinen Konto abgebucht worden. Einige Wochen später erhielt er von mehreren Veranstaltern unaufgefordert e-mails mit günstigen Urlaubsangeboten in der Südsee ...

1 Anwendungsbereiche

Die Entwicklung der Datenverarbeitung begann mit zentral aufgestellten Rechensystemen; im Hinblick auf eine stärkere Anwenderorientierung wurden später entfernt aufgestellte Sichtgeräte und Drucker (Terminals) angeschlossen; die Rechenleistung wurde zentral erbracht und die Daten zentral gespeichert. Wegen der geforderten kurzen Antwortzeiten wurden Rechensysteme in der zweiten Entwicklungsstufe mehr zum Anwender hin verlagert und Ressourcen direkt am Arbeitsplatz bereitgestellt. Allerdings waren nun nicht mehr alle Daten zentral verfügbar; diese Lösung führte daher zu Mehrfachspeicherungen von Daten auf verschiedenen Rechensystemen.

Daher wurden in der dritten Stufe unternehmensinterne Netze (local area networks - LAN) sowie regionale (metropolitan area networks - MAN) und internationale (wide area networks - WAN) Netze realisiert.

Auf dieser Basis baute in der vierten Stufe die Integration der bisher getrennt genutzten Textverarbeitung, Tabellenkalkulation, Grafikverarbeitung auf: Multimedia; dazu gehören im engen Sinne Anwendungen wie Animationen, Standbilder, Bewegtbilder (Video) und Film sowie akustische Signale, Sprache und Musik. Durch die dreidimensionale Darstellung entsteht die virtuelle Realität.

Bei Hypermedia steht die Verknüpfungsmöglichkeit dieser Medien im Vordergrund: Lesen eines Textes (z.B. Biographie von Beethoven); Betrachten eines zugehörigen Bildes oder Videos; Anhören einer Symphonie. Durch Verknüpfungen kann sehr schnell zwischen verschiedenen oder auch erläuternden Informationen hin- und hergesprungen werden.

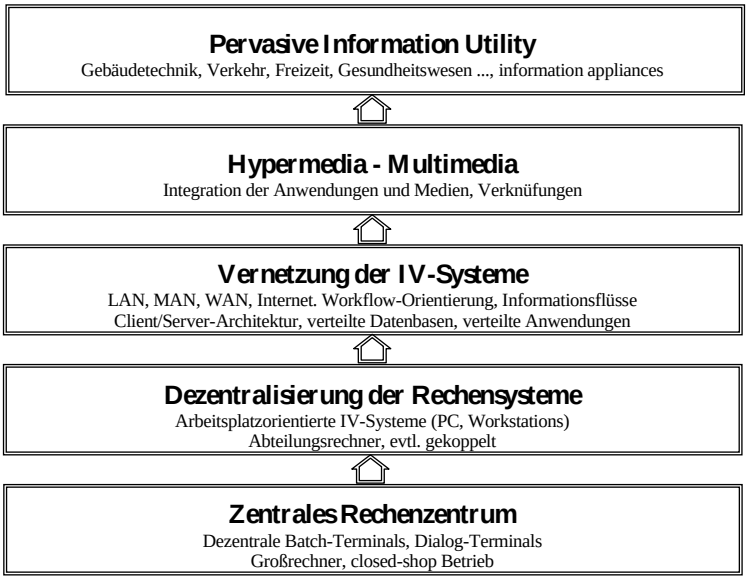

Abbildung 2: Entwicklung der Informationsverarbeitung.

In der fünften Stufe werden alle Bereiche menschlichen Lebens durch die Informationsverarbeitung durchdrungen und verknüpft. Die Informationsverarbeitung begleitet uns global - also ortsunabhängig - im Beruf, in der Freizeit sowie in allen Lebenssituationen.

In der GII wirken die folgenden vier Partner zusammen:

- Netzwerkbetreiber (network provider) stellen die notwendigen Datenübertragungsleitungen - die auch als Richtfunkstrecken oder Satellitenverbindungen realisiert sein können - zur Verfügung zusammen mit den derzeit aktuellen Übertragungsdiensten wie ISDN, ATM.
- Diensteanbieter (service provider) bieten - in Datenbanken auf Computern gespeicherte - Informationen an sowie die Auswertung und Verknüpfung von Informationen.
- Geräte- und Programmhersteller und die Lieferanten: Zum Anschluß an Datenübertragungsleitungen und zur Nutzung der Diensteangebote sind Geräte wie Personal Computer und Workstations - insbesondere aber Programme (Software) notwendig sowie Geräte und Programme zur Verknüpfung mit der unternehmensinternen Informationsverarbeitung (lokale Netze). Derartige Programme sind auch nötig zur Speicherung der bereitgestellten Informationen sowie zu ihrer Aufbereitung.
- Zielgruppen der GII sind End-Anwender in Großunternehmen, mittleren und kleinen Unternehmen, Behörden, Anstalten und zunehmend Private.

Die möglichen Sachziele und Anwendungsfelder der Globalen Informations-Infrastruktur können beispielhaft aufgeführt werden:

Sachziele der GII
Verteilte Verarbeitung von Daten.
Übertragung formatierter und unformatierter Daten (Programme und Daten).
Informationsbeschaffung, Sammeln, Filtern und Verteilen.
Asynchrone und mobile Kommunikation. Sprachliche, schriftliche, bildliche, akustische, taktile. Z.B. Beratungen und Diskussionen (mit Selbsthilfeeinrichtungen). Weltweite ortsunabhängige persönliche Erreichbarkeit.
Telearbeit, kooperatives Arbeiten an Projekten in und zwischen Unternehmen. Telemanipulation (manipulatives Arbeiten in großen Entfernungen): • Reparaturen in gefährlichen Bereichen (z.B. Weltraum, Kernkraftwerke), • Entfernte Diagnosen und Operationen (Gesundheitsbereich) etc.

Sofern nicht angemessene Sicherheitsmaßnahmen realisiert werden, sind die o.g. Sachziele und und die im folgenden aufgeführten Anwendungsfelder in ihrer Realisierung gefährdet.

Anwendungsfelder der GII
Erziehung, Bildung und Ausbildung - u.a. Familienplanung-begleitende sowie berufsbegleitende Veranstaltungen, private Information und Kommunikation.
Konsumorientierte Dienste: Tele- und Homeshopping, Telemarketing, Werbung, Finanzdienstleistungen, individualisierte Publikationen.
Freizeit, Unterhaltung: Bibliotheken, Rundfunk, Fernsehen, Pay-TV, (Near-) Video on Demand, Interaktives Fernsehen, Museen, Konzerte, Spiele, ...
Gesundheitswesen: Beratung, Ferndiagnose, Überwachung, Operation, Vorbeugung, ... Notfall-Nutzung bei Krankheit, Unfall, Katastrophen, Höherer Gewalt.
Wissenschaft und Forschung, Teleteaching, Telelearning.
Gebäudesteuerung, Verkehrssteuerung, Fabriksteuerung.
Produktion, Reparaturen, Fernwartung,
Verwaltung: Behördenaktivitäten wie Umweltschutz (Überwachung, Steuerung).
Wahlen, Abstimmungen, Bürgerbegehren, Befragungen.

Im folgenden werden die Nutzer der GII aufgelistet:

Einige Zielgruppen
Private, Vereine
Unternehmen, Konzerne
Behörden (Bund, Länder, Kommunen), Verbände, Bildungseinrichtungen.
Partiell immobile Gruppen: Kranke, Behinderte.

Konsequenterweise werden diese Zielgruppen die GII kaum nutzen, wenn Sicherheitsprobleme - insbesondere wiederholt - auftauchen. Beispielsweise dürfte Telemanipulation dann kaum genutzt werden, wenn die weit entfernten Geräte dank verfälschter Datenübertragung falsch bedient werden. Bei Teleoperationen im Gesundheitsbereich oder auch nur Telediagnose dürfte die Problematik noch deutlicher werden.

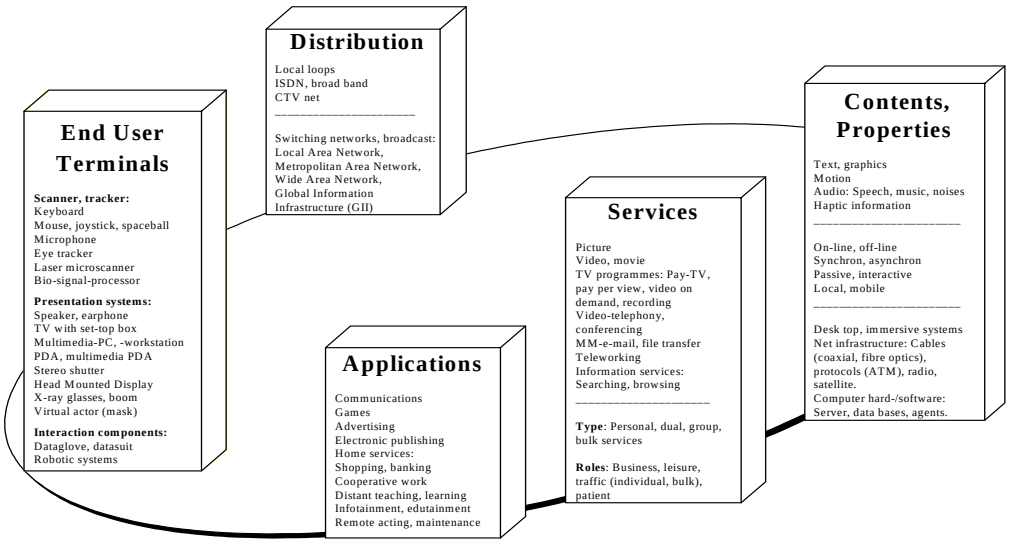

Abbildung 3: Multimediale Komponenten, Dienste und Anwendungen.

