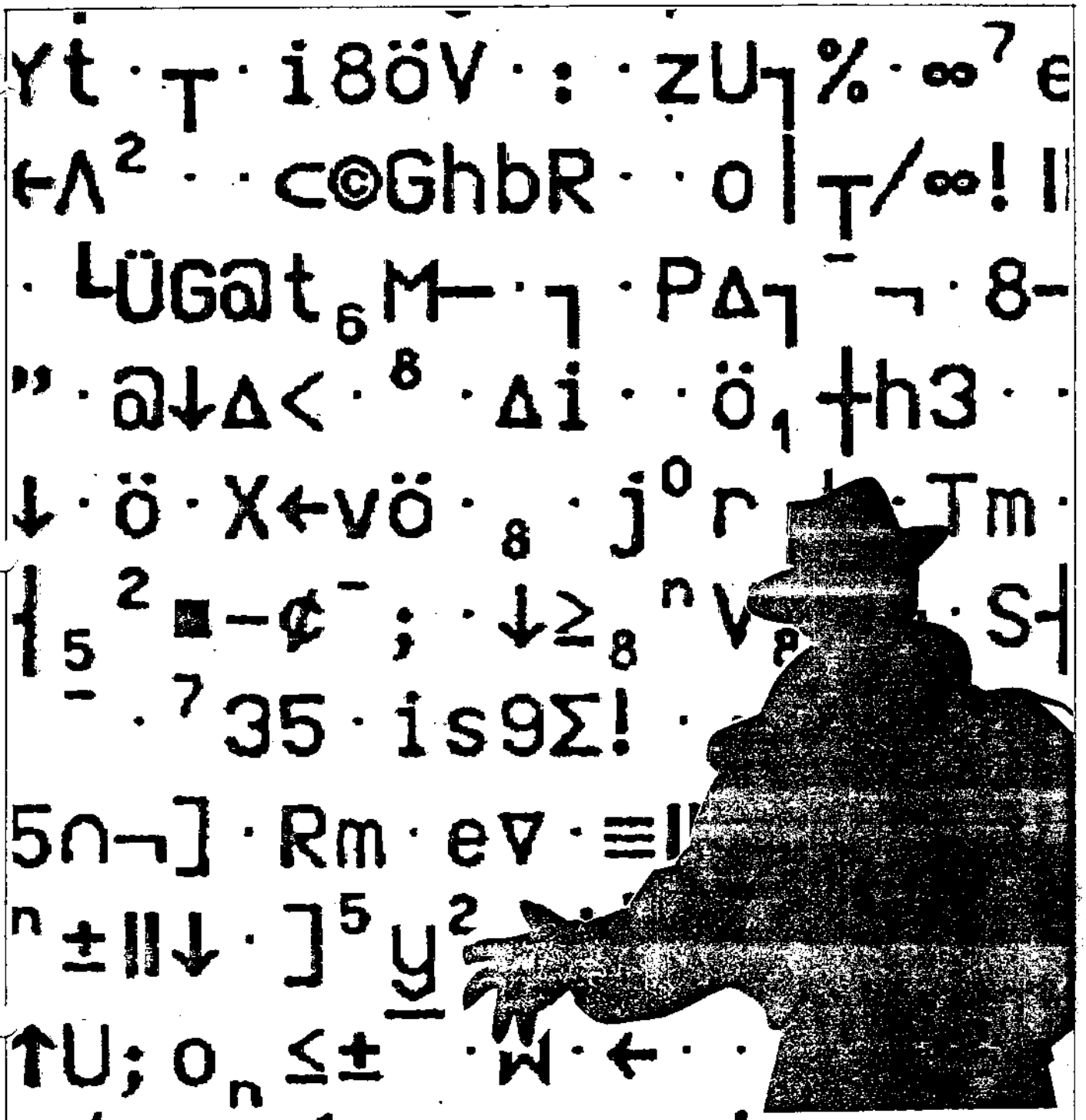

Johann Bizer
Volker Hammer
Ulrich Pordesch
Alexander Roßnagel

DAS NEUE BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

Planung - Kritik - Vorschläge

Gutachten
Im Auftrag der Fraktion

DIE GRÜNEN
IM BUNDESTAG

Zitiervorschlag:
Bizer, J. / Hammer, V. / Pordesch, U. / Roßnagel, A.: Das neue Bundesamt für Sicherheit in der Informationstechnik. Planungen – Kritik – Vorschläge. Gutachten im Auftrag der Fraktion DIE GRÜNEN im Bundestag, provet-Projektbericht 4, Darmstadt, Februar 1990.

Die Papierversion des Dokuments ist verfügbar über die Universitäts- und Landesbibliothek Darmstadt (ULB): https://hds.hebis.de/ulbda/Record/HEB029866367
Die elektronische Fassung wird auf der Webseite der Projektgruppe verfassungsverträgliche Technikgestaltung e.V. - provet - bereitgestellt: www.provet.org.

Hinweis zum OCR-Text:
Der PB04s ist die gescannte Fassung des entsprechenden Projektberichts von provet. Durch eine OCR-Software wurden das Scan-Ergebnis automatisch in Text umgewandelt und zusätzlich zu den Bildern in dieser Datei hinterlegt. Bitte beachten Sie, dass wir die Qualität der OCR-Umwandlung nicht überprüft haben.

Stand der elektronischen Fassung: Version 1.1 vom 15.11.2024

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) Sicherungsmöglichkeiten. 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 außschließlich 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

der Funktionssicherheit von IuK-Systemen sind auch unter der hier vertretenen erweiterten Zielsetzung von großer Bedeutung sind, da unabhängig von Untersuchungen der Abhängigkeit und von Schadenspotentialen IuK-Systeme durch unabhängige Instanzen bewertet werden müssen. Hersteller und Anwender können dieser Aufgabe aufgrund ihrer häufig auf kurzfristige Rentabilität ausgerichteten Interessen nicht gerecht werden.

Auf der Suche nach problemadäquaten Regelungen, Verfahren, und Institutionen darf das alleinige Heil nicht in der Errichtung eines neuen Bundesamtes gesehen werden. Dadurch entsteht die Gefahr, daß - wie im Bereich der Atomenergie - Sicherheit zu einem Problem bürokratischer Verantwortlichkeit wird. Je nach Anwendungsbereich und Problemstellung sollten vielmehr unterschiedliche organisatorische Zuordnungen und Regelungen getroffen werden. Die konkrete Ausgestaltung und Anwendung der IuK-Systeme sollte -soweit möglich - in sozialer Selbstverwaltung zwischen Anwendern und Betroffenen erfolgen, wobei der Gesetzgeber für adäquate Verfahren und eine ausgeglichene Beteiligung zu sorgen hätte.
Das Bundesamt für die Sicherheit in der Informationstechnik sollte übergreifende Aufgaben wahrnehmen. Zur Erhaltung der Lernfähigkeit der Gesellschaft hätte es beispielsweise Studien zu Alternativentwicklungen zu vergeben und alternative Gestaltungsvorschläge zu laufenden Planungen zu unterbreiten. Um öffentlichkeit zu gewährleisten und kritische Diskurse zu ermöglichen, sollte das Bundesamt jährliche Berichte zur Lage der Verletzlichkeit herauszugeben. Um das Bundesamt aber überhaupt erst in die Lage zu versetzen die Verletzlichkeit zu beurteilen, swäre vorzusehen, daß jeder Anbieter und Anwender von IuK-Systemen eines noch zu bestimmenden Zuschnitts anzeigt, daß er ein IuK-System anbietet oder ein solches System in einer bestimmten Anwendungsumgebung einsetzt. Eine Hauptaufgabe des Bundesamtes müßte darin bestehen, alle Entscheidungsträger zu unterstützen, das Kriterium der Verletzlichkeit systematisch in ihre Entscheidungen einzubeziehen. Dazu müssen Kriteriensysteme spezifiziert werden, die über die IT-Sicherheitskriterien hinausgehen und vor allem die Abhängigkeit und gesellschaftliche Schadenspotentiale einbeziehen. Das Bundesamt sollte das Recht und für bestimmte näher zu bezeichnende Bereiche auch die Pflicht haben, sich an Planungs- und Entscheidungsverfahren zu beteiligen. Zur Steuerung der Technikentwicklung sind für Systeme mit besonders hohem Schadenspotential sind sogar formelle Zulassungs- und Genehmigungsverfahren vorzusehen.

Zusammenfassend ist festzustellen, daß die Bundesregierung zwar Sicherheitsprobleme erkennt, Problemsicht und vorgeschlagenen Maßnahmen aber viel zu kurz greifen. Im Interesse der Sicherheit der Bürger und des Schutzes der Grundrechte ist es dringend geboten das technokratische Sicherheitsdenken durch eine am Problem der gesellschaftlichen Verletzlichkeit orientierte Sicherheitsphilosophie zu ersetzen!

Johann Bizer, Volker Hammer
Ulrich Pordesch, Alexander Roßnagel

DAS NEUE BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

Planungen - Kritik - Vorschläge

provet

Projektgruppe verfassungsverträgliche Technikgestaltung
Darmstadt

provet

Projektgruppe verfassungsverträgliche Technikgestaltung

Prof. Dr. jur. Alexander Roßnagel
Dipl. Inform. Volker Hammer
Dipl. Inform. Ulrich Pordesch
Dr. jur. Peter Wedde

c/o Fachhochschule Darmstadt
Schöfferstraße 3
6100 Darmstadt
Tel. 06151 / 31 66 76

Johann Bizer, Volker Hammer
Ulrich Pordesch, Alexander Roßnagel

DAS NEUE BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

Planungen - Kritik - Vorschläge

Gutachten

Im Auftrag der Fraktion
DIE GRÜNEN im Bundestag

Darmstadt, Februar 1990

INHALT

I. PLANUNGEN UND HINTERGRÜNDE

1. Ein neues Bundesamt - Die aktuellen Planungen der Bundesregierung 1

2. Von der Zentralstelle für das Chiffrierwesen zum Bundesamt für Sicherheit in der Informationstechnik - geschichtliche Hintergründe und internationale Parallelen 3

3. Die Zielsetzungen der Bundesregierung 5

4. Die rechtliche Zulässigkeit des Bundesamt für Sicherheit in der Informationstechnik 6

II. KRITIK UND BEFÜRCHTUNGEN

1. Kritik der Zielsetzungen 10

2. Kritik des Handlungskonzepts 13

3. Kritik der Organisationsformen 15

4. Befürchtungen für die Bürgersicherheit 17

III. VORSCHLÄGE UND FORDERUNGEN

1. Verletzlichkeit - neue Aufgaben in der 'Informationsgesellschaft' 21

Verringerung der Verletzlichkeit der Gesellschaft 21, Gewährleistung der Daseinsvorsorge 23, Verbesserung der Bürgersicherheit 25, Verbrauchersicherheit 26, Verbesserung der Funktionsicherheit technischer Systeme 28

