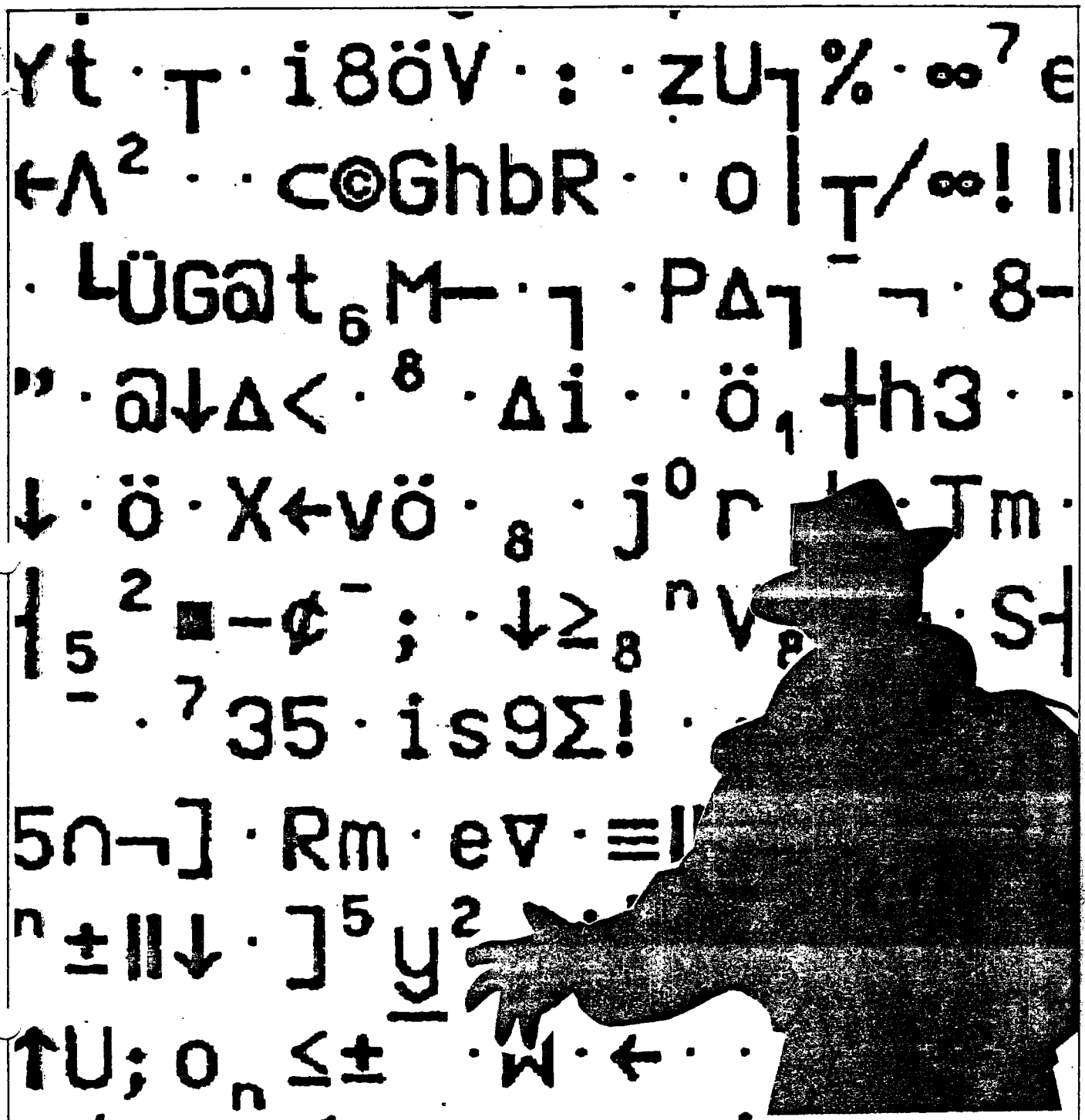

Johann Bizer
Volker Hammer
Ulrich Pordesch
Alexander Roßnagel

DAS NEUE BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

Planung - Kritik - Vorschläge

Gutachten
Im Auftrag der Fraktion

DIE GRÜNEN
IM BUNDESTAG

HerausgeberInnen

DIE GRÜNEN
IM BUNDESTAG

v.i.S.d.P.
Bärbel Rust MdB
Manfred Such MdB

Das Gutachten ist zu
beziehen über:

DIE GRÜNEN IM BUNDESTAG
Arbeitskreis VII -
Bildung, Wissenschaft
und Forschung
Barbara Böttger
Bundeshaus -
Hochhaus im Tulpenfeld
5300 Bonn 1

Bonn, im März 1990

Vorbemerkung

Nach dem Gesetzentwurf "zur Fortentwicklung der Datenverarbeitung und des Datenschutzes", der auch die Arbeit der Sicherheitsbehörden (Verfassungsschutz, Bundesnachrichtendienst und Militärischer Abschirmdienst) regeln soll und dem Poststrukturgesetz, in dem durch eine Änderung von Art. 10 GG die Kontrolle des Fernmeldeverkehrs erheblich ausgeweitet wird, folgt nun als dritter Streich seitens der Bundesregierung der "Entwurf eines Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik" (BSI-Errichtungsgesetz, verabschiedet vom Bundeskabinett am 21.2.1990).

Ob diese 1991 zu errichtende Oberste Bundesbehörde allerdings ihre selbstgestellte Aufgabe, die Sicherheit in der Informationstechnik zu fördern, auszufüllen imstande sein wird, ist hochgradig zweifelhaft. Eher steht zu befürchten, daß unter dem Mantel der Kompetenzerweiterung und Öffnung der zum BSI umgewandelten bisherigen "Zentralstelle für Sicherheit in der Informationstechnik - ZSI (bis zum 1.6.1989 hieß sie eindeutiger "Zentralstelle für das Chiffrierwesen"), die dem BND zugeordnet ist, faktisch ein **neuer "ziviler Geheimdienst"** entsteht, der die Verschlüsselungscodes, die er produziert, selbstverständlich auch über den Bereich der "nationalen Sicherheitsinteressen" hinaus im privaten und öffentlichen Bereich knacken kann.

Obwohl die Aufgabe der Dechiffrierung offiziell bei der alten ZSI im BND bleiben soll, erweckt die sonstige Tätigkeit des "Oberlauschers der Nation" z.B. bei der Bespitzelung des Atomwissenschaftlers Traube, des Schriftstellers Wallraff, unliebsamer Bundestagsabgeordneter und Bürgerinitiativen gerade nicht das Vertrauen, um das die Bundesregierung bei der Bewältigung der von ihr selbst zugestandenen Risiken durch die zunehmende Abhängigkeit von Informations- und Kommunikationstechniken (IuK-Techniken) wirbt.

Ähnlich wie bei dem rechtlich verbindlichen Zugriff auf nahezu alle Datenbestände öffentlicher und halböffentlicher Stellen durch die sogenannten Sicherheitsgesetze unter dem Mantel des Datenschutzes ist zu erwarten, daß hier unter dem Label "Sicherheit in der Informationstechnik" weniger dem Schutz der Privatsphäre und dem informationellen Selbstbestimmungsrecht als "elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens" entsprochen wird, wie es das Volkszählungsurteil bestimmt, sondern vielmehr dem Bedürfnis des Staates nach innnerer und äußerer Sicherheit und dem Wunsch nach Verbesserung der Wettbewerbsfähigkeit der bundesdeutschen Wirtschaft.