In der vorstehenden Abbildung sind einige Komponenten und Geräte dargestellt, mit denen die GII genutzt werden kann und es sind die Anwendungsbereiche der GII dargestellt.

Unternehmen bringen der Infrastruktur und den Diensten im Multimediabereich der GII großes Interesse entgegen. Die folgende Abbildung zeigt die am Netzbetrieb und den Dienstleistungen beteiligten Unternehmen bzw. die Planungen auf sowie ihre Verflechtungen nach dem Stand vom Juli 1995.

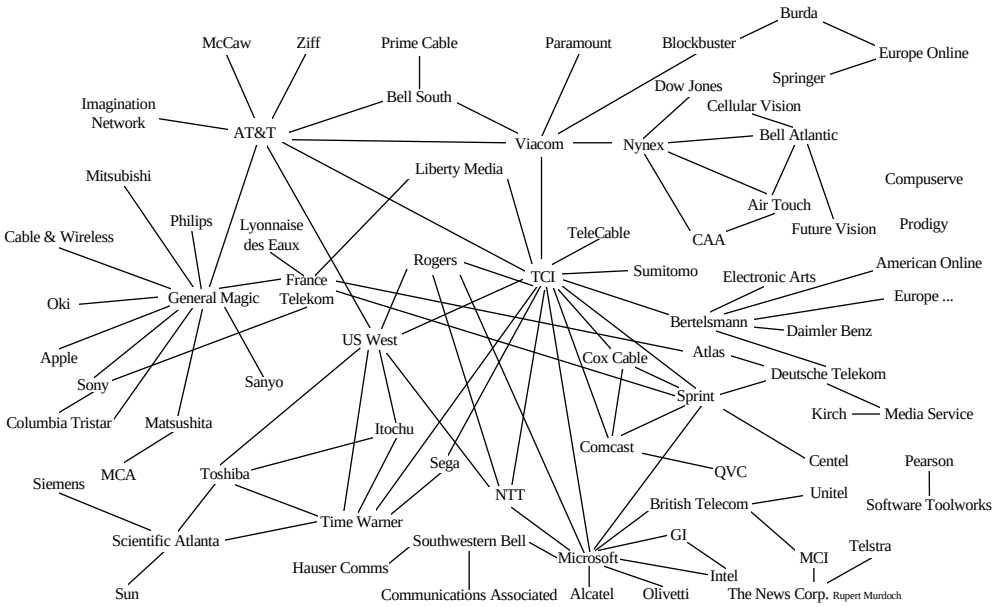

Abbildung 4: Allianzen und Joint Ventures im Multimediabereich.

Seitdem sind mehr oder weniger wöchentlich weitere Kooperationen und freundliche oder feindliche Übernahmen oder zumindest Übernahmeversuche bekannt geworden.

2 Aktuelle und zukünftige Probleme der Informationssicherheit der GII

Für die GII und ihre zu erwartende technische Entwicklung kann das Internet als Beispiel oder Vorläufer betrachtet werden - zumindest stellt es die derzeitige Realisierung dar. Allerdings sind hier bereits eine Reihe von Sicherheitsproblemen aufgetaucht. Bei Weiterentwicklungen der Informationsinfrastruktur in Richtung einer GII dürften in Zukunft diese sowie vergleichbare weitere und schwerwiegendere Sicherheitsprobleme in weit größerer Zahl auftreten.

Früherkennung

Diese absehbare Vielzahl von Problemen dürfte Sicherheitsmaßnahmen erforderlich machen, die über die derzeit vorhandenen und in der Entwicklung befindlichen hinausgehen. Derartige Entwicklungen müssen frühzeitig angestoßen werden.

Akzeptanz

Sofern die Endanwender nicht sicher sein können, daß ihre digitale Kommunikation unverfälscht beim Adressaten ankommt, die Nachrichteninhalte Unberechtigten nicht zugänglich sind und die Kommunikation von Dritten nicht überwacht wird (Datenschutz, Vertraulichkeit), wird die GII weder von Unternehmen noch von Privaten in der Form angenommen werden, wie es heute vielfach geplant ist. Darausfolgend dürfte ein erheblicher volkswirtschaftlicher Schaden entstehen, wenn angemessene Sicherheitsmaßnahmen nicht realisiert werden. So muß z.B. insbesondere für den privaten Bereich Anonymität und Pseudonymität bei Nachrichtenaustausch und finanziellen Transaktionen sichergestellt werden.

Angriffe

Die Störungen der Globalen Informations-Infrastruktur (GII) und die Angriffe auf sie erfolgen programmgesteuert unter Einsatz von Computern. Sie können daher sehr schnell erfolgen (mehrfach im Sekundenbereich) und wiederholt werden, ohne daß ein Mensch noch eingreifen muß. Darauf beruht eine Vielzahl von Angriffen. Durch Programmänderungen können Angriffe modifiziert werden, sodaß einfache Sicherheitsmaßnahmen unterlaufen werden können.

Die Angriffe erfolgen weltweit, weil die meisten Computer vernetzt sind. Häufig ist auch der Ursprung eines Angriffs gar nicht mehr erkennbar! Zwar sind nicht alle Computer direkt an das Internet angeschlossen; viele sind über lokale oder unternehmenseigene Netze oder über Netzbetreiber oder andere Service Provider gekoppelt. Alle direkt oder indirekt mit dem Internet verbundenen Computer können von Angriffsprogrammen auch erreicht werden.

Bevor Warnungen fundiert ausgesprochen werden können, sind viele Computer bereits Opfer dieser Angriffe geworden. Veröffentlichte Warnungen beziehen sich daher meist auf vorbeugende Maßnahmen gegen Wiederholungen gleichartiger Angriffe sowie auf die Vermeidung von Folgeschäden.

Die Bedeutung der Informationsverarbeitung als risikobehaftete Technik wird in den im folgenden beispielhaft erwähnten Bereichen besonders deutlich: Kernkraftwerk-Steuerung, Eisenbahn-Verkehrssteuerung, Avionik, Steuerung des Individualverkehrs, sowie medizinische Geräte wie z.B. Tomographen und Bestrahlungsgeräte.

2.1 Sachziele der Informationssicherheit

Einige Sachziele der Aktivitäten im Rahmen der Informationssicherheit lassen sich wie folgt formulieren:

Sachziele der Informationssicherheit	
Verfügbarkeit	availability
Integrität	integrity
Vertraulichkeit	confidentiality
Rechtsverbindlichkeit	liability
Anonymität	anonymity
Pseudonymität	pseudonymity
Nicht-Zurückweisung	non-repudiation
Unbeobachtbarkeit	unobservability
Abrechenbarkeit	accountability

Verfügbarkeit

Anwender erwarten, daß die GII die von ihnen gewünschten Leistungen erbringt: Sachziel Verfügbarkeit. Dazu ist es notwendig, daß eine Vielzahl von Computern, die steuernden Betriebssysteme und insbesondere die verarbeitenden Programme ordentlich funktionieren und die gewünschten Daten zugreifbar sind, damit die gewünschten Dienstleistungen erbracht werden können D.h. zwar nicht, daß die Computer immer ohne Unterbrechung arbeiten müssen; d.h. aber, daß sie die gewünschten Ergebnisse mit einer akzeptablen Antwortzeit bereitstellen. Übertragene Nachrichten sollen den Empfänger auch erreichen.

Integrität

Die verarbeitenden Programme sollen genau die Dienstleistungen erbringen, die der Anwender erwartet - und nicht mehr oder weniger: Sachziel Integrität. Insbesondere die nicht-dokumentierten Nebenwirkungen - sog. Trojanische Pferde - haben zu Sicherheitsproblemen geführt. Die weithin bekannten Computerviren sind nur ein Beispiel; andere sind sog. Würmer etc. Die zu verarbeitenden Daten müssen exakt sein, korrekt, genau, unverfälscht und auf dem aktuellen Stand. Übertragene Nachrichten sollen den Empfänger auch unverändert erreichen.

Vertraulichkeit

Auf die verarbeiteten - gespeicherten und übertragenen - Daten dürfen Unberechtigte nicht zugreifen können: Sachziel Vertraulichkeit.

Soweit zu den insbesondere in Deutschland und der Europäischen Union von staatlicher Seite akzeptierten Sachzielen. Allerdings ist der Katalog der Sachziele durch neuere Arbeiten inzwischen auch von den Normungsgremien international erweitert worden. Einige relevante werden im folgenden genannt:

Unbeobachtbarkeit

Der gesamte private und geschäftliche Datenverkehr muß unbeobachtet vollzogen werden können: Sachziel Unbeobachtbarkeit. Insbesondere darf der Inhalt der Kommunikation nicht beobachtbar sein und auch die Sender- und Empfängeradressen dürfen nicht kontrolliert werden können, um den Aufbau von Verkehrsprofilen (wer kommuniziert mit wem, wer hat mit wem geschäftliche Verbindungen) und den Aufbau von Verhaltensprofilen zu verhindern.