2. Bedingungen der Aufgabenerfüllung 29

3. Handlungsbedarf und Handlungsmöglichkeiten 30

Bestehende Zulassungsverfahren 31, IuK-spezifische Zulassungsverfahren 37, Haftung 39, Normung 41, Voraussetzungen der Grundrechtssicherung durch Verschlüsselungsverfahren 42

IV. DAS BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

1. Aufgaben und Befugnisse 45

Befugnisse zur Erhaltung der Lernfähigkeit der Gesellschaft 45, Befugnisse zur Gewährleistung von Öffentlichkeit 46, Befugnisse zur Unterstützung Dritter 48, Befugnisse zur Kontrolle und Steuerung der Technikentwicklung 49, Befugnisse in Public-Key-Systemen 51

2. Organisation 52

LITERATUR 55

ABKÜRZUNGSVERZEICHNIS 59

VORBEMERKUNG

Die Projektgruppe verfassungsverträgliche Technikgestaltung - Provet - in Darmstadt wurde von der Fraktion 'DIE GRÜNEN IM BUNDESTAG' gebeten, die Planungen der Bundesregierung zur Errichtung eines Bundesamts für Sicherheit in der Informationstechnik kritisch zu würdigen. Die Bewertung sollte mit dem von Provet entwickelten Kritrium der Verletzlichkeit durchgeführt werden.

Schwierigkeiten bereitete diese Prüfung vor allem deshalb, weil die Quellenlage sehr dürftig ist. Uns liegen als Materialien zu den Planungen der Bundesregierung nur drei verschiedene Fassungen eines "Rahmenkonzeptes zur Gewährleistung der Sicherheit bei Anwendung der Informationstechnik (IT)" sowie der erste Gesetzentwurf zur Errichtung des Bundesamtes vor:

Rahmenkonzept vom 30.12.1988, (Maschinenschrift).

Rahmenkonzept ohne Datum, veröffentlicht in: Datenschutz und Datensicherheit 1989, S. 291 ff.

Rahmenkonzept vom 27.9.1989, (Maschinenschrift), das vom Bundesinnenministerium als Kabinettsvorlage vom 25.10.1989 benutzt wurde.

Entwurf eines Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik, Anlage zur Kabinettvorlage des Bundesinnenministeriums vom 12.2.90.

Der Gesetzentwurf erreichte uns erst kurz vor Abschluß des Berichts und konnte deshalb nicht mehr in allen Details berücksichtigt werden.

Ansonsten waren wir auf die in der Literaturliste genannten Stellungnahmen, Presseerklärungen und Zeitungsberichte angewiesen.

Die Ausführungen zu den Planungen der Bundesregierung sind daher unter diesem Vorbehalt zu lesen und aufgrund ihrer ständigen Weiterentwicklung selbstverständlich nur auf den Zeitpunkt der Quellen zu beziehen. Dennoch erschienen sie uns ausreichend, um an ihrem Beispiel vor absehbaren Fehlentwicklungen zu warnen und konstruktive Vorschläge zu entwickeln.

Wir beschränken uns in dieser Untersuchung auf das Problem der Verletzlichkeit der Gesellschaft - wohl wissend, daß die künftige Nutzung der IuK-Technik noch viele andere Probleme hervorbringen wird. Diese bewußte, dem Auftrag entsprechende Beschränkung bitten wir bei einer kritischen Würdigung unserer Überlegungen zu beachten.

DAS NEUE BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

Planungen - Kritik- Vorschläge

I. PLANUNGEN UND HINTERGRÜNDE

1. EIN NEUES BUNDESAMT - DIE AKTUELLEN PLANUNGEN DER BUNDESREGIERUNG

Die Bundesregierung hat in der Kabinettsitzung vom 23. November 1989 ein vom Bundesinnenminister entworfenes "Rahmenkonzept zur Gewährleistung der Sicherheit bei der Anwendung der Informationstechnik (IT) - IT-Sicherheitsrahmenkonzept" verabschiedet. Dieses enthält einen "Handlungsrahmen für diejenigen Stellen des Bundes, die für Grundsatzangelegenheiten im Zusammenhang mit der IT-Sicherheit zuständig sind".[1] Im inzwischen vorgelegten Gesetzentwurf, der mit dem 1. Januar 1991 in Kraft treten soll, heißt es:

"Bundesamt für Sicherheit in der Informationstechnik

Der Bund errichtet das Bundesamt für Sicherheit in der Informationstechnik als Bundesoberbehörde. Es untersteht dem Bundesminister des Innern."[2]

Die Aufgaben des zukünftigen Bundesamts für Sicherheit in der Informationstechnik werden im Gesetzentwurf zur Errichtung des Bundesamtes für Sicherheit in der Informationstechnik wie folgt beschrieben:

"Das Bundesamt hat zur Förderung der Sicherheit in der Informationstechnik folgende Aufgaben:

1. Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik, soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist,

2. Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten,

3. Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und Erteilung von Sicherheitszertifikaten,

4. Zulassung von informationstechnischen Systemen oder Komponenten, die im Bereich des Bundes oder bei Unternehmen im Rahmen von Aufträgen des Bundes für die Verarbeitung oder Übertragung amtlich geheimgehaltener Informationen (Verschlußsachen) eingesetzt werden sollen, sowie die Herstellung der Schlüsseldaten, die für den Betrieb zugelassener Verschlüsselungsgeräte benötigt werden,

---

[1] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 2.1

[2] § 1 BSIG-E.

5. Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen; soweit der Bundesbeauftragte für den Datenschutz unterstützt wird, geschieht dies im Rahmen der Unabhängigkeit, die ihm bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz zusteht,

6. Unterstützung der zuständigen Behörden des Bundes bei der Verhütung und Verfolgung von Straftaten sowie bei der Beobachtung der in § 3 Abs. 1 des Gesetzes über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes genannten Bestrebungen und Tätigkeiten, soweit dies erforderlich ist, um strafbare Handlungen, Bestrebungen oder Tätigkeiten, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen, zu verhindern oder zu erforschen,

7. allgemeine Beratung der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik."[3]

§ 4 des Gesetzentwurfs regelt die Erteilung eines vom Bundesamt zu vergebenden Sicherheitszertifikats.

Der Anhang 3 des IT-Sicherheitsrahmenkonzept nennt die Aufgaben, die die bisherige Zentralstelle für Sicherheit in der Informationstechnik (ZSI) bis zum Inkrafttreten des Errichtungsgesetzes - also bis zum 1.1.1991 - wahrnehmen soll.[4] Die dort genannten Aufgaben sind jedoch so langfristiger Natur, daß auch das neue Bundesamt mit ihnen noch konfrontiert sein wird. Da es zugleich als einzige Institutionalisierung das neue Bundesamt für Sicherheit in der Informationstechnik vorsieht, darf wohl davon ausgegangen werden, daß die beschriebenen Aufgaben diesem übertragen werden sollen. Konkretisierende oder ergänzende Aufgaben sind nach dem Rahmenkonzept deshalb außerdem:

- die Mitwirkung bei Normungsarbeiten, soweit diese die Sicherheit bei Anwendung der Informationstechnik berühren,[5]

- die Begleitung staatlich geförderter Forschungs- und Entwicklungsvorhaben, soweit sie Aspekte der Sicherheit bei der Anwendung der Informationstechnik zum Gegenstand haben.[6]

- Prüfung der Produkte/Systeme der Informationstechnik, die im Bereich der Bundesbehörden oder bei Unternehmen für Verschlußsachenaufträge des Bundes eingesetzt werden sollen, auf die Einhaltung von Sicherheitsanforderungen, soweit die zuständige Bundesbehörde darum ersucht[7].

- die Mitwirkung bei der Festlegung der Rahmenbedingungen für Exportbeschränkungen bei Produkten/Systemen der Informationstechnik, insbesondere bei Chiffrierverfahren im Zusammenhang mit der Begutachtung beim Export solcher Güter durch das Bundesamt für Wirtschaft[8].

- die Entwicklung von Empfehlungen, deren Berücksichtigung in der Verantwortung des jeweiligen Anwenders verbleibt[9].

---

[3] § 3 BSIG-E.

[4] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 9.5.1. In der in Datenschutz und Datensicherung 1989, S. 291 ff. veröffentlichten Fassung wurde die Aufgabenbeschreibung ohne Rücksicht auf das noch zu erlassende Errichtungsgesetz vorgenommen.

[5] Vgl. IT-Sicherheitsrahmenkonzept vom 27.9.1989, Anlage 3, f).

[6] Vgl. IT-Sicherheitsrahmenkonzept vom 27.9.1989, Anlage 3, g). In der Fassung DuD 1989, S. 291 wird der ZSI noch die Aufgabe der "Durchführung oder Vergabe spezieller Forschungs- und Entwicklungsarbeiten" zugedacht. Siehe hierzu auch IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 9.4.2.

[7] Vgl. IT-Sicherheitsrahmenkonzept vom 27.9.1989, Anlage 3, e).

[8] Nach der Ausfuhrliste zur Außenwirtschaftsverordnung unterliegen Kryptosysteme grundsätzlich Ausfuhrbeschränkungen, d.h. sie bedürfen einer Genehmigung des Außenwirtschaftsamtes. Für Verschlußsachen zugelassene Kryptosysteme sind darüber hinaus zumindest in Teilen selbst als Verschlußsache eingestuft - vgl. IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 7.2.

[9] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 5.5.

- der Einsatz von Beratungs- und Prüfgruppen, die die IT-Anwender beraten (einschließlich der Erstellung von Risikoanalysen und Sicherheitskonzepten) und vorhandene Sicherheitseinrichtungen im Verdachtsfall sowie nach Bedarf stichprobenartig auf sichere Funktion bzw. mögliche Manipulation überprüfen[10].

- die Prüfung der nach Sicherheitskriterien erstellten Produkte. Die Kriterien richten sich nach dem öffentlichen Sicherheitsinteresse, zu dem insbesondere zählen
  - der Datenschutz nach dem BDSG,
  - Wirtschaft und Wissenschaft,
  - der staatliche Geheimschutz und
  - die Verteidigung[11].