Die organisatorische Einbettung und Weisungsabhängigkeit des geplanten Bundesamtes vom Innenministerium als dem "Ministerium der Bundespolizei", die personelle Kontinuität der Mitarbeiter (153 Stellen beim ZSI werden umgewidmet zum BSI) und die eingeschränkte Aufgabenstellung lassen beunruhigende Parallelen zu den Erfahrungen mit der National Security Agency (NSA) in den USA durchaus als realistisch erscheinen:

Immerhin haben dort der öffentliche Protest und der Widerstand von Industrie, Banken und Wissenschaft dazu geführt, daß dem größten Geheimdienst der Welt die delikate Aufgabenkombination sowohl für sichere Verschlüsselungssysteme für die Wirtschaft als auch für die Überwachung verschlüsselter Informationen zuständig zu sein, zumindest formal entzogen wurde. An der schon Thomas Hobbes bekannten Tatsache, daß derjenige, der in der Lage ist, die Bürger zu schützen, damit auch fähig ist, sie zu verfolgen, änderte die Zuständigkeitsbeschränkung auf den Geheimbereich allerdings wenig. Kryptologen sind offenbar eine so seltene und teure Spezies, daß allein dieser Umstand unseren obersten Datenschützer zu einer milderen Beurteilung der eigentlich als zu intensiv empfundenen Beteiligung der alten ZSI am neuen BSI bewogen hat. So begrüßt der Bundesbeautragte für den Datenschutz bedauerlicherweise die Konzeption der Bundesregierung.

Die GRÜNEN machen sich hingegen die radikale und zugleich differenzierte Kritik des vorliegenden Gutachtens sowie die darin enthaltenen Alternativvorschläge zu eigen. Besonders hervorzuheben wären darin zwei Gesichtspunkte:

1. Die bisher völlig unzureichende Trennung des Bundesamtes vom militärischen und nachrichtendienstlichen Bereich muß durchgeführt werden.Eine solche zivile Bundesoberbehörde müßte weisungsunabhängig sein und bei der Beurteilung der Risiken und Schutzmaßnahmen hinreichend Öffentlichkeit gewährleisten, um den gegebenen Interessenkonflikt zwischen Staatssicherheit und Bürgersicherheit nicht einseitig zugunsten "nationaler Sicherheitsinteressen aufzulösen.
   Damit der Grundrechtsschutz der Bürger und die Anonymität und Vertraulichkeit übermittelter Nachrichten gesichert werden kann, darf es kein Prüfverfahren, kein Schlüsselmanagement und keine Chipkartenvergabe geben, die in erster Linie den Geheimschutzinteressen des Innenministeriums dienen.
   Stattdessen sollten die freiheitserweiternden Möglichkeiten der IuK-Techniken, wie sie z.B. das Public-Key-System anbieten, im Sinne einer Verringerung der Verletzlichkeit der Gesellschaft gefördert werden.

2. Der Begriff der Sicherheit darf nicht - wie im Gesetzentwurf vorgesehen - auf die Erhaltung von innerer und militärischer Sicherheit, Betriebssicherheit von IuK-Technik und die internationale Wettbewerbsfähigkeit reduziert werden. Es geht vielmehr um Handlungsvorschläge zur Verringerung der Verletzlichkeit der Gesellschaft und zur Wahrung der Interessen der Menschen als Staats-

bürger, Arbeitnehmer, Verbraucher und "Privatmenschen".

Denn in Zukunft werden die für das Leben in der Industriegesellschaft notwendigen Versorgungssysteme ausnahmslos von IuK-Technik gesteuert und damit von deren Funktionieren abhängig. Darüberhinaus werden immer mehr Lebensäußerungen und soziale Funktionen an informationstechnische System übertragen, Verhalten und Lebensgewohnheiten der Menschen werden verstärkt elektronischem Zugriff ausgeliefert. Um diesem rasanten und weitgehend anarchischen Informatisierungsprozeß entgegenzuwirken, muß zumindest

- ein gesellschaftlicher Konsens über die zukünftige Techniknutzung erzielt werden, um so auch die Angriffsmotive zu reduzieren,
- müssen technische und nichttechnische Alternativen erwogen werden, um die Abhängigkeit von IuK-Systemen und damit die Schadenspotentiale zu vermindern,
- muß die Technik so gestaltet werden, daß Angriffsmöglichkeiten und Beherrschbarkeitsprobleme geringer werden,
- müssen ausreichende Notfallplanungen vorgesehen werden.