Übertragene Nachrichten sollen den Empfänger auch nachweislich erreichen; den Empfang einer Nachricht soll der Empfänger nicht abstreiten können: Sachziel Non-repudiation.

Non-repudiation

Abrechenbarkeit Alle auf der GII angeforderten und erbrachten Leistungen müssen einem Verursacher zugeordnet werden können und ihm gegenüber abgerechnet werden können:

Sachziel Abrechenbarkeit. U.a. muß der programmgesteuerte Versand von Werbung nachvollzogen werden können, um sie ggf. abwehren zu können.

Anonymität

Nicht alle Aktivitäten in der GII sollen den agierenden Personen auch tatsächlich zugeordnet werden können. Daher werden Funktionen und Dienste gefordert, die anonyme Aktionen zulassen wie z.B. in der bisherigen Welt kleinere Einkäufe mit Bargeld. In der GII ist dies digital cash: Sachziel Anonymität.

Rechtsverbindlichkeit

Private und Unternehmen müssen über die GII rechtsverbindliche Kommunikation treiben können und Verträge abschließen können. Diese Kommunikation muß gerichtsverwertbar und prozeßfest erfolgen: Sachziel Rechtsverbindlichkeit.

Copyright

Weiterhin problematisch ist derzeit die Durchsetzung eines Copyrights bei sog. elektronischen Dokumenten.

2.2 Mißbrauchsfälle

Sabotage

Aus der Vielzahl untersuchter und nur zum kleinen Teil veröffentlichter Fälle von Computer- Mißbrauch sollen hier einige wenige beispielhaft skizziert werden.

Der Feierabendtäter

Ein ungetreuer Mitarbeiter eines international agierenden deutschen Finanzdienstleisters schaltet zum Dienstschluß in Deutschland die Verbindung zwischen dem internen lokalen Netz und dem Internet ab. Dies wird am nächsten Morgen bemerkt und die Verbindung wiederhergestellt. Allerdings waren in der Zwischenzeit die über die Welt verstreuten Kunden nicht in der Lage, dem Unternehmen Aufträge zu erteilen. Wegen der Dringlichkeit der beabsichtigten Finanztransaktionen beauftragten sie Mitbewerber des deutschen Finanzdienstleisters.

Die e-mail-Bombe*: Einem - eines Umweltskandals verdächtigten - Unternehmen werden von Aktivisten aus aller Welt e-mails zugesandt mit der Aufforderung die Produktion einzustellen. Obwohl der Verdacht binnen Stunden von seiten der staatlichen Aufsichtsbehörde ausgeräumt werden kann, nimmt die Flut der e-mails nur sehr langsam ab. Innerhalb der ersten Woche gehen insgesamt 20.000 e-mails dieser Art ein. Da diese e-mails nicht eindeutig gekennzeichnet sind und in die Mailbox immer wieder zu bearbeitende e-mails eingehen, müssen alle 20.000 e-mails gelesen werden. Da die Absenderadresse fälschbar ist, werden die Sender nicht bekannt, das betroffene Unternehmen kann den Sendern auch keine Richtigstellung übersenden oder gar die Sender wegen Betriebsstörung verklagen.*

Berücksichtigt werden muß der äußerst niedrige Preis für den Versand einer e-mail-Bombe mit etwa DM 0,03 pro e-mail.

Die verfälschte Überweisung

Eine per Datenübertragung versandte Überweisung zwischen Banken wird auf dem Netz abgefangen und es wird der überwiesene Betrag sowie der SWIFT-Code zusammen mit der Kontonummer abgeändert. Bei der nun adressierten Bank wird der Betrag von den Tätern teils in bar abgehoben teils an weitere Banken überwiesen.

Die Fehlschaltung

Bei Reparaturarbeiten am Switching Center in der Landeshauptstadt setzt der von seiner bisherigen Karriere enttäuschte Mitarbeiter Peter Müller einen Parameter bewußt falsch und geht in die Mittagspause. Durch die Parametersetzung wird der gesamte Datenverkehr zu den drei westlich gelegenen Städten unterbunden. Die ersten Beschwerden gehen am frühen Nachmittag ein. Der Mitarbeiter tut fast noch den ganzen nächsten Tag so, als sei er emsig mit der Fehlersuche beschäftigt, bis er den Parameter am späten Nachmittag des zweiten Tages zurücksetzt.

Spionage

Die Vielflieger-Liste

Einem mittleren Luftverkehrsunternehmen wird von einem Mitbewerber die Vielflieger-Liste aus dem Computer kopiert. Diese Vielflieger werden vom Mitbewerber angeschrieben und mit speziellen Sonderangeboten geködert.

Der Aids-PC

Aus einem Krankenhaus wird die Datei mit sämtlichen Daten (Name, Adresse, Alter, Infektionsart und Jahr, Anamnese, Diagnose, Behandlungsarten wie Kuren, Medikamente etc.) der hier behandelten AIDS-Kranken von einem unberechtigten Dritten kopiert. Die Verwendungsmöglichkeiten wie Erpressung sind offensichtlich.

Die grundsätzliche Bedeutung der Computer-Spionage und der Computer-Sabotage liegt darin, daß sie wegen der weltweiten Vernetzung von jedem an die GII angeschlossenen Computer der Erde - natürlich auch von mobilen Computern - ausgeführt werden kann.

Von nationalen Strafverfolgungsbehörden werden Angriffe auf dem Internet von Institutionen aus **Drittländern** gemeldet, die wirtschaftlich relevante technische Informationen aus den Bereichen Forschung und Entwicklung suchen.

Auch in der GII werden - wie bereits heute auf dem Internet - die beiden Problembereiche Sabotage und Spionage die entscheidende Rolle spielen.

Ein aktuell "beliebter" Angriff ist das **Scannen** der Nachrichten auf den Netzen hinsichtlich Absendern, Adressaten, Inhalt, Abonnements von Mailboxen und Digests (z.B. nach Interessen).

Angriffsverfahren

Sniffer-Attacken: Weiterhin werden systematisch angeschlossene Rechensysteme untersucht und das jeweils installierte Betriebssystem auf Eindringmöglichkeiten geprüft. Anschließend werden die gespeicherten Daten und Programme auf ihre Verwendungsmöglichkeit hin überprüft. Benutzerberechtigungen und Paßwörter werden kopiert und es werden unberechtigt neue Benutzerberechtigungen eingerichtet, um sie später noch einmal verwenden zu können. Ein- und ausgehende Nachrichten werden hinsichtlich Absender- und Empfängeradresse geprüft mit dem Ziel, mit Hilfe dieser Adressen in andere Rechensysteme einzudringen.

Sog. **Agentenprogramme** werden eingesetzt, um Mißbrauchsmöglichkeiten zu erschließen.

Stealth-Techniken: Sie werden nicht nur bei Viren eingesetzt sondern auch bei anderen Angriffen wie Sniffer-Attacken etc. Die Manipulationen reichen bis hin zu Modifikationen an Betriebssystemen. Damit werden die Angriffsprogramme ein Teil des Betriebssystems. Betriebssysteme werden auch bei Anwendern heimlich ausgetauscht. Dann wird der Rechner zum Angriffsrechner ohne daß dies der Anwender bemerkt.

Ebenfalls als Angriffe angesehen werden sexuelle Darstellungen in Bild und Ton verschiedenster Art. Dies ist insbesondere ein Problem für Eltern jüngerer - auf das Internet zugreifender - Kinder.

Freiheitsrechte

Die Kombination der verschiedenen Dienstleistungen in Netzwerken in Multimediaqualität wie Road Pricing, Disease Management, Mobilkommunikation etc. kann zu einer vollständigen Überwachung aller Menschen führen. Zumindest ist die Überwachung durch die Konstruktion der derzeit realisierten Systeme technisch unvergleichlich einfach zu realisieren - viel einfacher als in früheren Zeiten. Dadurch kann sich die Balance zwischen staatlichen Aufgaben und den Freiheitsrechten des Einzelnen und den Kontrollrechten gegenüber dem Staat verschieben. Vorbeugend müßte hier geprüft werden, inwiefern bei diesen sehr stark erweiterten technischen Möglichkeiten ein Ausgleich gefunden werden muß zwischen den Überwachungsinteressen des Staates und der Bürgerfreiheit.

3 Ursachen der Informations-Unsicherheit in der GII

Im folgenden sollen die vier Ursachen für die derzeitig aktuellen und die zu erwartenden Sicherheitsprobleme aufgezeigt werden und damit die auch zukünftig zu erwartenden Sicherheitsprobleme skizziert werden.

1. Nutzung der Programmsteuerung (freie Programmierung durch den Anwender) von Computern.
2. Weltweite Verfügbarkeit von Computern.
3. Vernetzung: Weltweite Verknüpfung der unternehmenseigenen und privaten Computer.
4. Durchdringung des gesamten - beruflichen und privaten - Lebens mit der Informationsverarbeitung (pervasive computing).