- das Veranlassen einer Prüfung durch die zuständige NATO-Behörde für die Aufnahme in die "Nato-Recommended Products-List (NRPL)" auf Antrag des Herstellers.[12]

Zur Erfüllung all dieser Aufgaben soll auch das neue Bundesamt für Sicherheit in der Informationstechnik - ebenso wie bisher die ZSI[13] - "unmittelbar mit den zuständigen nationalen, ausländischen, über- und zwischenstaatlichen Stellen" zusammenarbeiten.[14]

Um nun diese Planungen einer kritischen Überprüfung unterziehen zu können, sind ihre Geschichte und ihre Zielsetzungen mit in die Untersuchung einzubeziehen. Ohne Berücksichtigung der geschichtlichen Entwicklung bleiben viele Risiken und Befürchtungen unverständlich und ohne die Analyse der verfolgten Ziele bleibt eine Kritik des Konzepts auf die Wirksamkeit einzelner Maßnahmen der Bundesregierung beschränkt. Daher werden im folgenden anhand verfügbarer Quellen kurz die Vorgeschichte des Rahmenkonzeptes und der Errichtungen eines Bundesamts für Sicherheit in der Informationstechnik skizziert und im Anschluß daran die mit diesen Maßnahmen verfolgten Zielsetzungen der Bundesregierung beschrieben.

2. Von der Zentralstelle für das Chiffrierwesen zum Bundesamt für Sicherheit in der Informationstechnik - geschichtliche Hintergründe und internationale Parallelen

Der erste Vorläufer des Bundesamtes für Sicherheit in der Informationstechnik (BSI) war die Zentralstelle für das Chiffrierwesen (ZfCH)[15]. Über diese Behörde des Sicherheitsbereiches ist nur sehr wenig bekannt. Sie war dem Bundesnachrichtendienst zugeordnet und unterstand dem für die Koordination der Geheimdienste zuständigen Staatssekretär im Bundeskanzleramt. Die Zentrale liegt in Bonn Bad Godesberg. Offiziell hatte sie vor allem die Aufgabe, sich mit Fragen der Chiffrierung zu befassen und Chiffriersysteme für den amtlichen Gebrauch (VS-Bereich) zuzulassen.[16] So wurde die ZfCH beispielsweise für die Sicherung der Kommunikation des auswärtigen Amtes mit Botschaften im Ausland hinzugezogen.[17] Ferner sollte die ZfCH die von Behörden eingesetzte Computerhardware auf die Einhaltung der Standards für elektromagnetische Abstrahlsicherheit überprüfen.

In den USA sind die Bereiche Entwicklung von Kryptosystemen für den Sicherheitsbereich und Dechiffrierung von abgehörten Nachrichten bei einer Behörde, der "National Security Agency" (NSA), konzentriert, die

---

[10] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 5.6. Prüfungen sollen vor allem bei abstrahlgeschützter Hardware sowie bei Software mit Sicherheitsfunktionen durchgeführt werden.

[11] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 6.2; 2.2.

[12] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 6.2.

[13] Vgl. IT-Sicherheitsrahmenkonzept vom 27.9.1989, Anlage 3, 4.

[14] Angesichts des aufgezählten Aufgabenkataloges zählen zu diesen Stellen offensichtlich neben den inländischen Diensten auch ausländische "Schwesterbehörden". Vgl. auch O. Leiberich sowie H. Neusel, Wissenschafts-Pressekonferenz, 6.2.1990.

[15] Zur Geschichte siehe auch das Hintergrundpapier von Hans Neusel auf der Wissenschaftspressekonferenz vom 6.2.1990, Bonn.

[16] H.Kersten, 6.RDV-Forum der DAFTA, 13.Tagung der DAFTA am 16. und 17.11.89.

[17] FR 29.11.89.

dem Department of Defense (DoD) untersteht.[18] Ursache dieser organisatorischen Zusammenfassung entgegengesetzter Aufgaben soll der internationale Mangel an Fachkräften der Kryptologie sein. Dies gilt offensichtlich auch für die ZfCH, die "die Aufgabenbereiche 'Entzifferung' und 'Entwicklung von Verschlüsselungsgeräten' (Code-breaker und Code-maker unter einem Dach)" vereinigt[19], auch wenn die ZfCH selbst nicht als Geheimdienst beim Abhören tätig ist und wohl nur technische und fachliche Unterstützung liefert.

Wie, warum, wann und in welcher Weise Aspekte der Computersicherheit durch die ZfCH und andere Bundesbehörden aufgegriffen und weiter verfolgt wurden, läßt sich aus den uns verfügbaren Quellen nur äußerst lückenhaft rekonstruieren. Nach Angaben des Staatssekretärs im Bundesinnenministerium Neusel war Fach- und Sachkunde zur Computersicherheit bisher nur beim Bundeskriminalamt zu finden.[20] Dort beschäftigt sich eine spezielle Abteilung mit Fragen der Computerkriminalität. Deren Schwergewicht liegt aber eher auf der Verbrechensbekämpfung und Gefahrenabwehr und nicht auf der technischen Sicherheit von Informations- und Kommunikationssystemen. Auch die klassische Aufgabenstellung der ZfCH deckte viele wichtige Aspekte der Computersicherheit wie beispielsweise die Zugangskontrolle in vernetzten Systemen oder die Softwaremanipulationssicherheit nicht ab.

Ausgangspunkt für ein wachsendes Bewußtsein in der Bundesverwaltung und -politik für die Manipulations, Spionage- und Sabotagerisiken der elektronischen Datenverarbeitung und Kommunikation waren offenbar einige spektakuläre Fälle von Computerkriminalität und Hacking. Sie führten zu der Erkenntnis, daß über den Geheimschutzbereich hinaus Maßnahmen getroffen werden müssen um der wachsenden Verwundbarkeit der Datenverarbeitung und Kommunikationstechnik zu begegnen.[21]

Zu diesem Zweck wurde ein "Interministerieller Ausschuß für die Sicherheit in der Informationstechnik" (ISIT) gegründet. Er hat die Aufgabe, unter Beteiligung der zuständigen Stellen, insbesondere der Wirtschaft, Strategien zu beraten, damit Daten und IT-Systeme in allen Anwendungsbereichen im gebotenen Maße geschützt werden können.[22] 1987 wurde außerdem der Aufgabenbereich der ZfCH um die Computer-Sicherheit erweitert.[23] Im Rahmen dieses Tätigkeitsfeldes leistete die ZfCH technisch-wissenschaftliche Grundlagenarbeiten, mit denen die Sicherheit von Produkten der IuK-Technik geprüft werden kann.

In ihrer Arbeit ließen sich ISIT und ZfCH von der Entwicklung in den USA leiten. Dort wurden bereits vor einigen Jahren Sicherheitskriterien für informationstechnische Systeme entwickelt (Orange Book)[24], die es ermöglichen sollen, Sicherheitserfordernisse zu definieren und IuK-Systeme entsprechend ihren Sicherheitseigenschaften zu klassifizieren. Mit Vorüberlegungen zur Computersicherheit muß die ZfCH 1986/87 begonnen haben. Damals wurde als erster Schritt auf dem Wege zu nationalen Kriterien eine sachliche Kritik an den US-amerikanischen Kriterien formuliert und es wurden Überlegungen für eine verbesserte Prüf- und Bewertungssystematik angestellt. 1987/88 wurde dann ein eigener nationaler Kriterienkatalog im Auftrag der ZfCH von der Industrie Anlagen Betriebsgesellschaft (IABG) erstellt und zusammen mit namhaften DV-Herstellern, Hochschul- und Forschungsinstituten und Verbänden in einem Arbeitskreis "Nationale Kriterien" diskutiert. September 1988 wurde der vom Arbeitskreis gebilligte Katalog dem ISIT zugeleitet und Anfang 1989 verabschiedet. Das betreffende Dokument "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (kurz "IT-Sicherheitskriterien"), ein Pendant zum amerikanischen Orange Book ist am 1. Juni 1989 im Bundesanzeiger veröffentlicht worden. Diese IT-Sicherheitskriterien definieren auf der Basis der Grundbedrohungen Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit von Informationen unter-

---

[18] Zur US-amerikanischen Situation ausführlich: Bernhard/Rufmann, ZSI: Die Bundesregierung will den Bock zum Gärtner machen, CW 22.12.89, S. 6 f. Die NSA soll ausgestattet mit einem 100000 Mann Heer und einem 15 Milliarden Dollar Jahresetat ein weltumspannendes Netz der Telekommunikationsüberwachung unterhalten, das der US-Regierung 95% aller nachrichtendienstlichen Erkenntnisse liefert; aus: NSA&Co - Aufklärungsdienste der USA in der Bundesrepublik, MEDIATUS, Sondernummer Juni 1989.

[19] Vgl. H. Neusel, Wissenschafts-Pressekonferenz, 6.2.1990, S. 1.

[20] Protokoll der Sitzung des Haushaltsausschusses vom 27.9.89. erstellt 19.10.89.

[21] Nach Worten des Innenstaatssekretärs Neusel zieht die Bundesregierung mit der ZSI Konsequenzen aus dem Spionagefall von 1988, bei dem Hacker im Auftrage des KGB in Computernetze in der ganzen Welt eindrangen - FR 24.11.89.

[22] IT-Sicherheitsrahmenkonzept vom 27.9.1989, S. 3.

[23] Vgl. H. Neusel, Wissenschafts-Pressekonferenz, 6.2.1990, S.2.

[24] Department of Defense (USA), Trusted Computer System Evaluation Criteria, DoD 5200.28 STD, Dezember 1985; vgl. dazu z.B. Cerny, Vertrauenswürdige DV-Systeme nach dem Orange Book, DuD 1/88, S. 11-13.

bedrohungen Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit von Informationen unterschiedliche Sicherheitsklassen für informationstechnische Systeme. Sie sollen "grundlegende Richtlinie für Produktprüfungen" sein, die Behörden und Wirtschaft zur Verfügung stehen sollen.[25]

Entsprechend der Aufgabenerweiterung um den Bereich Computersicherheit wurde die ZfCH 1989 in "Zentralstelle für Sicherheit in der Informationstechnik" (ZSI) umbenannt. Zur Zeit werden von der ZSI ca. 10 IuK-Systeme evaluiert, ein IT-Evaluationshandbuch erstellt und Vorarbeiten für ein IT-Sicherheitshandbuch geleistet.[26] Nach dem nun von der Bundesregierung gebilligten "Rahmenkonzept zur Gewährleistung der Sicherheit bei Anwendung der Informationstechnik (IT)" soll die ZSI um 300 Planstellen erweitert und ab 1.1.1991 in eine obere Bundesbehörde im Geschäftsbereich des Bundesminister des Innern umgewandelt werden.