Beispielsweise könnte dies bedeuten, daß das Bundesamt,

- jedem Anbieter und Anwender von IuK-Technik eine Anzeigepflicht im Sinne der oben genannten Ziele vorschreibt,
- einen jährlichen Bericht zur Entwicklung und Bewertung der Verletzlichkeit der Gesellschaft herausgibt,
- kritische Diskurse über die Einführung von IuK-Techniken initiiert,
- öffentliche Zulassungs- und Genehmigungsverfahren mit mit dem Ziel vorschreibt, daß für IuK-Systeme ebenso wie für Kraftfahrzeuge und Flugzeuge der jeweils festzulegende Mindeststandard an Sicherheit und Schadensvorsorge gewährleistet ist.

Barbara Böttger
AK VII, Bildung, Wissenschaft und Forschung

Zusammenfassung der Ergebnisse

Planungen und Hintergründe

Die Bundesregierung hat im November 1989 ein "Rahmenkonzept zur Gewährleistung der Sicherheit bei der Anwendung der Informationstechnik (IT) - IT-Sicherheitsrahmenkonzept" verabschiedet. Dieses Rahmenkonzept bildet den Hintergrund für den inzwischen vorgelegten Gesetzentwurf zur Errichtung eines Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die Schaffung des Bundesamtes kann als wichtigste Maßnahme innerhalb des Rahmenkonzeptes verstanden werden.

Das Rahmenkonzept benennt in seiner einleitenden Vorbemerkung zutreffend die zunehmende Abhängigkeit aller gesellschaftlichen Bereiche von der Informationstechnik und die Gefahren für die Vertraulichkeit der der Daten der Bürger und der Wirtschaft. Diese Problemsicht geht jedoch bei der Detaillierung der Probleme und der Formulierung der Zielsetzungen verloren. Das eigentliche Sicherheitsproblem liegt nicht in der Sicherheit der Informationstechnik, sondern - umfassender - in der Verletzlichkeit der Gesellschaft.[1] Denn das relevante Problem ist nicht die Unversehrtheit der Technik, sondern die Möglichkeit des Entstehens großer Schäden für das soziale und politische System durch den Mißbrauch oder die Unbeherrschbarkeit der Informationstechnik. Handlungskonzepte zur Verminderung der Verletzlichkeit müssen daher vor allem auf die Verringerung der gesellschaftlichen Abhängigkeit und Schadensfolgen, der Verminderung von Mißbrauchsmotiven und dem Ausschluß von Fehlerquellen zielen. Dies schließt ergänzende und begleitende Maßnahmen zur Erhöhung der technischen Sicherheit von IT-Systemen ein, ist jedoch keinesfalls darauf begrenzt.

Inhaltlich zeigen die aus dem Rahmenkonzept und dem Gesetztesentwurf ersichtlichen Zielsetzungen, daß es der Bundesregierung bei der Forcierung der Informatisierung der Gesellschaft in erster Linie um die begleitende Sicherstellung der internationalen Wettbewerbsfähigkeit, die Sicherung der Akzeptanz der Informations- und Kommunikations-Techniken und die Gewährleistung der "Inneren" und "Äußeren" Sicherheit geht. Die Gefahren für Bürgergrundrechte beim Gebrauch und Mißbrauch personenbezogener Daten durch private und staatliche IuK-Betreiber und das Gefährdungspotential für die Versorgung der Bevölkerung werden von der Bundesregierung überhaupt nicht thematisiert. Die Sicherheit der Bürger vor den Risiken der Informatisierung sozialer Funktionen und die Freiheits- und Demokratiekosten der dann unvermeidlichen Sicherungsmaßnahmen zählen nicht zu den gewählten Aufgabenstellungen.
Nicht nur die Zielsetzungen der Bundesregierung sind ungenügend, sondern auch die Lösungsansätze. So fehlt die Frage danach, wo und in welcher Form IuK-Technik künftig eingesetzt werden könnte, bzw. aus Risikogesichtspunkten auf einen Einsatz verzichtet werden sollte. Diese fehlende Zukunftsorienterung ist jedoch unumgänglich wenn künftige Abhängigkeiten, Schadenspotentiale,

[1] S. näher A.Roßnagel/P.Wedde/V.Hammer/U.Pordesch: Die Verletzlichkeit der Informationsgesellschaft, 2.Aufl. Opladen 1990.