4 Szenarien

Hilfreich zur plastischen Darstellung von Problemen und Lösungsmöglichkeiten kann die Formulierung von Szenarien sein, in denen Angebote und Nutzungsweisen der GII durch Endanwender dargestellt werden sowie Simulationsstudien, in denen reale Situationen in begrenzter Umgebung dargestellt und bearbeitet werden mit dem Ziel, Handlungsweisen und Reaktionen von Endanwendern erkennen zu können. Im folgenden werden zwei Szenarien zur Informationssicherheit der GII entwickelt, die technisch machbar und wirtschaftlich sind.

Disease Management

Die über Patienten gespeicherten Daten werden in der GII verfügbar gemacht. Damit sind

die vollständigen Krankenakten zugreifbar und es werden die folgenden Bereiche vernetzt: Labore, Praxen, Ärzte, Kassenärztliche Vereinigungen, Arbeitgeber, Datenregister (Tumore, ...). Damit wächst auch das Risiko, daß Unberechtigte Krankheitsdaten gezielt oder willkürlich gewählten Personen zuordnen - z.B. in der Absicht, diese zu diskreditieren.

So wird derzeit für 110.000 niedergelassene Ärzte in Deutschland eine sog. ISDN-Plattform geschaffen, die es ermöglichen wird, bei Operationen im Bedarfsfall Spezialisten online hinzuzuziehen (Winkelhage, 1995).

Einige Staaten bemühen sich derzeit bereits darum, off-shore den Aufbau von Datenverarbeitungskapazität dadurch attraktiv zu machen, daß Datenschutzgesetze nur sehr schwache Forderungen enthalten oder daß derartige Gesetze gar nicht existieren.

Technoterrorismus

Durch Manipulation des Global Positioning System (GPS) werden im Rahmen der Navigationsunterstützung für Schiffe, Flugzeuge und Fahrzeuge falsche Koordinaten gesendet. Dadurch kommt es zu Fehlleitungen, Kollisionen und Abstürzen .

Der Mordprozeß

Face tracking ist eine Funktion, die programmgesteuert die Aufnahme eines Gesichts mit allen seinen Bewegungen (Mimik) einer konkreten Person ermöglicht. Über Mikrofone kann zeitgleich die digitale Aufnahme der Stimme erfolgen. Ergänzend kann der zugehörige menschliche Körper komplett d.h. mit Hautfarbe, Haaren und ihrer Farbe bis hin zu den Gliedmaßen mit allen Bewegungen (Gestik und Körpersprache) mit einem sog. 3-D-Scanner digital erfaßt (eingescannt) und in Computern gespeichert werden.

Diese Funktion ermöglicht generierten Filmfiguren das Gesicht, den Körper, die Stimme und die Bewegungen einer konkreten Person zuzuordnen. Die Erfassung, Übermittlung und Speicherung persönlicher Körperdaten (wie Größe, Gewicht, Umfänge, Formen, Farbe der Haare, des Teint) kann sinnvoll genutzt werden zur Visualisierung von in elektronischen Shopping-Center angebotenen Kleidungstücken am vom Computer generierten Körper der Betrachterin oder des Betrachters. Damit wird die virtuelle Anprobe beim homeshopping möglich: Die aus einer Kollektion ausgewählten Kleider, Anzüge etc. werden den einmal gescannten Körperdaten "übergezogen", die betrachtende Person kann unmittelbar am Bildschirm erkennen, ob die ausgewählten Kleidungsstücke zu ihrem Typ, Größe, Körperform, Farbe, Teint etc. passen; eine weitere klassische physische Anprobe wird überflüssig.

Allerdings kann der Körper mit Kopf, Gesicht und Stimme auch in Szenen oder Filme von Landschaften und Umgebungen, die die digital gescannte Person nie gesehen und nie besucht oder betreten hat, eingespielt werden: "Otto Normalverbraucher zusammen mit seiner Frau Gabriele Mustermann am Schreibtisch im Oval Office des Weißen Hauses". Das klingt lustig.

Die Szene kann aber brisant werden, wenn gezielt eine Person digital in eine Filmsequenz manipulierend einspielen, die den Tatort eines Mordes zeigt. Als Beispiel soll hier ein Video vom Tatort des Doppelmordes aus dem sog. O. J. Simpson Fall genommen werden. In das Video werden anschließend die eingescannten Körperdaten von O. J. Simpson vom Computer eingespielt. Bei Vorlage des Films im Prozeß dürfte O. J. Simpson von den Geschworenen schuldig gesprochen werden.

Den Gesamtaufwand an Personal- und Sachkosten für einen in dieser Weise computergestützt erstellten Film vom "Doppelmord" kann mit insgesamt 2 Mio. DM abgeschätzt werden. Ein Bruchteil der von Simpson gezahlten Rechtsanwaltskosten von 9 Mio. US $. Die zu dem Verfahren benötigten Geräte sind kommerziell erhältlich, der Kaufpreis liegt unter DM 500.000.- Die computergestützt erstellten Filme können von "echten" nicht unterschieden werden - die Filme **sind** echt.

Netzwerkaspekt: Der generierte Film wird in der GII verteilt - damit kann ihn jedermann ansehen. In der GII läßt sich nur äußerst schwer feststellen, wer diesen Film in die GII eingespeist hat.

Desinformation dürfte sich als eine wesentliche Angriffsart in der GII entwickeln. Derzeit wird den von unbekannten Dritten übertragenen Nachrichten eine hohe Glaubwürdigkeit beigemessen. Eine Bewertung der Authentizität einer Nachricht dürfte insbesondere dann schwer fallen, wenn sie multimedial übersandt wird: Außer der Akustik wird eine dreidimensionale Videosequenz angeboten.

Der mißliebige Regierungschef

In einem orthodox denkenden Land wird unberechtigt ein computergeneriertes Video mit

einer die religiösen Sitten verletzenden Szene in den Fernsehsatelliten eingespielt und landesweit als Teil einer Nachrichtensendung ausgestrahlt.

Der Regierungschef oder auch die gesamte Regierung dürfte unmittelbar nach der Sendung abgesetzt werden.

Klassisches Telefonsystem sowie Datenleitungen: Das rechnergestützt und programmgesteuerte Telefonsystem eines Landes kann von einem Angreifer so modifiziert werden, daß Vorwahlnummern und Teilnehmernummern verändert werden. Anrufe erreichen dann keinen - jedenfalls nicht den adressierten Empfänger. Derartige Aktivitäten werden als Sabotage oder Technoterrorismus bezeichnet. Der zu tätigende Aufwand ist nicht groß. Notwendig ist das Wissen, welche - ggf. dezentral installierten - Rechner die Adressinformation gespeichert haben und wie sie online zu erreichen sind. Mit einem derartigen Angriff könnte sogar die gesamte Wirtschaft eines Landes nachhaltig gestört werden. Auf diese Weise kann nicht nur das Festnetz sondern können auch die Mobilfunknetze erfolgreich angegriffen werden, indem die Steuerrechner manipuliert werden.

Stromversorgung: Grundlegender können die Kommunikationsnetze gestört werden durch Angriffe auf die Stromversorgung des Landes. Die Stromversorgung wird durch einige wenige Rechner gesteuert. Werden diese manipuliert, kann die Stromversorgung von Landstrichen oder eines ganzen Landes sporadisch oder auch für längere Zeit unterbrochen werden. Schon sporadische Unterbrechungen führen zu Ausfällen bei den angeschlossenen Rechensystemen, die nicht mehr weiterarbeiten können: Bankautomaten, Computer in Geschäften, Unternehmen wie Banken, Versicherungen, Industrie. Notstromversorgungen können nur solange den Stromausfall überbrücken wie die installierten Batterien reichen bzw. Treibstoff für die Motoren der Generatoren vorhanden ist. Nachlieferungen von Treibstoff sind nicht möglich, da dieser rechnergestützt abgefüllt wird. Der Schienen- und Straßen- und Luftverkehr liegt auch darnieder, da Strom zum Betrieb und zur Verkehrsleitung nicht zur Verfügung steht.

Daher müssen risikobehaftete Systeme weltweit unter Sicherheitsaspekten systematisch bewertet werden und die Systeme mit den eklatantesten Schwachstellen hinsichtlich Sicherheit nachgebessert werden.

5 Sicherheitsmaßnahmen für die GII

Die derzeitige grundsätzliche Offenheit des Internets sollte unabhängig vom Anschluß weiterer Computer und Systeme oder Netze beibehalten werden. Allerdings wird diese Offenheit nicht von allen Staaten praktiziert - einige reglementieren den Zugriff über Netze. In anderen bildet die Sprache eine mindestens kulturelle Barriere.

Historisches Ziel des ARPANET - als Vorgänger des Internet - war die erhöhte Verfügbarkeit von Computern und Netzen. Das Ziel ist geblieben; es ist bisher aber nicht erreicht worden. Im Gegenteil: Das Sicherheitsrisiko der Nichtverfügbarkeit ist sehr hoch geworden.

Sicherheitsarchitektur

Für die GII ist daher die Entwicklung einer Sicherheitsarchitektur als Rahmen für alle als erforderlich angesehenen Sicherheitsmaßnahmen notwendig. Ggf. kann diese Architektur schrittweise realisiert und weiterentwickelt werden.