3. Die Zielsetzungen der Bundesregierung

Diese Planungen sind außer dem generellen Wunsch nach mehr Sicherheit in der Informationstechnik, der sich durch das gesamte Rahmenkonzept hindurchzieht, durch eine Reihe spezifischer Zielsetzungen geleitet. Diese lassen sich aus dem Rahmenkonzept selbst und verschiedenen Äußerungen der Bundesregierung hierzu rekonstruieren:

- internationale Wettbewerbsfähigkeit

  Einen wesentlichen Hintergrund des Rahmenkonzeptes bildet die Sorge um die Exportfähigkeit der bundesdeutschen Industrie. Ein Ziel ist daher, "die internationale Wettbewerbsfähigkeit deutscher/europäischer IT-Hersteller unter dem Aspekt eines hohen Sicherheitsstandards" zu stärken. Ihre Produkte müßten im internationalen Wettbewerb in dieser Hinsicht ein hohes Qualitätsniveau erreichen und halten[27]. Befürchtet wird, daß bundesrepublikanische Hersteller ohne Zertifizierung von IT-Produkten auf internationalen, insbesondere US-amerikanischen Märkten Marktanteile verlieren könnten oder dort, wo Sicherheitszertifikate vorgeschrieben werden, nicht mehr liefern dürften.[28] Um die Durchsetzbarkeit der eigenen Zertifikate zu erhöhen, seien EG-weite bzw. internationale Kriterien zur Bewertung, Prüfung und Zertifizierung von IT-Systemen und Komponenten anzustreben[29]. Thematisiert wird auch die Abstimmung und wechselseitige Anerkennung der Sicherheitskriterien der Bundesrepublik mit denen der EG bzw. der NATO[30].

- Betriebssicherheit

  Durch Anforderungen an informationstechnische Systeme sowie deren Überprüfung und Zertifizierung soll generell die Betriebssicherheit von IT-Produkten erhöht werden. IT-Anwender sollen in die Lage versetzt werden, system- und anwendungsbezogene Risikoanalysen zu erstellen und angemessene Sicherheitskonzepte zu entwickeln und zu realisieren. Umgekehrt soll ein Markt für sichere IT-Systeme geschaffen werden, auf dem IT-Systeme und -komponenten mit einem ausreichenden Sicherheitsstandard zur Verfügung stehen.[31]

---

[25] Vgl. hierzu auch van Essen (ZfCH), CW 28.4.89, S. 41.

[26] Kersten, 13. DAFTA, 1989.

[27] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt.1.2, 1. Abs. sowie Pkt. 3.1. dritter Spiegelstrich.

[28] IT-Sicherheitsrahmenkonzept vom 27.9.1989. Dazu die Aussage von Innenstaatssekretär Neusel in der Sitzung des Haushaltsausschusses vom 27.9.89, Protokoll.

[29] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt.2.1, 2. Abs.; 9.8.1; 9.8.2; 9.8.3.

[30] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 6.2; 8; 9.1.

[31] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 3.1 und Weck, Gerhard, Datensicherung - Konzepte und Bewertung, DuD 8/1989, S. 391 f.

- Innere Sicherheit

Das Rahmenkonzept konzentriert sich in der Problembeschreibung wesentlich auf Aspekte der Inneren Sicherheit. Mehrfach wird Bezug genommen auf die gestiegene Computerkriminalität als auch auf Sabotage extremistisch/ terroristischer Gruppierungen, sowie organisierte Kriminalität.[32].

- militärische Sicherheit

Verwiesen wird hier vor allem auf die Arbeit gegnerischer Nachrichtendienste[33] wobei der feindlichen "Fernmeldeaufklärung" ein besonderer Stellenwert zugewiesen wird.[34] In der Anlage 2 werden die Möglichkeiten des "Abhörens" von Richtfunkverbindungen sowie elektrischer oder elektromagnetischer "Abstrahlung" skizziert. Es wird darauf verwiesen, daß trotz zunehmender Kryptierung Rechenzentren und DV-Anlagen sowie DV-Endeinrichtungen zunehmend gefährdet sind, da dort die Informationen im Klartext vorliegen. Herausgehoben wird an mehreren Stellen die Notwendigkeit einer Übernahme oder Anerkennung der IT-Sicherheitskriterien durch die NATO.[35] Dies gilt vor allem für die gegenseitige Anerkennung der Sicherheitsstandards durch die NATO Behörde SECAN und deren Prüfergebnisse.[36] Den Hintergrund bilden hier wohl schärfere Dokumentationspflichten der Prüfabläufe innerhalb der NATO als sie das Sicherheitskonzept der Bundesregierung vorsehen will.[37]

4. Die rechtliche Zulässigkeit des Bundesamt für Sicherheit in der Informationstechnik

Für die Beurteilung der rechtlichen Zulässigkeit eines Bundesamt für Sicherheit in der Informationstechnik ist zu berücksichtigen, daß das Rahmenkonzept dessen zukünftige Aufgaben und Befugnisse nicht ausdrücklich festlegt, sondern sich auf den Zeitraum bis zum Erlaß eines Errichtungsgesetzes beschränkt. Dementsprechend sind die Aufgaben und Befugnisse im Rahmenkonzept enger gefaßt als sie wohl durch ein zukünftiges Errichtungsgesetz geregelt werden sollen.

Das Bundesamt für Sicherheit in der Informationstechnik soll als selbständige Bundesoberbehörde nach Art. 87 Abs. 3 Satz 1 GG errichtet werden. Als Ausnahme von der Regel der Verwaltungskompetenz der Länder bestimmt Art. 87 Abs. 3 Satz 1 GG:

> "Außerdem können für Angelegenheiten, für die dem Bunde die Gesetzgebung zusteht, selbständige Bundesoberbehörden und neue bundesunmittelbare Körperschaften und Anstalten des öffentlichen Rechts durch Bundesgesetz errichtet werden."

Voraussetzung für ein Errichtungsgesetz ist demnach, daß der Bund die Gesetzgebungskompetenz auf dem Gebiet und für die einzelnen Angelegenheiten hat, für das die neue Behörde eingerichtet werden soll.

Eine Gesetzgebungskompetenz für die Regelung der technischen Sicherheit enthält das Grundgesetz nicht. Gleichwohl lassen sich für die einzelnen Aufgaben Kompetenzzuweisungen ableiten.

Soweit das Bundesamt für Sicherheit in der Informationstechnik Produktprüfungen und Zertifizierungen vornehmen soll, nach denen die Hersteller ihre Produkte ausrichten, ist der Wirtschaftsbereich betroffen, für den der Bund nach Art. 74 Nr. 11 GG eine konkurrierende Gesetzgebungskompetenz hat.[38]

---

[32] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 4.3.

[33] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkte. 2.2.; 4.3.; 4.6.

[34] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 4.6. sowie Anlage 2.

[35] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 9.1.; 9.7.

[36] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 9.7.2. Dazu auch Rahmenkonzept 1988, Pkt. 7.6.2, das die Bedeutung der SECAN erstens mit deren Aufgabenerweiterung vom Fernmeldebereich auf den gesamten IT-Bereich begründet und zweitens auf den Wettbewerbsnachteil für europäische Anbieter verweist, der dadurch entsteht, daß SECAN seinen Sitz in den USA hat.

[37] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 9.7.3.

[38] Vgl. umfassend Maunz, in: Maunz/Dürig 1989, Art. 74, Rn. 130 (133).

Soweit das Bundesamt für Sicherheit in der Informationstechnik Vorgaben für den Bereich der militärischen Sicherheit leisten soll, hat der Bund eine ausschließliche Gesetzgebungskompetenz nach Art. 73 Nr. 1 GG.

Für den Bereich der Inneren Sicherheit fehlt dem Bund eine Gesetzgebungskompetenz, wenn man unter der Inneren Sicherheit die klassischen Polizeiaufgaben der Gefahrenabwehr, die Länderaufgabe sind, faßt. Sollte das Bundesamt für Sicherheit in der Informationstechnik klassische Aufgaben der Gefahrenabwehr übernehmen, fehlt dem Bund die Gesetzgebungskompetenz. Dagegen hat der Bund für den Bereich der Strafverfolgung eine Kompetenz nach Art. 74 Nr. 1 GG. Keine Kompetenzkonflikte entstehen auch im Bereich der Inneren Sicherheit, wenn das Bundesamt für Sicherheit in der Informationstechnik nicht originäre Aufgaben der Gefahrenabwehr übernehmen, sondern über Vorgaben auf die Hersteller Standardisierungen bewirken soll, die die zuständigen Behörden der Inneren Sicherheit für eigene Zwecke zugrundelegen können.

Soweit die ZSI selbst Sicherheitskomponenten entwickelt oder entwickeln läßt, ist fraglich, ob es sich um eine Forschungsförderung handelt, für die dem Bund nach Art. 74 Nr. 13 GG eine konkurrierende Gesetzgebung zusteht, oder um Ressortforschung, für die der Bund, wenn überhaupt, lediglich eine Verwaltungskompetenz besitzt.[39] Fest steht jedenfalls, daß eine bloße Verwaltungskompetenz für die Einrichtung einer Bundesoberbehörde nicht ausreicht. Die Wahrnehmung der Gesetzgebungskompetenz nach Art. 74 Nr. 13 GG ("Förderung der wissenschaftlichen Forschung") könnte fraglich sein, weil das Rahmenkonzept selbst nicht von Aufgaben der wissenschaftlichen Forschung spricht, sondern nur von der Entwicklung. Die Abgrenzung ist im einzelnen schwierig. Maunz beispielsweise sieht das Gegenstück zur wissenschaftlichen Forschung in der technischen Vorbereitung insdustrieller Fertigung. Dazwischen sieht er die "sogen. technologische Entwicklung", die häufig nur schwer von der wissenschaftlichen Forschung abzugrenzen sei.[40] Daneben bleibt aber auch die Möglichkeit, die Entwicklung der Sicherheitskomponenten der Gesetzgebungskompetenz nach Art. 74 Nr. 11 (Wirtschaft) zuzuordnen, denn schließlich soll die neue Bundesoberbehörde Sicherheitsstandards gerade auch für den wirtschaftlichen Verkehr der IT-Techniken entwickeln. Einigkeit besteht insoweit nämlich über die Weite dieser Kompetenzbestimmung, die alle Normen, die das wirtschaftliche Leben und die wirtschaftliche Betätigung regeln, umfaßt.[41]

Darüberhinaus bedarf die Errichtung einer Bundesoberbehörde nicht, wie beispielsweise die konkurrierende Gesetzgebung nach Art. 72 Abs. 2 GG, einer zusätzlichen Rechtfertigung durch ein besonderes Bedürfnis nach bundesgesetzlicher Regelung. Das BVerfG hat eindeutig judiziert, daß Art. 87 Abs. 3 Satz 1 GG eine ausschließliche Gesetzgebungskompetenz zur Errichtung von Bundesoberbehörden enthält, deren Ausübung nicht an weitere Voraussetzungen wie Art. 72 Abs. 2 GG gebunden sind.[42]

Die Organisation einer Verwaltungseinheit als selbständige Bundesoberbehörde bedeutet nach der Rechtsprechung des BVerfG außerdem, daß sie

> "nur für Aufgaben errichtet werden kann, die der Sache nach für das ganze Bundesgebiet von einer Oberbehörde ohne Mittel- und Unterbau und ohne Inanspruchnahme von Verwaltungsbehörden der Länder - außer für reine Amtshilfe - wahrgenommen werden können".[43]

Der Errichtung der Bundesoberbehörde und damit der Verwaltungsinitiative des Bundes ist insofern eine weitere Grenze gezogen, als sich auch bei Vorliegen einer Gesetzgebundskompetenz nur bestimmte Aufgaben zur zentralen Erledigung eignen.