Mißbrauchsmöglichkeiten und -motive abgeschätzt werden sollen. Statt bei der wachsenden Abhängigkeit der Gesellschaft von IuK-Technik mit dem ihr inhärenten Katastrophenpotential, beispielsweise beim Ausfall wichtiger Telekommunikationsdienste, anzusetzen wird das Problem zur Mißbrauchsverhinderung hin verschoben. Schadensmöglichkeiten, auch Sekundärschäden, für das soziale und politische System mit ihren Auswirkungen auf die Menschen bleiben gänzlich unberücksichtigt.
Dem zu engen Ansatz "Sicherheit der Informationstechnik" folgend sollen nur abstrakte "Angreifermodelle" gebildet, nicht aber die heutigen und künftigen Motive und Möglichkeiten potentieller Angreifer untersucht werden. Bei derartig unzureichenden Bedrohungsanalysen kann jedoch das heutige und künftige Sicherungsniveau nicht abgeschätzt werden. Wegen der hohen Investitions- und Betriebskosten unproduktiver Sicherheitsmaßnahmen hängt dies immer von der subjektiven Bedrohungseinschätzung nach vorher erfolgten Angriffen ab. Es liegt deshalb meist weit unter den (theoretischen) Sicherungs*möglichkeiten*. Nicht problematisiert wird die mangelnde Verläßlichkeit von Sicherungssystemen. Der Erfolg von Sicherungsmaßnahmen hängt jedoch von der Zuverlässigkeit organisatorischer und menschlicher Voraussetzungen ab, von denen sich beispielsweise in der Atomtechnik gezeigt hat, daß sie praktisch kaum zu gewährleisten sind.
Bei allen Überlegungen der Bundesregierung fehlt die Suche nach soziotechnischen Alternativlösungen oder nicht-technischen Lösungen zur Verminderung der Abhängigkeit und Erhöhung der Datensicherheit. Dabei bietet gerade die IuK-Technik ein breites Spektrum von Alternativlösungen, wie beispielsweise in wissenschaftlichen Untersuchungen zu datenschutzgerechten Telekommunikationsnetzen als Alternative zum Post-ISDN detailliert nachgewiesen wurde.
Nachteilige Effekte von Sicherungsmaßnahmen auf die Grundrechte von Arbeitnehmern, Netzteilnehmern oder sonstigen Betroffenen beispielsweise im Zusammenhang mit Zugangs- und Zugriffskontrollen werden nicht vorausschauend abgeschätzt. Durch das unkontrollierte Erzeugen von Sicherungszwängen wird jedoch die Gesellschaft zunehmend in das Dilemma getrieben, künftig zwischen Freiheit und Sicherheit entscheiden zu müssen. Dieser Mangel ist eine völlige Verkennung der gesellschaftspolitischen Dimension des Problems.
Dem Problem der Verletzlichkeit völlig unangemessen sind schließlich die im Rahmenkonzept und im Gesetzesentwurf vorgeschlagenen Maßnahmen. Notwendige aktive Steuerungsmaßnahmen werden abgelehnt. Nur im staatlichen Bereich sollen Richtlinien für die Verwendung 'sicherer' IuK-Technik erlassen werden. Für den nichtstaatlichen Bereich ersetzt das Hoffen auf den Markt erforderliche regulierende Eingriffe. Das Entstehen von Abhängigkeiten und großen Schadenspotentialen soll weder im staatlichen noch im nicht-staatlichen Bereich beeinflußt werden.
Im Ergebnis wird eine Politik, die Sicherheit ausschließlich durch nachträgliche und ergänzende Verbesserung einer als gegeben unterstellten Technik erreichen will, weder die Verletzlichkeit der Gesellschaft verringern, noch den bereits den auf die Belange der Wirtschaft und des Staates begrenzten Zielsetzungen des Rahmenkonzeptes gerecht werden können.