Zugriffskontrolle

Zu den Inhalten der Architektur gehört neben den Protokollen zur multimedialen Datenübertragung insbesondere

- die Kontrolle aller Zugriffe auf Dienste, Programme und Daten
- mit einer angemessenen Anwenderüberwachung sowie
- Agentenprogrammen zur Suche von Informationen und
- Filter zur Abwehr ungewollter Informationen sowie
- Kontrollen der Systeme zur Erkennung von Angriffen und Mißbrauch der Systeme und Dienste (intrusion detection).

Sensibilisierung

- Die Sensibilisierung aller Anwender für die Risiken und Mißbrauchsmöglichkeiten ist ein wesentlicher Teil.

Eine Untersuchung in den USA im Jahre 1995 ergab, daß nur die Hälfte der an das Internet angeschlossenen Unternehmen auf dem Stand der Technik mit sog. Firewalls abgesichert ist. Etwa 10% der Unternehmen waren das Opfer von Computer-Spionage und -Sabotage aus dem Internet geworden, obwohl sie eine Firewall installiert hatten. Allerdings mußte eine Reihe von Unternehmen eingestehen, daß sie

sich nicht ordentlich über die organisatorischen und technischen Einsatzbedingungen der Sicherheitsmaßnahmen informiert hatten. Insgesamt muß auf eine zu geringe Bereitschaft geschlossen werden, Sicherheitsmaßnahmen vorbeugend (!) zu realisieren.

Zur Sensibilisierung gehört die Diskussion der Verantwortung der Netz- und Service-Provider für die von Dritten eingespeisten Nachrichteninhalte (z.B. Pornographie) mit dem Ziel des Jugendschutzes.

5.1 Einsatz von Verschlüsselungsverfahren

Wegen der Vielzahl angeschlossener IV-Systeme kann heute nicht flächendeckend kontrolliert werden, in welchen angeschlossenen Systemen Fehlverhalten auftritt und von welchen Systemen unberechtigte Aktionen ausgehen wie z.B. Behinderung oder sogar Verhinderung der Kommunikation, unberechtigte Kenntnisnahme von Daten oder unberechtigte Veränderung. Zur vertrauenswürdigen Nutzung der Netze ist es auch notwendig, daß die übertragenen Nachrichten authentisch sind und den Kommunikationspartnern verbindlich zugeordnet werden können.

Wegen ihrer umfassenden Bedeutung als Sicherheitsmaßnahme muß die Verschlüsselung als Schlüsseltechnologie zur Erreichung der o.g. Sachziel der Informationssicherheit bezeichnet werden. Unternehmen und Staaten, die die Verfahren der Verschlüsselung - und damit meist auch der Entschlüsselung - beherrschen, können mit ihrem Know-how und ggf. ihren Reglementierungen bei der Nutzung dieser Verfahren Einfluß ausüben.

Derzeit bemühen sich insbesondere die USA um eine vielen Interessen gerecht werdende Lösung. Allerdings unterliegen in den USA höherwertige Verschlüsselungsverfahren einem Exportverbot. Durch diese Restriktion glauben sich die US-Behörden (hier insbesondere die Strafverfolgungsbehörden) in der Lage, den mit schwächeren Verfahren verschlüsselten weltweiten Nachrichtenverkehr überwachen zu können. Damit besteht potentiell die Möglichkeit der Wirtschafts- und anderer Spionage sowie der Sabotage.

5.2 Verschlüsselung zur Erreichung von Vertraulichkeit

Symmetrische Verschlüsselung

- Sender und Empfänger benutzen denselben Schlüssel zur Verschlüsselung und Entschlüsselung der übersandten Nachricht. Vertrauliche Kommunikation ist also nur mit bekannten Partnern möglich. Allerdings ist der (sporadisch notwendige) Schlüsselaustausch aufwendig, da der Schlüssel nicht ohne Schutzmaßnahme versandt werden kann.

Asymmetrische Verschlüsselung

- Asymmetrische Verschlüsselung ermöglicht verschlüsselte Kommunikation mit jedermann, wenn der Sender den sog. öffentlichen Schlüssel des Empfängers kennt - und z.B. einem öffentlich zugänglichen Schlüsselverzeichnis entnommen hat. Der Empfänger kann dann die verschlüsselte Nachricht mit seinem eigenen sog. geheimen (weil nur ihm bekannten) Schlüssel entschlüsseln. Allerdings müssen Sender und Empfänger dann dem Verzeichnis vertrauen. Z.B. kann nämlich ein böswilliger Dritter den Schlüssel des Empfängers in dem Verzeichnis austauschen gegen einen ihm bekannten Schlüssel und dann alle Nachrichten an den Empfänger entschlüsseln und mitlesen.
  Mit dem asymmetrischen Verfahren können symmetrische Schlüssel verschlüsselt übersandt werden.

Staatliche Reglementierung

In den letzten Jahren ist international wiederholt eine staatliche Reglementierung von Sicherheitsmaßnahmen in der Informationsverarbeitung und in Kommunikationssystemen diskutiert worden. Diese Diskussion ging von Fachleuten in den USA aus und wurde auch in die Öffentlichkeit getragen. In Europa wurde eine derart breite Diskussion bisher öffentlich noch nicht geführt.

Die Bedeutung der Kommunikationssicherheit wird von Privaten, Unternehmen und Behörden zunehmend erkannt. Klar erkannt werden auch die weltweiten Überwachungsmöglichkeiten jeglicher Kommunikation durch Dritte wie Behörden und Organisationen und das damit mögliche Mithören und Mitlesen - auch verschlüsselt übertragener Daten - bis hin zur Industriespionage. Sichere Kommunikation zwischen Unternehmen, Behörden und Privaten ist daher ohne den Einsatz von Verschlüsselung nicht realisierbar.

Verschlüsselungsverfahren können insbesondere die folgenden Leistungen erbringen:

- Schutz der Kommunikation sowie von ge-

speicherten Daten und Nachrichten vor unberechtigter Kenntnisnahme durch Verschlüsselung der Daten (Konzelation). Ziel: Nachrichtenvertraulichkeit.

- Schutz der Kommunikation vor Veränderung und Manipulation der Daten und Nachrichten,. Ziel: Integrität der Nachrichten.
- Zugriffskontrolle mit Identifizierung und Authentifizierung.
- Weiterhin Kennzeichnung der Authentizität des Absenders und ggf. seiner rechtlich bindenden Willenserklärung: Die digitale Signierung von Dokumenten kann zur Erzeugung einer rechtlich bindenden Willenserklärung benutzt werden. Um die digitale Signatur einer natürlichen oder juristischen Person zuordnen zu können, muß sie für jedermann erkennbar und nachvollziehbar von einer vertrauenswürdigen Instanz (Trust Center) zertifiziert werden.

Digitale Signatur

Technisch wird die digitale Signatur mit den sog. asymmetrischen Verfahren vorgenommen. Der Anwender verschlüsselt mit einem nur ihm bekannten (sog. geheimen) Schlüssel die Nachricht und übermittelt das Ergebnis (die digitale Signatur) zusätzlich als seine "Unterschrift". Berechtigte Leser der Nachricht kennen den sog. öffentlichen Schlüssel oder können ihn beim Trust Center erfragen oder ihn auch öffentlichen Schlüsselverzeichnissen entnehmen und mit diesem Schlüssel die digitale Signatur nachprüfen. Damit erkennen sie die Nachricht als authentische dieses Senders.

Da der geheime Schlüssel (hoffentlich) vom Sender geheimgehalten wird, kennt ihn niemand anderes. Daher kann auch niemand die digitale Signatur nachmachen und damit fälschen. Allerdings kann sie jeder leicht nachprüfen.

Steganografie

Seit langem sind Verfahren bekannt, die ein Verstecken von Nachrichten in normalem Text ermöglichen; dies wird als Steganografie bezeichnet. Bei diesem Verfahren ist gar nicht erkennbar, daß - neben dem übertragenen normalen Text - Informationen übertragen werden, die Dritte nicht sehen sollen. Sofern das Risiko besteht, daß die versteckten Nachrichten zufällig offenbar werden, können sie vor dem Verstecken verschlüsselt werden.

Daraus folgt, daß ein womöglich gesetzlich geregeltes Verschlüsselungsverfahren und damit das Verbot anderer Techniken nicht greift: Steganografie kann kaum bemerkt werden. Ein Gesetzesverstoß könnte nur schwer nachgewiesen werden.

Darüberhinaus sinkt der Widerstandswert von Verschlüsselungsverfahren Technologiebedingt rasch. Diese "Verfallsgeschwindigkeit" hat nicht nur Auswirkungen auf die Verschlüsselung von Nachrichten mit dem Ziel der Vertraulichkeit sondern z.B. auch auf die Gültigkeitsdauer einer digitalen Signatur, die nach Ablauf dieser Dauer fälschbar und auch nicht mehr überprüfbar ist. Diese Probleme könnten zukünftig andersartige Sicherheitsverfahren notwendig machen.

Insgesamt wird von Wirtschaftsverbänden die weiterhin freie Wahl von Verschlüsselungsverfahren und Schlüsseln (und Schlüsselverteilung) gefordert; die Verfahren sollten wahlweise in Hardware oder Software implementiert werden und international standardisiert werden.