Soweit die neue Behörde mit Aufgaben betraut ist, die die Verwaltungszuständigkeit der Länder "erheblich verdrängt", ist sie nicht unzulässig, sondern ihre Errichtung bedarf der Zustimmung des Bundesrates.[44] Für

---

[39] Maunz, in: Maunz/Dürig 1989, Art. 74, Rn. 177 ff. Kritisch zur Anerkennung der Ressortforschung als Verwaltungskompetenz, Bull, in Alternativkommentar zum Grundgesetz, vor Art. 83, Rn. 36, aber Anerkennung einer Verwaltungskompetenz des Bundes für Vorhaben der wissenschaftlichen Großforschung z.B. auf dem Gebiet der Datenverarbeitung, ders., in: Alternativ-Kommentar zum Grundgesetz, Art. 83, Rn. 13.

[40] Maunz, in: Maunz/Dürig, Art. 74, Rn. 178; Bothe, in: Alternativ-Kommentar zum Grundgesetz, Art. 74, Rn. 31.

[41] BVerfGE 8, 143 (148 f.) 55, 274 (308); 68, 310 (330), Maunz, in: Maunz/Dürig 1989, Art. 74, Rn. 130, Bothe, in: Alternativ-Kommentar zum Grundgesetz, Art. 74, Rn. 21.

[42] BVerfGE 14, 197 (213 f.).

[43] BVerfGE 14, 197 (211).

[44] BVerfGE 14, 197 (211).

den absehbaren Aufgabenbereich des Bundesamts für Sicherheit in der Informationstechnik ist nicht ersichtlich, inwieweit bestehende Verwaltungskompetenzen der Länder beschränkt werden sollten.

Als Ergebnis ist festzustellen, daß der Bund grundsätzlich für die Errichtung des Bundesamts für Sicherheit in der Informationstechnik als Bundesoberbehörde über eine ausreichende Kompetenz in Art. 87 Abs. 3 Satz 1 GG verfügt. Die Errichtung muß aber durch ein Bundesgesetz erfolgen.

Die verfassungsrechtliche Zulässigkeit des Bundesamts für Sicherheit in der Informationstechnik ist aber nicht nur nach den Voraussetzungen seiner Errichtung zu prüfen, sondern ebenso auch nach der Reichweite seiner Aufgaben.

Soweit das Bundesamt für Sicherheit in der Informationstechnik Sicherheitsstandards für den öffentlichen Bereich erstellen soll, ist dies verbindlich nur für die Bundesverwaltung möglich. Nach Art. 86 GG erläßt die Bundesregierung die allgemeinen Verwaltungsvorschriften für den Bereich der bundeseigenen Verwaltung. In diesen könnte auch die Verbindlichkeit der Standards geregelt werden. Falls derartige Verwaltungsvorschriften nicht erlassen würden, bleibt immer noch eine Regelung der Verbindlichkeit nach der jeweiligen Ressortkompetenz. So könnte beispielsweise der Postminister für seinen Geschäftsbereich die Standards vorschreiben.

Soweit die Länder Bundesgesetze als eigene Angelegenheiten (Art. 84 GG) oder im Auftrag des Bundes (Art. 85 GG) ausführen, kann die Bundesregierung allgemeine Verwaltungsvorschriften erlassen, bedarf hierfür aber der Zustimmung des Bundesrates (Art. 84 Abs. 2, 85 Abs. 2 GG).[45] Verbindlich könnten die Standards des Bundesamts für Sicherheit in der Informationstechnik in diesem Bereich somit nur mit Zustimmung des Bundesrates werden.

Verbindliche Vorgaben für die Verwendung von IuK-Techniken für die Landesverwaltungen, soweit sie Landesgesetze ausführen, kann der Bund nicht erlassen. Ihm fehlt insoweit sowohl die Verwaltungs- als auch die Gesetzgebungskompetenz. Allerdings steht es den Ländern frei, sich nach den Empfehlungen des Bundesamt für Sicherheit in der Informationstechnik zu richten.

Zu den Aufgaben der ZSI bis zum Erlaß des Errichtungsgesetzes zählt die Prüfung der Produkte/Systeme der Informationstechnik bei den Bundesbehörden oder den von ihr eingesetzen Unternehmen[46]. Das IT-Sicherheitskonzept beschränkt seinen Handlungsrahmen auf die Stellen des Bundes, die für Grundsatzangelegenheiten im Zusammenhang mit der IT-Sicherheit zuständig sind.[47] Es soll im übrigen der Konkretisierung der "Richtlinien für den Einsatz der IT in der Bundesverwaltung" dienen[48].

Nach dem Rahmenkonzept ist eine über den Bereich der Bundesbehörden hinausgehende Tätigkeit nur bei der Unterstützung der Sicherheitsbehörden der Länder zu erwarten[49]. Die hier anvisierte fachliche Unterstützung liegt allerdings im Rahmen einer durch Amtshilfevorschriften legitimierten Unterstützung der zuständigen Landesbehörden durch das Bundesamt für Sicherheit in der Informationstechnik.

---

[45] Bull, in: Alternativ-Kommentar zum Grundgesetz, Art. 84, Rn. 31; Art 85, Rn. 11.

[46] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Anlage 3, Pkt. 3 e).

[47] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 2.1; sowie Anlage 3 (Aufgaben der ZSI), Nr. 3 e).

[48] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 3.2.

[49] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Anlage 3, Pkt. 3 h).

Nach dem Rahmenkonzept sollen Produkte mit einem "Sicherheitszertifikat" versehen werden.[50] Die Prüfung erfolgt orientiert an "öffentlichen Sicherheitskriterien". Damit sind Vorgaben verbunden, für welche Bereiche welche Standards und damit welche Produkte anzuwenden sind. Die Kabinettsvorlage sieht weiter vor, daß die Hersteller von nicht im öffentlichen Auftrag entwickelten Produkten die Kosten der Prüfung zu tragen haben. Ebenso soll der Hersteller mit der Erteilung des Sicherheitszertifikats verpflichtet werden, die Sicherheitseigenschaft auch im Rahmen der Wartung und Reparatur gewährleisten (Sicherheitsservice).[51] Außerdem erwähnt das Rahmenkonzept den verstärkten Einsatz von "Beratungs- und Prüfgruppen". Zu ihren Aufgaben soll die Prüfung der vorhandenen Sicherheitseinrichtungen im Verdachtsfall sowie stichprobenartig im Bedarfsfall zählen.[52] Eine Begrenzung nur auf Bundesbehörden ist nicht ersichtlich. Eher ist zu vermuten, daß sie auch für die beauftragten privaten Unternehmen gelten sollen. Alle mit solchen Maßnahmen verbundenen Eingriffe in die Grundrechte aus Art. 12 Abs. 1, 2 Abs. 1 und 3 Abs. 1 GG der Hersteller machen es erforderlich, das Verfahren und die Kriterien für den Erlaß der Sicherheitszertifikate und Prüfbesuche durch Gesetz zu regeln.

---

[50] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 6.2.

[51] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 6.2.

[52] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 5.6.

II. KRITIK UND BEFÜRCHTUNGEN

Aus einer kritischen Betrachtung dieser Planungen und einer Betrachtung möglicher negativer Entwicklungen sollen konstruktive Vorschläge entwickelt werden, wie den künftigen Gefahren einer zunehmenden Nutzung informations- und kommunikationstechnischer Systeme begegnet werden kann. In diesem Abschnitt werden zuerst die Zielsetzungen und Planungen der Bundesregierung kritisch geprüft und im folgenden Abschnitt dann erörtert, wie den festgestellten Defiziten abgeholfen werden könnte.

Das Rahmenkonzept der Bundesregierung umreißt einige Probleme der Sicherheit der Informationstechnologie zutreffend und entwickelt in einigen Bereichen weiterführende Handlungsvorschläge. Dennoch werden die Zielsetzungen, Aufgabenbeschreibungen und Handlungsvorschläge weder der eigenen Problembeschreibung noch einem um die gesellschaftliche Dimension erweiterten Verständnis der Sicherheitsprobleme gerecht - selbst wenn akzeptiert wird, daß die Bundesregierung mit dem Rahmenkonzept und der Schaffung eines Bundesamts für Sicherheit in der Informationstechnik nicht allen Risiken gleichzeitig begegnen kann, die sich aus der Entwicklung der IuK-Technologien und deren Anwendung ergeben.

1. KRITIK DER ZIELSETZUNGEN

In seiner einleitenden Vorbemerkung verweist das IT-Sicherheitsrahmenkonzept vom 27.9.1989 darauf, daß

> "in zunehmendem Maße nahezu alle Bereiche (öffentliche Verwaltung, Wirtschaft, Verteidigung usw.) weitgehend von dem einwandfreien Funktionieren und der uneingeschränkten Verfügbarkeit der IT abhängig sein" werden. "Zugleich ist mit der Zunahme von Risiken zu rechnen, die die Vertraulichkeit der Daten des einzelnen Bürgers wie die der Wirtschaft und des Staates gefährden."[53]

Dieser Problembeschreibung werden die nachfolgenden Antworten des Rahmenkonzeptes jedoch nicht gerecht. Während in der Vorbemerkung das Problem zutreffend noch in der steigenden Abhängigkeit des einzelnen Bürgers und der Gesellschaft insgesamt vom Funktionieren der Informations- und Kommunikationstechniksysteme und in den sozialen Folgen ihres Ausfalls oder Mißbrauchs gesehen wird, so geht diese Problemsicht in der Detaillierung der Probleme und in der Formulierung von Handlungszielen und -konzepten zunehmend verloren.