Nach dem vorliegenden Gesetztesentwurf soll das Bundesamt der Rechts- und Fachaufsicht des Bundesinnenministers unterstellt werden. Dieser kann damit in allen Verfahrens- und Sachangelegenheiten bindende Weisungen erteilen. Da dieser zugleich Aufsichtsbehörde für das Bundeskriminalamt, den Bundesgrenzschutz und den Verfassungsschutz ist, dürften intensive Beziehungen zu diesen Behörden zu erwarten sein. Zwar soll der für den staatlichen Geheimschutz wichtige Bereich der "Entzifferung", in Fortführung des BSI-Vorläufers Zentralstelle für das Chiffrierwesen (ZfCH) ausgegliedert und direkt dem Bundekanzleramt unterstellt werden, das für die Geheimdienste zuständig ist. Dennoch sind durch die personelle Kontinuität zwischen ZfCH und BSI und in Anbetracht des Mangels an Kryptoexperten fortdauernde Beziehungen zu den Geheimdiensten zu erwarten. Außerdem hat das Bundesamt weiterhin Leistungen im Bereich militärischer Sicherheit und staatlicher Geheimhaltung zu erbringen.
Durch die so festgeschriebenen und vorprogrammierten Verflechtungen zwischen Sicherheitsbehörden, Geheimdiensten und dem Bundesamt sind für die Zukunft Interessenkonflikte absehbar, die die Verletzlichkeit erhöhen und sich sehr nachteilhaft auf die Bürgersicherheit auswirken können. So sollen nach dem Rahmenkonzept für zertifizierte Produkte über den Bereich von Kryptosystemen hinaus Ausfuhr- und Vertriebsbeschränkungen angeordnet werden können. Damit besteht tendenziell die Gefahr, daß bestimmte Sicherheitsprodukte im zivilen Bereich nicht verwendet werden können und dort das technisch mögliche Sicherheitsniveau nicht erreicht wird.
Nachteile für die Bürgersicherheit könnten entstehen, wenn Sicherheitsbehörden über das Innenministerium oder direkt wirkungsvolle Verschlüsselungssysteme im zivilen Bereich blockieren, um sich Zugriffsmöglichkeiten auf Datenbanken, Telefon, Informationssysteme und andere IuK-Systeme zu erhalten. Die durch die IuK-Technik geschaffenen Möglichkeiten sicherer und anoymer Teletransaktionen, die den Schutz der Bürger vor Beobachtung und Verdatung garantieren, könnten durch diese Interessenkonstellation verhindert werden.
Die Sicherheit in der Informationstechnik ist von ähnlicher Bedeutung wie der Datenschutz. Die Unabhängigkeit der zuständigen Behörden ist daher ebenso im Interesse der Freiheitsgrundrechte des Bürgers und der Demokratie gefordert, wie im Interesse einer objektiven - hersteller- und anwenderunabhängigen - Begutachtung von Sicherheitsfragen. Dem BMI sollte daher lediglich die Rechtsaufsicht über das BSI zustehen.