Gerade die international einheitliche Handhabung ist angesichts der weltweiten unternehmerischen Aktivitäten unabdingbar. Anderenfalls wäre ein grenzüberschreitender Datenverkehr nur ungeschützt möglich. Bereits heute übertragen sicherheitsbewußte Unternehmen ihre wichtigsten Daten nicht über Netze und speichern ihre wichtigsten Daten auch nicht auf Rechnern, die an Netze - auch nur sporadisch - angeschlossen sind.

5.3 Interessenlage der Strafverfolgungs- und Sicherheitsbehörden

Computer sind seit einiger Zeit so billig, leistungsfähig und klein, daß die derzeit bekannten Verschlüsselungsverfahren fast beliebig genutzt werden können.

Seit einigen Jahren beklagen die Strafverfolgungsbehörden und auch die im Vorfeld arbeitenden Nachrichtendienste der Industriestaaten denn auch ihre Unfähigkeit, mit den oben geschilderten Verschlüsselungsverfahren verschlüsselte Nachrichten mitlesen zu können; dies erscheint ihnen deswegen notwendig, weil die international aktive - meist organisierte - Kriminalität überwiegend verschlüsselt kommuniziert.

Strafverfolgungsbehörden behaupten damit ihr Unvermögen, Kommunikation im wünschenswerten Umfang zu überwachen. Diese Behauptung kann von der Öffentlichkeit nicht

verifiziert werden. Eine weitere Schwachstelle dieser Argumentation ist die fehlende Darstellung oder der Nachweis des Zielerreichungsgrads, die Erläuterung der Erfolgsquote oder generell die Wirtschaftlichkeit der durchgeführten Abhörmaßnahmen.

5.4 Initiative der USA

Key-Escrowing

Daher fordern die Strafverfolgungsbehörden die Hinterlegung des zur Verschlüsselung benutzten Schlüssels bei einer staatlichen Instanz, um (nach einer richterlichen Anordnung) auf den hinterlegten Schlüssel zugreifen zu können und die übertragenen Nachrichten entschlüsseln zu können.

Im sog. Key-Escrow-Verfahren wird der benutzte Schlüssel aus Sicherheitsgründen nicht bei einer einzigen staatlichen Instanz hinterlegt, sondern wird in Teile (mindestens zwei) zerlegt und die Teile werden bei verschiedenen Instanzen hinterlegt. Damit soll also erreicht werden, daß Unberechtigte sich nicht des Schlüssels bemächtigen können und die Nachrichten des Betroffenen entschlüsseln können. Der bekannteste Vorschlag dazu kommt aus den USA unter dem Namen Clipper und kann in der Telefonkommunikation eingesetzt werden. Zur Datenverschlüsselung wird ein verwandtes Verfahren namens CAPSTONE eingesetzt. In den USA wird dieses Verfahren im Behördenbereich seit Oktober 1995 eingesetzt; das gesamte Verschlüsselungsverfahren ("FORTEZZA") ist auf einer Chipkarte realisiert.

Um wirksam sein zu können müßte das Key-Escrow-Verfahren für alle verbindlich gemacht werden. Die Kommunikation derjenigen, die sich nicht an diese Vereinbarung halten, kann dann gleichwohl nicht überwacht werden. Es kann darüberhinaus gar nicht erkannt werden, ob sich jemand an die Vereinbarung hält oder nicht. Dies sind kaum erfüllbare Voraussetzungen.

Die Strafverfolgungsbehörden, Nachrichtendienste und die deren Interessen vertretenden Behörden fordern daher unter Federführung der USA dreierlei:

1. Grundsätzlich müssen Verschlüsselungsverfahren in Produkten so schwach sein, daß sie (ohne Kenntnis des Schlüssels) von diesen Behörden gebrochen werden können und jegliche Kommunikation mitgelesen werden kann. Dies gilt insbesondere für die internationale Kommunikation. Bei diesem Vorgehen liegt allerdings ein Nachteil in der Tatsache, daß außer den Sicherheitsbehörden des exportierenden Landes auch andere, die derart schwach verschlüsselte Kommunikation entschlüsseln können.
2. Eine Verwendung starker Verfahren durch Nutzer des eigenen Landes (heimische Wirtschaft) soll zulässig sein, wenn die benutzten Schlüssel bei den Behörden hinterlegt werden.
3. Um internationale Kommunikation zu ermöglichen, werden "befreundete" Staaten und deren Private, Unternehmen und Behörden so behandelt, als seien sie Nutzer des eigenen Landes. Dies könnte beispielsweise für die NATO-Mitgliedsstaaten gelten.

Dieser dreigliedrige Vorschlag der USA ("ESCROW" und "Clipper") birgt sieben bisher ungelöste Probleme:

1. Voraussetzung für die Wirksamkeit des Verfahrens ist, daß auch das sog. internationale organisierte Verbrechen genau dieses Verfahren anwendet - und nicht etwa ein anderes - und auch die zutreffenden Schlüssel einer Hinterlegungsbehörde mitteilt und nicht etwa modifizierte oder andere Schlüssel einsetzt. Vorausgesetzt wird weiterhin, daß der Nutzer nicht bereits vor Einsatz des (zugelassenen) Verfahrens seine Daten mit einem anderen Verfahren verschlüsselt hat. Überhaupt ist Voraussetzung, daß keine anderen Verfahren als dieses staatlich zugelassene benutzt werden. Eine Reihe von Staaten planen daher einen Genehmigungsvorbehalt für Kryptoprodukte. Eine kühne Forderung angesichts der mehr als 700 verschiedenen Verschlüsselungsgeräte und -programme, die von mehr als 300 Unternehmen aus 33 Ländern der Erde weltweit vertrieben werden.
2. Kommunikation mit Drittländern kann nur mit schwachen Verschlüsselungsverfahren durchgeführt werden; diese Kommunikation kann dann allerdings von Dritten entschlüsselt und mitgelesen werden. Dieser Verzicht auf den Einsatz moderner Technologie erscheint vielen unzumutbar, weil er Wettbewerbsnachteile zur Folge haben dürfte (Konkurrenz liest mit!).
3. Der Anwender kann die Qualität der benutzten Verschlüsselungsalgorithmen sowie die des gesamten Verfahrens nicht beurteilen - der Algorithmus ist als Verschlußsache (SECRET, NOFORN) einge-

stuft und damit unzugänglich. Differenzierte Qualitätsbeurteilungen sind nicht veröffentlicht. Gerade an Bewertungsparametern, Evaluierungen unabhängiger Institutionen und staatlichen Zertifikaten für Verschlüsselungsprodukte sind Anwender in hohem Maße interessiert. Darüberhinaus können zukünftige eingehendere Untersuchungen des Verschlüsselungsalgorithmus doch noch eine (evtl. auch von den Entwicklern nicht beabsichtigte) "Falltür" offenlegen. Dann bliebe nur noch die Hoffnung, daß das Wissen um die Falltür nicht in "unberechtigte" Hände fällt - oder doch zumindest frühzeitig veröffentlicht wird.

4. Der den Algorithmus speichernde Chip soll sich bei Ausleseversuchen selbst zerstören. Dabei stellt sich die Frage, ob der Algorithmus nicht bereits ausgelesen worden ist oder auf anderem Wege in Erfahrung gebracht wurde. Schließlich kennen bereits heute viele Mitarbeiter der Behörden und der entwickelnden und produzierenden Unternehmen den Algorithmus und seine Implementierung. In jedem Fall dürften dem Adressaten dieser Sicherheitsmaßnahmen - dem internationalen organisierten Verbrechen - hinreichend große Geldbeträge zur Finanzierung von Untersuchungen des Chips sowie zum Nachbau zur Verfügung stehen. Ein Nachbau ist um so "sinnvoller" als das Verfahren selbst als sicher bezeichnet wird. Weiterhin ist das Vertrauen von Privaten und Unternehmen in die Hinterlegungsbehörde(n) begrenzt. An die Verfassungsverträglichkeit müßten besondere Anforderungen gestellt werden.
5. Die Hinterlegungsinstanz - auch als trust center bezeichnet - trägt in jedem Fall ein unvergleichlich hohes Risiko, weil hier *alle* Schlüssel der Nation oder Nationen konzentriert sind. Der Angreifer, der diese Schlüsselzentralen klassisch-materiell oder DV-technisch knackt, kann alle privaten und wirtschaftlichen Informationen dieser Nationen unberechtigt mitlesen. Dies betrifft jegliche Informationen, die in der Vergangenheit gespeichert und übertragen wurden und in Zukunft verarbeitet werden - jedenfalls mindestens bis zur Entdeckung des erfolgreichen Angriffs. Durch die Errichtung von zwei Hinterlegungsbehörden kann das Sicherheitsrisiko der trust center nur graduell gesenkt werden.
6. Außerdem wird die Möglichkeit der "unendlichen" legalisierten Abhöraktion gesehen, weil ein zurückgegebener Schlüssel gleichwohl weiterhin - und zwar dann unkontrolliert - zum Abhören benutzt werden kann.
7. Der im Chip gespeicherte Serienschlüssel ermöglicht die Identifikation und auch eine Lokalisierung von Sender und Empfänger - auch im Mobilfunk.