Der Problembeschreibung angemessen wäre es gewesen, nach der Verletzlichkeit der Gesellschaft durch den zunehmenden Einsatz der Informations- und Kommunikationstechnik zu fragen.[54] Werden durch die konkreten sozialen Anwendungen der IuK-Technik die Möglichkeiten großer Schäden für einzelne oder die Gesellschaft erhöht oder reduziert? Welche sozialen Auswirkungen haben die möglichen Schäden, aber auch die erforderlichen Maßnahmen zu ihrer Verhinderung oder Verminderung für das soziale und politische System?

Das Problem der Verletzlichkeit entsteht vor allem dadurch, daß soziale Funktionen von Menschen auf Informations- und Kommunikationssysteme übertragen werden. Informationsverarbeitung und Kommunikation werden dadurch vom Funktionieren einer Technik abhängig, auf die sich die Menschen verlassen. Im Vertrauen auf die Technik erhöhen sie deren Leistungsfähigkeit - und damit zugleich das Schadenspotential. Durch diese Übertragung werden zudem Informationsverarbeitungs- und Kommunikationsprozesse für Dritte zugänglich. Sie können diese leichtfertig oder mißbräuchlich ausforschen, manipulieren, unterbinden, beschädigen oder zerstören. Fehler und Manipulationen können so die Erfüllung der dem technischen System übertragenen gesellschaftlichen Funktionen beeinträchtigen. Diese Erkenntnis führt zu zwei Folgerungen:

---

[53] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 1.1.

[54] Vgl. zum Kriterium der Verletzlichkeit ausführlich A.Roßnagel/P.Wedde/V.Hammer/U.Pordesch, Die Verletzlichkeit der Informationsgesellschaft, Opladen 1989. Diese Studie ist der erste Teil des im Auftrag des Ministers für Arbeit, Gesundheit und Soziales des Landes Nordrhein-Westfalen durchgeführten Forschungsprojekts "Informatisierung der Gesellschaft: Verfassungsverträglichkeit und Verletzlichkeit des sozialen und politischen Systems".

Zum einen ist nicht nur ein technisches System (Computer) zu analysieren und zu bewerten, sondern auch dessen soziale Funktion im Rahmen einer konkreten Anwendung. Denn nur so kommen die Abhängigkeit des einzelnen oder der Gesellschaft von der Technik und die mit einem Funktionsversagen verbundenen Schadenspotentiale in den Blick. Daher ist es notwendig, die IuK-Systeme auch in Sicherheitsanalysen als soziotechnische Systeme zu betrachten.

Zum anderen ist nicht nur die Sicherheit von Geräten und Softwareprodukten zu verbessern. Vielmehr sind vor allem Handlungskonzepte zu entwerfen,

- um die gesellschaftliche Abhängigkeit von Systemen der IuK-Technik zu verringern,
- um die potentiellen Schäden eines Mißbrauchs oder Fehlers der IuK-Systeme und die sozialen Folgen eingetretener Schäden zu vermindern,
- um zu verhindern, daß durch die Techniknutzung neue Mißbrauchsmotive hervorgerufen werden,
- um auszuschließen, daß die IuK-Technik neue Mißbrauchsmöglichkeiten und Fehlerquellen eröffnet, und zu erreichen, daß sie bestehende reduziert,
- um zu verhindern, daß die unvermeidlichen Sicherungsmaßnahmen negative Folgen für die Grundrechtsausübung des einzelnen und das soziale und politische System insgesamt hervorrufen.

In den Blick zu fassen, sind daher nicht nur die Risiken, die aus Sicherheitsmängeln technischer Produkte entstehen, sondern auch die Risiken, die von den sozialen Bedingungen und Folgen der IuK-Technik-Nutzung und -sicherung im betrieblichen und gesellschaftlichen Kontext hervorgerufen werden.[55] Und als Risiken dürfen nicht nur die Ausfallkosten eines defekten Techniksystems, der Verrat militärischer Geheimnisse, die finanziellen Verluste durch Computerkriminaltität oder verminderte Exportchancen verstanden werden. Als Risiken sind auch und vorwiegend die Nachteile zu betrachten, die dem einzelnen Bürger und der Gesamtheit durch den Ausfall der auf die IuK-Technik übertragenen sozialen Funktionen (Verkehr, Strom, Handel, Zahlungsverkehr, usw.) entstehen. Außerdem sind die negativen Folgen zu begreifen, die sowohl durch die möglichen Schäden als auch durch die Sicherungsmaßahmen zu ihrer Verhinderung für die Ausübung von Grundrechten und einen freien Prozeß politischer Willensbildung entstehen können.[56]

Diese Erkenntnis erfordert Zielsetzungen, die dieser Problembeschreibung gerecht werden, und Maßnahmen, die durch eine präventive Gestaltung der IuK-Technik diese Risiken vermeiden oder zumindest verringern.

Dagegen beschränkt die Bundesregierung die Zielsetzungen ihres Rahmenkonzepts auf einen schmalen Ausschnitt aus dem Problemfeld der Verletzlichkeit der Gesellschaft:

Die Stärkung internationaler Wettbewerbsfähigkeit bundesrepublikanischer IuK-Produkte durch die Verbesserung ihrer Sicherheitseigenschaften ist ein legitimes Ziel, gemessen an dem zentralen Problem der Verletzlichkeit der Gesellschaft aber ein eher randständiges Folgeproblem.

Auch die Verbesserung der Spionage- und Sabotagesicherheit militärischer Informationsverarbeitung und Kommunikation ist ein begreifliches Ziel, für die Sicherheit der Bürger und der Zivilgesellschaft aber ohne aktuelle Relevanz.

---

[55] Zu einem erweiterten Verständnis von Sicherheit vgl. auch Raubold, Sicherheit ist mehr als Schutz vor Angriffen, GMD-Spiegel, 1989, S. 16 ff.

[56] Vgl. zur Notwendigkeit repressiver und präventiver Sicherungsmaßnahmen und ihrer Freiheits- und Demokratiekosten näher A.Roßnagel u.a., Die Verletzlichkeit der Informationsgesellschaft, Opladen 1989, S. 199 ff.; V.Hammer/U.Pordesch/A.Roßnagel, "Freiheit oder Sicherheit - ein Widerspruch informationstechnischer Vernetzung?", in: Valk, R. (Hrsg.), Vernetzte und komplexe Informatiksysteme, 18.GI-Jahrestagung Hamburg 1988, Heidelberg 1988, 506ff. Hier ergibt sich auch eine deutliche Parallele zur Atomtechnik. Vergl. A,Roßnagel, Bedroht die Kernenergie unsere Freiheit, München 1983

Und selbst die Zielsetzungen der 'Inneren Sicherheit' und der Betriebssicherheit von IuK-Systemen, die Bürgerinteressen anklingen lassen, werden von der Bundesregierung viel zu eng bestimmt. Sie sieht in ihrem Rahmenkonzept die Bedrohung von Bürgergrundrechten offenbar allein in Angriffen mit kriminellem oder staatsfeindlichem Hintergrund, gegenüber denen es gelte, die Sicherheit der IuK-Technik zu gewährleisten. Überhaupt nicht thematisiert werden die Gefahren für Bürgergrundrechte, die sich durch die privaten und staatlichen Betreiber von IuK-Systemen ergeben, die aufgrund ihrer technischen Verfügungsgewalt leichter als externe oder interne "Angreifer" Mißbrauch betreiben könnten. Gefahren dieser Art bestehen in erster Linie darin, daß diese auf personenbezogene Daten, die etwa im Rahmen von Teletransaktionen wie dem elektronischen Zahlungsverkehr oder dem elektronischen Bestellabruf gespeichert werden, zugreifen und diese für ihre Zwecke auswerten können.

Ebensowenig als Ziel setzt sich die Bundesregierung in ihrem Rahmenkonzept die Abwehr von Grundrechtsgefahren, die durch den Gebrauch[57] von IuK-Systemen entstehen. Gefahren dieser Art entstehen etwa durch die zweckspezifische Sammlung von personenbezogenen Daten zur Durchsetzung von Partikularinteressen der Betreiber von IuK-Systemen. Banken beispielsweise werden über Vermögens-, Einnahme- und Ausgabeprofile verfügen, Versicherungen über Einkommens-, Risiko- und Versicherungsprofile, Handels- und Marketingfirmen über Konsumprofile und Personalabteilungen über Leistungs-, Eignungs- und Verhaltensprofile. Verbrauchsdaten, Nutzungsdaten oder Abrechnungsdaten können für unterschiedliche Zeiträume bei Temex-Anbietern, Versorgungsunternehmen, Datenbankanbietern und TELEKOM gesammelt werden. Sie alle bilden keine aktuelle, aber eine **optionale übergroße dezentrale Datenbank.**

Sie bestimmen schon allein durch ihre Anteilnahme an privaten Verhältnissen und die Zuordnung von Bedeutungen zu Sachverhalten das Verhalten von Bürgern.[58]

Unberücksichtigt bleiben in der Zielsetzung der Bundesregierung schließlich die Gefahren für die Sicherheit der Bürger, die nach einer Veränderung der politischen Verhältnisse in den dann geschaffenen umfassenden Zugriffs- und Steuerungsmöglichkeiten des Staates - etwa im Bereich der Telekommunikation - liegen. Eine Erweiterung der Diskussion um diesen Aspekt erscheint schon deshalb sinnvoll, weil bereits die Angst der Bürger vor einem solchen Überwachungsstaat zum Motiv oder zur Rechtfertigung für Angriffe gegen IuK-Systeme zu werden droht.

Schließlich bleibt auch das Ziel der Betriebssicherheit auf den Aspekt der technischen Sicherheit beschränkt. Das IT-Sicherheitsrahmenkonzept verschließt sich allen unmittelbaren Anwendungsproblemen und deren sozialen Folgen. Nicht berücksichtigt werden insbesondere soziale Auswirkungen eines Ausfalls einzelner Systeme in komplexen Netzen. Die Sicherheit der IuK-Technik kann jedoch nicht reduziert werden auf die bloße "Gerätesicherheit". Vielmehr ergibt sich erst aus der konkreten Anwendung einer IuK-Technik das spezifische Gefährdungspotential für die Betroffenen.

Insgesamt zeigen die aus dem Rahmenkonzept ersichtlichen Zielsetzungen, daß es der Bundesregierung bei Forcierung der Informatisierung der Gesellschaft in erster Linie um die begleitende Sicherstellung der internationalen Wettbewerbsfähigkeit, die Sicherung der Akzeptanz der IuK-Techniken und die Gewährleistung der "Inneren" und "Äußeren" Sicherheit geht. Die Sicherheit der Bürger und der Gesellschaft vor den Risiken der Informatisierung sozialer Funktionen und die Beschränkung der Freiheits- und Demokratiekosten der unvermeidlichen Sicherungsmaßnahmen zählen nicht zu den gewählten Aufgabenstellungen.