Vorschläge und Forderungen
Während sich die Bundesregierung in ihrer Problemsicht bisher auf einen ausschließlich technischen Sicherheitsbegriff beschränkt und vor allem Wettbewerbsinteressen sowie die "Innere" und "Äußere" Sicherheit berücksichtigt, nehmen wir die Verletzlichkeit der Gesellschaft und die Interessen der Menschen als Staatsbürger und Verbraucher zum Ausgangspunkt unserer Überlegungen.
Ziel muß es sein die Entwicklung und den Einsatz informationstechnischer Systeme so zu beeinflussen, daß die Verletzlichkeit reduziert und nicht nur die Datensicherheit erhöht wird. Neben

Datensicherungsmaßnahmen geht es dabei vor allem darum
- für die künftige Techniknutzung einen breiten gesellschaftlichen Konsens zu suchen, um so Angriffsmotive zu reduzieren
- die gesellschaftliche Abhängigkeit von IuK-Systemen und damit die Schadenspotentiale zu verringern, indem soziotechnische Alternativen erwogen werden
- die Technik so zu gestalten, daß Angriffsmöglichkeiten und Beherrschbarkeitsprobleme reduziert werden, sowie
- ausreichende Notfallplanungen vorzusehen.

In Zukunft werden die für das Leben in der Industriegesellschaft notwendigen Versorgungssysteme ausnahmslos mit Hilfe von IuK-Technik gesteuert und sind von deren Funktionieren vollständig abhängig. Ein zentrales Anliegen jeder Sicherheitsstrategie muß daher die Gewährleistung der Daseinsvorsorge sein. Verletzlichkeitsuntersuchungen sind in allen wichtigen gesellschaftlichen Bereichen, wie z.B. bei der Geldwirtschaft, in Verwaltungen, bei der Prozeßsteuerung und Verkehrssystemen erforderlich. Bei IuK-Infrastruktursystemen, wie z.B. Telekommunikationsdiensten, muß die Entwicklung der Abhängigkeit der Gesellschaft ständig beobachtet werden, um ungewollte Entwicklungen frühzeitig zu erkennen. Beim weiteren Ausbau dieser Systeme sind unter dem Kriterium der Verletzlichkeit unterschiedliche Optionen zu entwickeln. öffentliche und private Betreiber müssen zur Einhaltung ausreichender Sicherheitsniveaus angehalten werden können. Bei Basistechniken komplexer IuK-Systeme reichen Sicherheitsstandards und Zertifizierungen nicht aus, um Vielfachschäden - beispielsweise durch Softwaremanipulationen - zu begrenzen. Deshalb muß beobachtet werden, welche Systemtypen in welchen Bereichen Einsatz finden, um gegebenenfalls durch steuernde Eingriffe für eine genügend große Diversifikation zu sorgen.

In der 'Informationsgesellschaft' erfolgen immer mehr Lebensäußerungen über vernetzte Systeme und werden immer mehr Daten gespeichert. Dadurch stehen die Verhaltensweisen und Lebensgewohnheiten der Menschen verstärkt elektronischem Zugriff offen. So werden gegenwärtig durch die Digitalisierung des Fernsprechnetzes und ISDN die Möglichkeiten des Zugriffs auf Nutz- und Verbindungsdaten wesentlich vereinfacht. Zur Gewährleistung der Bürgersicherheit und zum Schutz der informationellen und kommunikativen Selbstbestimmung müssen daher Techniken entwickelt werden, die Eingriffe in diese Grundrechte verhindern. Mit technischen Maßnahmen, wie dem Einsatz von Kryptoverfahren in Telekommunikationssystemen, der gezielten Schaffung von Inkompatibilitäten zwischen Systemen verschiedener Behörden und der Verpflichtung zu ausreichenden Zugriffsschutz- und Revisionssystemen ist ein garantierbarer und amthilfefester Datenschutz sicherzustellen.

Sicherheit in der Informationstechnik ist ferner notwendig, um die Verbraucher, Käufer, Anwender und Betroffenen von IuK-Technik zu schützen. Der Verbraucherschutz gegenüber Kundentransparenz und -manipulation könnte erheblich verbessert werden, wenn Teletransaktionen durch Kryptosysteme anonym und sicher abgewickelt werden könnten. Zur Verbesserung des Konsumentenschutzes sollten für bestimmte Produkte Zertifizierungen vorgeschrieben und an zertifizierte Produkte Haftungsregelungen geknüpft werden.

Die im Rahmenkonzept beschriebenen Aufgaben zur Gewährleistung