Diese Aspekte - und sicherlich noch eine Reihe weiterer - sollten in einer breiten öffentlichen Diskussion mit dem Ziel einer demokratischen Konsensbildung dargestellt und gegeneinander abgewogen werden. Diskutiert werden müßten die technischen Probleme und Möglichkeiten (u.a. Informationssicherheit) und die politischen Implikationen - insbesondere die Datenschutz- und Persönlichkeitsrechte sowie Staatsschutz und Innere Sicherheit tangierenden Aspekte - sowie die Anforderungen der Unternehmen.

5.5 Weitere Entwicklung in den USA

Die US-Regierung hat in jüngerer Zeit als Kompromiß die folgenden Kriterien für den Export von Verschlüsselungssoftware vorgeschlagen (NIST, 1995):

1. Offener - nicht als Verschlußsache eingestufter - Algorithmus mit 64 Bit Schlüssellänge eines Key Escrow Systems.
2. Unterstützung der Mehrfachverschlüsselung.
3. Der Key Escrow Mechanismus muß einen hohen Widerstandswert gegen Manipulationsversuche des Benutzers aufweisen. Nach einer evtl. erfolgten Manipulation soll die Verschlüsselungsfunktion nicht mehr nutzbar sein.
4. Die Escrow Agenten bedürfen einer Zulassung durch die US-Regierung oder einer anderen Regierung, die allerdings den Zugriff auf die Nachrichten unter dem Gesichtspunkt der gegenseitigen Amtshilfe der Behörden für nationale Sicherheit sowie der Strafverfolgungsbehörden gewährleisten soll.

Verschlüsselung wird heute von Unternehmen und Regierungen sowie zunehmend von Privaten als eine unersetzliche Sicherheitsmaßnahme in der GII angesehen, um Nachrichten vertraulich behandeln zu können und Nachrichten rechtlich verbindlich den Sendern und Empfängern zuordnen zu können.

5.6 Electronic Borders

Unter diesem Begriff wird derzeit die Forderung nach einer - auch inhaltlichen - Kontrolle

des gesamten Netzverkehrs an den Grenzen in den USA diskutiert. Gefordert wird insbesondere:

1. Kontrollierbare Gateways, Bridges und Router an den Zugängen zum US-amerikanischen Internet.
2. Spezielle Überwachungsrechner sollen Eindringversuche und programmgesteuerte Angriffe erkennen.
3. Gegenüber Angreifern sollen aktive Abwehrmaßnahmen ergriffen werden.

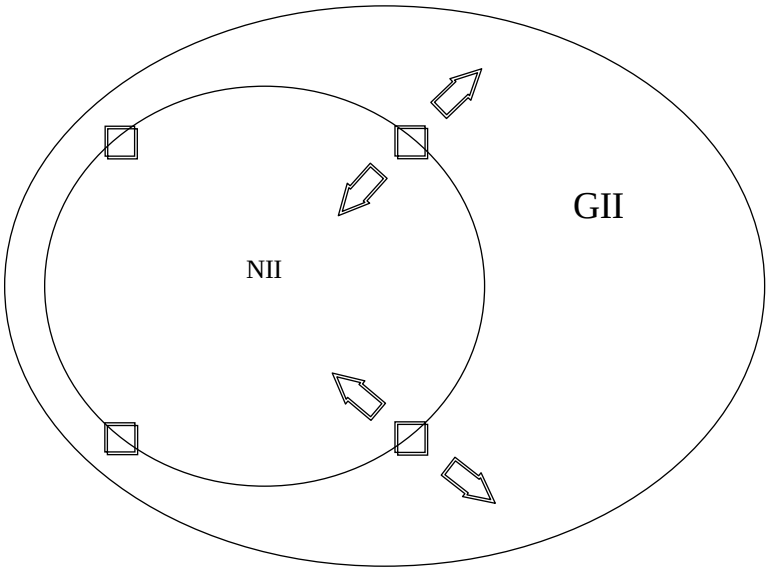

Abbildung 5: Kontrollierende Grenzrechner zwischen US-NII und GII.

Diese Forderung erscheint recht weitgehend. Sie ist allerdings nicht neu. Bereits vor Jahren wurde sie von militärischen Stellen erhoben und schließlich auf das sog. Milnet eingeschränkt.

Ein weiterer "Vorteil" derartiger border computer liegt darin, inhaltlich die internationalen Datenströme kontrollieren zu können und damit auch wirtschaftlich relevante Informationen auffangen und den heimischen Unternehmen zur Verfügung stellen zu können. Dabei gehen die Urheber des Vorschlags davon aus, daß sie die verschlüsselt übertragenen Nachrichten entschlüsseln können.

Weiterhin wäre die Erhebung von Zöllen und Steuern auf Daten-Im- und -Exporte möglich - aus fiskalischer Sicht sicherlich eine interessante Perspektive. Natürlich wäre auch der Aufbau von Kommunikationsprofilen der Kommunikation von Privaten, Behörden, Institutionen und Unternehmen möglich.

Eine grundsätzlich unterschiedliche US-amerikanische Sicht macht sich auch in der Begriffsnutzung bemerkbar: Grundsätzlich wird von der anzustrebenden National Information Infrastructure (NII) gesprochen - erst in zweiter Linie wird die weltweite Struktur untersucht.

6 Handlungsoptionen für die anstehenden Entscheidungen

6.1 Gesellschaftliche Regelungen zur Steuerung der GII

Um die oben dargestellten Sachziele der Informationssicherheit erreichen zu können werden einige Regelungen notwendig werden wie z.B. zur

- Abwicklung des Datenverkehrs (ggf. ein "Netz-Führerschein"), Formulierung von Mißbrauchstatbeständen und Sanktionen bei Fehlverhalten.
- Einrichtung von Organen zur Sicherstellung des Betriebs sowie der Verfolgung von Mißbrauch sowie Entwicklung von wirkungsvollen Tools zur Erkennung von Fehlverhalten und Mißbrauch zur Unterstützung der Strafverfolgungsbehörden.
- Sanktionen (technische, organisatorische, ...) bei Mißbrauch.
- Die freie Nutzung der GII darf dabei durch

die Aktivitäten der nationalen - und ggf. internationalen - Strafverfolgungsbehörden nicht behindert oder gar verhindert werden.

Neben den erwähnten technischen Maßnahmen dürften Entscheidungen über gesellschaftliche Regelungen zur Steuerung der GII notwendig werden: Nutzungseinschränkungen auf der Grundlage von Gesetzen in bestimmten Fällen wie Katastrophen sowie zum Jugendschutz.

Drei Aktivitätsbereiche können - gegliedert nach den möglichen Aufgabenerfüllern - formuliert werden:

- Koordinierung durch die Regierungen der angeschlossenen Staaten:
  - Copyright,
  - Filtern anstößiger Informationen.
- Regulation durch die Regierungen:
  - elektronisches Geld, Zölle und Steuern,
  - Internationales Recht der GII,
  - Strafrecht,
  - Kooperation der Strafverfolgungsbehörden.
- Privater Bereich:
  - Zugriffskontrollen, Netzzugänge und Übergänge zwischen Netzen,
  - Verschlüsselungsverfahren, Kopierschutz.

Zum allgemeinen Vorgehen bei der Errichtung der GII erscheint es von besonderer Bedeutung, Verfahren zu entwickeln, mit deren Hilfe Sicherheitsprobleme frühzeitig erkannt und analysiert werden - spätestens bei ihrem ersten Auftreten. Wegen der globalen Bedeutung der GII können Maßnahmen nicht einzelnen Personen oder auch nur einzelnen Staaten oder einzelnen Bündnissen überlassen werden.

6.2 Sicherheit als Killer-Funktion

Zu den entscheidenden Eigenschaften der GII (Killer-Funktionen) sind die folgenden vier zu zählen. Ohne die Absicherung der Kommunikation gegen die oben dargestellten Risiken wird diese neue Großtechnologie von Unternehmen, Behörden und Privaten nicht angenommen werden:

1. **Benutzerakzeptanz:** Akzeptanz von Sicherheitsmaßnahmen. Zu den quantitativ zu bewertenden Eigenschaften ist die Antwortzeit des Systems - auch **Geschwindigkeit** und insbesondere die Übertragungsgeschwindigkeit bei Anwendung der Sicherheitsmaßnahmen zu zählen. Die Bandbreite der Übertragungskanäle ist dann von Bedeutung, wenn bestimmte Datenmengen in festgelegten Zeitabschnitten übertragen werden sollen. Als Beispiel können hier alle Bewegtbilder wie Video oder Film genannt werden; mindestens die sich ändernden Teile des Bildes müssen übertragen werden, um den Effekt von etwa 20 Bildern pro Sekunde beim Anwender zu erreichen. Dazu kommen weitere technische, organisatorische, soziale Akzeptanzaspekte wie die Auswirkungen auf Einzelne, Familien, Vereinigungen und Unternehmen.
2. **Sachziele** der Informationssicherheit: Identifizierung und Authentifizierung der Anwender und nachprüfbare Bestätigung der Rechtsverbindlichkeit von Aktivitäten wie Senden, Empfangen, Anbieten, Verträge schließen (kaufen, versteigern etc.). Dies soll alles auch ohne Namensnennung (wenn der Käufer nicht explizit in Erscheinung treten will) also anonym oder auch unter einem Pseudonym möglich sein. Das Pseudonym kann dann nur von einem ausgewählten Kreis einer Person zugeordnet werden.
3. **Finanzierung**: Die grundlegenden Sicherheitsmaßnahmen in der GII müssen jedem Anwender zu angemessenen Preisen zur Verfügung gestellt werden. Darüberhinaus müssen qualitativ differenzierte Sicherheitsmaßnahmen angeboten werden.
4. **Rechtliche Aspekte** im Bereich Arbeitsrecht, Urheberrecht, Vertragsrecht bedürfen dringend einer Klärung. So kann derzeit jedermann Kopien von Daten anfertigen, ohne daß der eigentliche Urheber erkennbar geschützt ist.
5. Ausgehend von den USA mit den Trusted Computer Security Evaluation Criteria (TCSEC), dem sog. Orange Book wurden später auch von europäischen Staaten **Kriterien** zur Bewertung der Vertrauenswürdigkeit von Programmen

und Systemen entwickelt. Derartige Kriterien müssen auch genormt werden. Die derzeitige internationale Entwicklung der sog. Common Criteria erscheint als ein gangbarer Schritt in diese Richtung. Wesentliches Kriterium aus der Sicht der Anwender ist die Gliederung des Prozesses in die beiden folgenden Schritte: Evaluierung von Produkten durch unabhängige Stellen (Third Parties) und Zertifizierung durch gesetzlich beauftragte staatliche Stellen.