---

[57] Zum Unterschied von Mißbrauch und Gebrauch der IuK-Technik in dem hier diskutierten Zusammenhang vgl. Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', S. 9.

[58] Vgl. hierzu auch Roßnagel, Technik und die Gefahr für das Individuum, in: Bundeskriminalamt (Hrsg.), Technik im Dienst der Straftatenbekämpfung, Wiesbaden 1990.

2. Kritik des Handlungskonzepts

Das IT-Sicherheitsrahmenkonzept enthält viele - für sich genommen - nützliche und sinnvolle Handlungsvorschläge. Es enthält aber kein Handlungskonzept, das den in seiner Vorbemerkung angesprochenen Problemen gerecht werden könnte. Nicht nur die Zielsetzungen des Rahmenkonzepts sind ungenügend, sondern auch die geplante Art und Weise, sie zu lösen. Die Handlungsvorschläge werden weder die durch die Informatisierung der Gesellschaft steigende Verletzlichkeit verringern noch selbst die eingeschränkten Ziele der Bundesregierung erreichen. Im Detail ist an den Handlungsvorschlägen zu kritisieren:

- die fehlende Zukunftsorientierung

  Das Rahmenkonzept behandelt zwar zukünftig einsetzbare Sicherungstechniken, nicht jedoch die Frage, wo, wozu und in welcher Form IuK-Techniken künftig eingesetzt werden könnten und sollten oder wo und unter welchen Bedingungen aus Risikogesichtspunkten auf einen Einsatz verzichtet werden sollte. Derartige Untersuchungen sind aber unumgänglich, wenn für die künftige 'Informationsgesellschaft' die Abhängigkeit von IuK-Systemen, die Schadenspotentiale möglicher Fehler und Mißbräuche sowie die Motive und Möglichkeiten potentieller Angreifer abgeschätzt werden sollen.

- die Problemverschiebung zur Mißbrauchsverhinderung

  Das zentrale Problem der Verletzlichkeit der Gesellschaft wird nicht in ihrer Abhängigkeit von IuK-Technik-Systemen gesehen, sondern in der Verhinderung von Fehlern und Mißbrauchsaktionen. Das mögliche Schadensausmaß durch den Ausfall oder die Manipulation von IuK-Systemen wird als Problem nur angedeutet und dies auch ausschließlich als Problem der Technikanwender.[59] Weitere Schadensmöglichkeiten, auch Sekundärschäden, für das soziale oder politische System und ihre Auswirkungen auf die Menschen bleiben unberücksichtigt.[60] Das aus der verstärkten Anwendung der IuK-Technik resultierende Katastrophenpotential, beispielsweise beim Ausfall wichtiger Telekommunikationsdienste, wird nicht erkannt.[61] Eine qualitative Bewertung und Gewichtung von Schäden und Abhängigkeiten (gesellschaftliche Relevanz möglicher Schäden), die Erfordernisse von Sicherungsmaßnahmen politisch zu begründen hätte, findet nicht statt.

- unzureichende Bedrohungsanalysen

  Das Rahmenkonzept geht zwar unter dem Stichwort "Bedrohungspotential" auf Angriffsmöglichkeiten und Angreifer ein.[62] Die Art der Darstellung läßt aber befürchten, daß es dabei lediglich um die Bildung abstrakter "Angreifermodelle" geht, die Grundlage der Entwicklung technischer Sicherungsmöglichkeiten sein soll. Dem zu engen Ansatz "Sicherheit der Informationstechnik" entsprechend werden die heutigen und künftigen Motive und Möglichkeiten potentieller Angreifer nicht detailliert untersucht. Ohne derartige Untersuchungen kann aber nicht erkannt werden, wo das heute beobachtbare (meist noch begrenzte) Ausmaß von Schäden einem hohen Sicherungsniveau zu verdanken ist oder nur dem Fehlen entsprechend motivierter Angreifer. Für die Bewertung der künftigen Bedrohung ist diese Abschätzung ebenfalls wichtig, da das künftige Sicherungsniveau nicht nur von den technischen Sicherungsmöglichkeiten abhängt, sondern wegen der hohen Kosten von Sicherungsmaßnahmen auch von den möglichen Schäden nach erfolgten Angriffen. Das Beispiel der Stromversorgungsnetze zeigt, wie über Jahrzehnte hinweg eine Versorgungsstruktur entstanden ist, die gegenüber koordinierten Angriffen nicht geschützt werden kann, wie sich nach der Reaktorkatastrophe in Tschernobyl 1986 zeigte, als im Zuge des militanten Protestes gegen Atomkraftwerke Strommasten umgesägt wurden. Eine ähnliche Entwicklung ist auch bei Telekommunikationsnetzen nicht auszuschließen.[63]

---

[59] Vgl. IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 1.1.

[60] Vgl. im Gegensatz hierzu die Darstellung des Schadenspotentials in Roßnagel u.a., Die Verletzlichkeit der Informationsgesellschaft, 1989, S. 69 ff.

[61] Vgl. hierzu näher Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 69 ff.; Pordesch, Zum Katastrophenpotential der Telekommunikation, Zivilverteidigung II/1989, 41 ff.; Roßnagel/Pordesch, Informationstechnische Vernetzung und Verteidigungsfähigkeit, Sicherheit und Frieden, 1990 (im Erscheinen).

[62] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 4.

[63] Vgl. hierzu auch Pordesch, Zum Katastrophenpotential der Telekommunikation, Zivilverteidigung II/1989, S. 45.

- mangelnde Problematisierung der Verläßlichkeit von Sicherungsmaßnahmen

Technische und administrative Sicherungsmöglichkeiten werden nicht hinsichtlich ihrer immer nur begrenzten Verläßlichkeit problematisiert. Der Erfolg von Sicherungsmaßnahmen hängt jedoch zum einen von der Zuverlässigkeit organisatorischer und menschlicher Voraussetzungen ab, von denen sich in anderen Bereichen gezeigt hat[64], daß sie praktisch vielfach nicht zu gewährleisten sind.[65] Zum anderen müßten die Grenzen untersucht werden, die der Verläßlichkeit von Sicherungssystemen durch die von ihnen vorausgesetzten sozialen und politischen Rahmenbedingungen gezogen werden.[66] Nur eine Berücksichtigung der Grenzen der Verläßlichkeit von Sicherungsmaßnahmen führt zu einer realistischen Sicht des Restrisikos, das durch die Übertragung sozialer Funktionen auf ein Techniksystem in Kauf genommen werden soll.

- keine Betrachtung von Technikalternativen

Die IuK-technische Entwicklung wird als unbeeinflußbar hingenommen. Ihre Risiken sollen allein durch ergänzende Maßnahmen abgewendet werden. Als mögliche Strategie zur Erhöhung der Datensicherheit wird folglich die Option einer nichttechnischen Problemlösung (auch Datenvermeidung) oder die Suche nach sozio-technischen Alternativlösungen nicht berücksichtigt. Dabei bietet die technische Entwicklung immer wieder ein breites Spektrum von Alternativlösungen, die sich in ihrem Beitrag zur Verletzlichkeit der Gesellschaft beträchtlich unterscheiden. So wurden zum Beispiel für die Bundesrepublik detaillierte Vorschläge unterbreitet, wie Telekommunikationsnetze datenschutzgerechter konzipiert werden könnten.[67] Ohne Beachtung alternativer Lösungsmöglichkeiten kann aber die gesellschaftliche Abhängigkeit von IuK-Systemen nicht verringert werden, um auf diese Weise die Schadensmöglichkeiten und die Sicherungserfordernisse zu reduzieren.

- die Verkennung der gesellschaftspolitischen Dimension

Mögliche nachteilige Effekte von Sicherungsmaßnahmen auf die Grundrechte von Arbeitnehmern, Netzteilnehmern oder sonstigen Betroffenen werden nicht thematisiert (z.B. Personenüberwachung im Zusammenhang mit Zugangs- und Zugriffskontrollen und Protokollierungen). Die möglichen Freiheits- und Demokratiekosten der je nach Informatisierungsgrad der Gesellschaft unterschiedlich notwendigen Sicherungssysteme werden nicht vorausschauend abgeschätzt und politisch bewertet. Durch das unkontrollierte Schaffen von Sicherungszwängen, wird die Gesellschaft in das Dilemma getrieben, künftig zwischen Freiheit und Sicherheit entscheiden zu müssen.[68]

- die Ablehnung aktiver Steuerungsmaßnahmen

Die Aufgabe der Bundesregierung und der Bundesverwaltung wird lediglich in der entwicklungsbegleitenden Herstellung einheitlicher Sicherheitsstandards, in der Erforschung und Entwicklung von IT-Sicherheitskomponenten und -systemen sowie in der Beratung der Anwender und Hersteller von IT-Produkten gesehen. Möglichkeiten der aktiven Marktregulierung werden nicht erwogen. Lediglich eine freiwillige Überprüfung und Zertifizierung von IT-Produkten auf Kosten der Auftraggeber. Nur im staatlichen Bereich sollen Richtlinien für die Verwendung von 'sicherer' IuK-Technik, soweit sie nicht schon bestehen, erlassen werden. Die technische Entwicklung selbst bleibt jedoch außerhalb des Blickfeldes. Ein steuernder oder auch nur korrigierender Eingriff aus Sicherheitsgesichtspunkten ist nicht vorgesehen. Weder im staatlichen noch im nicht-staatlichen Bereich soll die zunehmende Abhängigkeit der Gesellschaft und das Entstehen großer Schadenspotentiale in irgendeiner Weise beeinflußt noch sollen gar gezielt sozio-technische Alternativen entwickelt werden.

---

[64] Vgl. etwa für den Bereich der Atomenergienutzung Roßnagel, Bedroht die Kernenergie unsere Freiheit? 2. Aufl. München 1983, S. 224 ff.

[65] Vgl. für die Sicherung der IuK-Technik Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 182 ff.

[66] Vgl. hierzu näher Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 187 ff.

[67] Vgl. dazu z.B. Pfitzmann/Pfitzmann/Waidner Datenschutz garantierende offene Netzwerke, Informatik Spektrum 1988, S. 118 ff.; Berger u.a., Optionen der Telekommunikations-Infrastruktur, 1988, Band III.

[68] Vgl. hierzu z.B. Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 175 ff.; Hammer/Pordesch/Roßnagel, 18.GI-Jahrestagung 1989, S. 506 ff.