Im Bereich der Bewertungskriterien bedarf es allerdings noch einer intensiven Beschäftigung mit Netzwerkaspekten und erst recht mit den Sicherheitsaspekten der GII.

Einer simplen Herstellererklärung ("sicheres Produkt") dürften Anwender kaum trauen.

Eine befriedigende Lösung der Probleme der Informationssicherheit ist insgesamt also eine grundlegende Voraussetzung für die Realisierung der Vorstellungen zu einer zukünftigen Informationsgesellschaft. Sie ist wichtig für den Endbenutzer, weil er die vielfältigen Angebote der GII nur dann annehmen wird, wenn er der Sicherheit (z.B. Vertraulichkeit, Integrität und Verfügbarkeit) der technischen Produkte und Dienste vertrauen kann. Für die Hersteller und Vertreiber der erforderlichen Produkte und Dienste besteht die Notwendigkeit, dieses Vertrauen durch geeignete Entwicklungen zu erreichen. Flankierende Maßnahmen in anderen Bereichen wie z.B. im Bereich der Gesetzgebung werden möglicherweise ebenfalls erforderlich werden.

Offene Diskussion

Im Gegensatz zu den USA fehlt in der Bundesrepublik und - soweit hier übersehbar - auch insgesamt in der Europäischen Union bisher eine entsprechende offene Diskussion der Informationssicherheit im Zusammenhang mit dem Weg Europas in die Informationsgesellschaft. Diese Diskussion mit dem Ziel einer Sicherheitsarchitektur muß frühzeitig geführt werden: Es kommt darauf an, in dieser Diskussion Sicherheitsprobleme aufzuzeigen und insbesondere auch Lösungen für die Sicherheitsprobleme anzubieten.

Literatur:

Bangemann, M. et al.: Recommendations to the European Council: Europe and the global information society. Brüssel 1994

Common Criteria Editorial Board (Hrsg.): Common Criteria for Information Technology Security Evaluation. CCEB-95/055. Version 0.92 95/08/30

Computer Science and Telecommunications Board - Commission on Physical Sciences, Mathematics, and Applications - National Research Council: Realizing the Information Future. The Internet and Beyond. Washington 1994

Computer Security Institute (CSI): Internet Security Survey. San Francisco 1995

Denning, D.: The Future of Cryptography. Internet Security Review 10, 4 - 14, 1995

Deutscher Bundestag: Gesetz über die Errichtung des Bundesamtes für die Sicherheit in der Informationstechnik (BSIG) vom 17. Dezember 1990, BGBl. I S. 2834

DIN (Hrsg.): Evaluation Criteria for IT Security; Part 2: Functionality of IT Systems, Products and Components. Working Draft. ISO/IEC JTC 1/SC 27 N1133. NI-27c/110-95. Berlin 1. Juni 1995

Hoffmann, L.J. (Ed.): Building in Big Brother. The Cryptographic Policy Debate. New York 1995

International Chamber of Commerce - ICC: ICC Position Paper on International Encryption Policy. Paris 1994

Krüger, G.: Telekommunikation Informatik Spektrum 18, 256 - 262, 1995

Möller, S.; Pfitzmann, A.; Stierand, I.: Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist. Datenschutz und Datensicherung 6, 318 - 326, 1994

Molini, J.: Border Computer. Closing Plenary "Security Challenges for the National Information Infrastructure and for Reinventing Government". 18. National Information Systems Security Conference. Baltimore 1995

National Institute for Standards and Technology (NIST): New Government Software Export Criteria. NIST, Gaithersburg, Maryland, September 6, 1995

NTIA NII Office: The National Information Infrastructure: Agenda for Action. Washington 1994

Organisation for Economic Co-operation and Development - OECD (Ed.): Guidelines for the Security of Information Systems. OCDE / GD (92)190. Paris 1992

Organisation for Economic Co-operation and Development - OECD (Ed.): Proposal for a business-government forum on global cryptography policy. Paris 1995

Pohl, H.: Einige Bemerkungen zu Anforderun-

gen, Nutzen und staatlicher Reglementierung beim Einsatz von Verschlüsselungsverfahren. In: Brüggemann, H.H. (Hrsg.): Verläßliche IT-Systeme. 4. GI-Fachtagung VIS '95. Wiesbaden 1995

Pohl, H.: Definition der Security Level bei Fernwartung und Outsourcing. BvD Kongreß. In: Kongehl, G. et al. (Hrsg.): Datenschutz 5 vor 2000. Europa und die Global Information Infrastructure. Ulm 1995

Pohl, H.: Harmonisation and Standardisation Aspects and the European Community. Eingeladener Vortrag für den Oxbridge Sessions Annual Summit on Secure System Development. The Hague 1991.

Pohl, H.: Organisatorische und technische Aspekte der Informationssicherheit als Aufgabe des Datenschutzbeauftragten. In: Simsek, E., Kongehl, G. (Hrsg.): Die Zukunft des Datenschutzbeauftragten – Praxisnaher Datenschutz oder EG-Bürokratie. Ulm 1993

Pohl, H.: Unternehmensübergreifende Sicherheitsarchitekturen - Entwicklung und Realisierung. In: Hammer, K.; Schmolke, D.; Stuchlik, F.: Synergie durch Netze. Fachtagung der Otto-von-Guericke-Universität Magdeburg. 1995

Pohl, H. et al.: Zur Computerkriminalität im 5. Strafrechtsänderungsgesetz (5. StÄG) der DDR und 2. Gesetz zur Bekämpfung der Wirtschaftskriminalität (2. WiKG) der Bundesrepublik aus der Sicht der Informationstechnik. Datenschutz und Datensicherung Teil 1: 10, 493 - 497, 1990 und Teil 2: 11, 551 - 558, 1990

Pohl, H.; Hütte, L.: Computer-Spionage: Ist die Katastrophe unvermeidbar? Journal für Wirtschaft und Gesellschaft - bonntendenz 4, III 1989

Pohl, H; Weck, G.: Stand Zukunft der Informationssicherheit. In: Pohl, H.; Weck, G. (Hrsg.): Einführung in die Informationssicherheit. München 1993.

Pohl, H.; Weck, G. (Hrsg.): Internationale Sicherheitskriterien. Kriterien zur Bewertung der Vertrauenswürdigkeit von IT-Systemen sowie von Entwicklungs- und Prüfumgebungen. München 1993

Pohl, H.; Weck, G. (Hrsg.): Managementaufgaben im Bereich der Informationssicherheit. München 1995

Pohl, H.; Weck, G. (Hrsg.): Strategische Aspekte der Informationssicherheit und staatliche Reglementierung. München 1995

Rheingold, H.: Virtuelle Welten - Reisen im Cyberspace. Reinbek 1995

Ross, J. A.: Crypto in Europe - Markets, Law and Policy. Working Paper des Special Interest Network". Paper for the Cryptography Policy and Algorithms Conference. Queensland 1995

Roßnagel, A.; Wedde, P.; Hammer, V.; Pordesch, U.: Die Verletzlichkeit der "Informationsgesellschaft". Opladen 1989

Roßnagel, A.; Bizer, J.; Hammer, V.; Kumbruck, C.; Pordesch, U.; Schneider, M. J. (Hrsg.): Soziale und politische Implikationen einer künftigen Sicherungsinfrastruktur. provet Arbeitspapier 150. Darmstadt 1994

Security Study Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences Mathematics, and Applications: Computers at Risk. Safe Computing in the Information Age. Washington 1991

Voßbein, R. (Hrsg.): Organisation sicherer Informationsverarbeitungssysteme. München 1995

Waffender, M.: CYBERSPACE - Ausflüge in virtuelle Wirklichkeiten. Reinbek 1993

Wiener, M.: DES Breaking Machine. Proceedings of the Crypto ´93. Berlin 1994

Winkelhage, J.: Karriere-Gespräch mit Telekom-Vorstand Hagen Hultzsch "Wir brauchen Visionäre auf allen Ebenen". Handelsblatt 27. Okt. 1995

o - o