Ingesamt erscheint das IT-Sicherheitsrahmenkonzept als ein halbherziger Versuch der Bundesregierung, einem von ihr mitverursachten Dilemma entgehen zu wollen. Auf der einen Seite forciert sie den Wettlauf in die 'Informationsgesellschaft'[69], auf der anderen Seite muß sie aber die Sicherheitsgefahren und Sicherungszwänge erkennen, die sie damit setzt. Diese Risiken gefährden nun die Akzeptanz des eingeschlagenen Weges in die 'Informationsgesellschaft' und zwingen die Bundesregierung zum Handeln. Da sie aber offensichtlich keineswegs bereit ist, ihre Politik einer forcierten Informatisierung der Gesellschaft zu verändern, versucht sie in ihrem Konzept diese Risiken so zu definieren, daß sie durch die Errichtung eines Bundesamtes und seiner im wesentlichen auf die Verbesserungen der Sicherheitstechnik begrenzten Aufgabenstellung lösbar erscheinen.

Im Ergebnis wird eine Politik, die Sicherheit ausschließlich durch nachträgliche und ergänzende Verbesserung der als gegeben unterstellten Technik erreichen will, weder die Verletzlichkeit der Gesellschaft verringern noch den bereits auf die Belange der Wirtschaft und des Staates begrenzten Zielsetzungen des Rahmenkonzepts gerecht werden können. Ohne vorbeugende Begrenzung der technischen Abhängigkeit der Gesellschaft und einer gezielten Reduzierung der Schadenspotentiale könnte es zu einem gefährlichen Wettlauf zwischen 'Angreifern' und technischer Sicherung kommen, den letztere kaum gewinnnen kann. Dies aber hätte zum einen einen unvertretbaren Anstieg des "Restrisikos" der Informationstechnologie und zum anderen einen sozialunverträglich hohen Zwang zur Sicherung zur Folge.[70]

3. Kritik der Organisationsformen

Nach dem Rahmenkonzept soll die Zentralstelle für Sicherheit in der Informationstechnik in eine obere Bundesbehörde im Geschäftsbereich des Bundesministers des Inneren umgewandelt werden. Dadurch unterliegt das neue Bundesamt für Sicherheit in der Informationstechnik der Rechts- und Fachaufsicht des Bundesinnenministers. Er kann dem Amt in allen Verfahrens- und Sachangelegenheiten bindende Weisungen erteilen. Zugleich soll das Bundesamt für Sicherheit in der Informationstechnik offensichtlich die alten Aufgaben der ZSI und deren Vorgängerin, der ZfCH, weiterführen.[71] Allerdings soll Aufgabenbereich "Entzifferung" beim Bundeskanzleramt verbleiben und räumlich wie organisatorisch vom Bundesamt für Sicherheit in der Informationstechnik getrennt werden.[72] Ob diese Trennung, besonders in personeller Hinsicht, konsequent durchgehalten werden kann, ist jedoch wegen der geringen Zahl von Krypto-Experten zweifelhaft.[73]

Durch die geplante organisatorische Lösung ergeben sich enge funktionelle und organisatorische Verknüpfungen zwischen den öffentlichen Sicherheitsdienstleistungen für zivile IuK-Technik-Hersteller und -Anwender und den Aufgaben der Geheimdienste. Zum einen ist der Bundesinnenminister gleichermaßen wie für das Bundeskriminalamt, den Bundesgrenzschutz und das Bundesamt für Sicherheit in der Informationstechnik auch Rechts- und Fachaufsichtsbehörde für das Bundesamt für Verfassungsschutz.[74] Zum anderen hat das Bundesamt für Sicherheit in der Informationstechnik selbst sowohl die geplanten zivilen Aufgaben zu erfüllen als auch - in Fortführung der alten Aufgaben der ZfCH - Leistungen im Bereich militärischer Sicherheit und staatlicher Geheimhaltung zu erbringen. Auch wenn das Bundesamt für Sicherheit in der Informationstechnik organisatorisch nicht mehr dem Bundeskanzleramt und dem ihm unterstellten Bundesnachrichtendienst zugeordnet sein wird, ist zu befürchten, daß die personelle und organisatorische Kontinuität von der ZfCH über die ZSI bis hin zum Bundesamt für Sicherheit in der Informationstechnik weiter besteht und zu einer zu engen Verflechtung des öffentlichen mit dem Geheimbereich führt.

---

69 Vgl. z.B. Zukunftskonzept Informationstechnik, 1989.

70 Vgl. hierzu näher Roßnagel u.a., Die Verletzlichkeit der 'Informationsgesellschaft', 1989, S. 199 ff.

71 Vgl. dazu IT-Sicherheitsrahmenkonzept und BSIG-E sowie O. Leiberich, Wissenschafts-Pressekonferenz, 6.2.1990.

72 Vlg. H. Neusel, Wissenschafts-Pressekonferenz, 6.2.1990, S. 3 f.

73 Zumal es nach H. Neusel, Wissenschafts-Pressekonferenz, 6.2.1990, S. 3 eng mit den anderen Sicherheitsbehörden und nach O. Leiberich, Wissenschafts-Pressekonferenz, 6.2.1990, S. 3 auch mit "Schwesterbehörden der befreundeten Länder" zusammenarbeiten soll. Auch der BfD äußert in seiner Stellungnahme von W.Schmidt, Wissenschafts-Pressekonferenz, 6.2.1990, S. 2 Bedenken dazüber, daß "die Beteiligung der ZfCh dann doch viel intensiver als gewollt war", da die notwendigen Experten nicht in ausreichender Zahl zur Verfügung stehen.

74 Der Verfassungsschutz hat übrigens nach §3 Abs. 2 Nr. 3 BVerfSchG die Aufgabe, "bei technischen Sicherungsmaßnahmen zum Schutz von im öffentlichen Interesse geheimhaltungsbedürftigen Tatsachen, Gegenständen oder Erkenntnissen gegen die Kenntnisnahme durch Unbefugte" mitzuwirken.

Erfahrungen aus den USA zeigen, daß eine derartige Verflechtung äußerst problematisch ist, weil unterschiedliche Interessen vorliegen. In den USA wurde nach der Direktive NSDD 145 (National Security Decision Direktive) der National Security Agency (NSA) auch der Bereich der Computersicherheit im zivilen Bereich zugeteilt. Aus dem größten Geheimdienst der Welt wurde dadurch eine für die Sicherheit ziviler und nichtziviler Daten zugleich verantwortliche Behörde.[75]

Diese Aufgabenkombination führt zum Beispiel dazu, daß die NSA einerseits Kryptosysteme für die Wirtschaft entwickeln sollte und andererseits im Interesse der Überwachung aber wirkungsvolle Kryptosysteme und insbesondere den Export von Hard- und Software zum Verschlüsseln verhindern wollte. Es wird vermutet, daß dieser Interessenkonflikt dazu führte, daß die NSA den Einsatz von Kryptosystemen forcierte, deren Algorithmen nicht offengelegt werden sollten und deren Wirksamkeit (auch gegenüber den Ausforschungsmöglichkeiten der NSA) sich der öffentlichen Kontrolle entzog. Die internationale Normierung der für den gesamten Bereich der Teletransaktionen zentralen Verschlüsselungsverfahren DES und RSA, deren Algorithmen bekannt und fachöffentlich diskutiert werden, soll hingegen auf Betreiben der NSA zu Fall gebracht worden sein.

Ferner führte die Direktive des Präsidenten zu einer erheblichen Ausweitung dessen, was die NSA als zu schützendes Gut ("sensitive Data") klassifizierte. Auf diese Weise versuchte die NSA, die Verbreitung dieser Daten zu kontrollieren. Die Einführung staatlicher Kontrolle über Daten im wirtschaftlichen und privaten Bereich erzeugte jedoch erhebliche Widerstände durch Industrie, Banken und wissenschaftliche Verbände. Dieser Druck führte letztlich zur Ablösung der NSDD 145 durch den Computer Security Act. Seither ist die Kontrolle über Maßnahmen der Computersicherheit im zivilen Bereich weitgehend wieder an das National Bureau of Standards übergegangen, das dem Department of Commerce untersteht.

Aufgrund der geplanten Organisationsform und Aufgabenstellung und der personellen und organisatorischen Kontinuität zur ZfCH ist auch für das Bundesamt für Sicherheit in der Informationstechnik zu befürchten, daß ähnliche Interessenkonflikte entstehen wie für die NSA. Diese Befürchtungen werden durch einige Indizien verstärkt. So soll die ZfCH bereits in der Vergangenheit erreicht haben, daß die Normung des DES durch das Deutsche Institut für Normung (DIN) eingestellt wurde.[76] Nach dem Rahmenkonzept sollen künftig spezielle Sicherheitskriterien als Verschlußsache eingestuft werden und nicht oder nur an Unternehmen herausgegeben werden, wenn sich diese der Geheimschutzbetreuung des Bundesministeriums der Wirtschaft unterwerfen.[77] Für zertifizierte Produkte sollen Ausfuhrbeschränkungen angeordnet werden können, wobei nicht mehr nur Kryptosysteme, sondern im Einzelfall auch andere IT-Produkte Vertriebsbeschränkungen unterliegen. Sollten die Bestimmungen des Rahmenkonzeptes eng ausgelegt werden, ist zu befürchten, daß die Sicherheit in der Informationstechnik in vielen gesellschaftlichen Bereichen nicht mehr durch regierungsunabhängige Stellen, Öffentlichkeit und Wissenschaft beurteilt werden kann. Auch ist nicht auszuschließen, daß der Grad der Sicherheit bei IT-Anwendungen im wirtschaftlichen Bereich aufgrund von Vertriebsbeschränkungen hinter den tatsächlichen Sicherungsmöglichkeiten zurückbleiben könnte. So sind derzeit abstrahlsichere Computersysteme und Datenverarbeitungsanlagen nur für die NATO und wenige Regierungsstellen nach vorheriger Genehmigung durch die ZSI, nicht aber für 'normale' Anwender verfügbar.[78]

---

[75] Vgl. dazu und zum folgenden Bernhard/Ruhmann, Computerwoche vom 22.12.89 mwN.

[76] Waidner/Pfitzmann/Pfitzmann, DuD 6/87, S. 297.

[77] IT-Sicherheitsrahmenkonzept vom 27.9.1989, Pkt. 6.1.

[78] Vgl. z.B. Schmidt, Kompromittierende Abstrahlung, DuD 1987, S. 276 ff.; Abel/Schmölz, Datensicherung für Betriebe und Verwaltung, 306 ff.; Wirtschaftswoche 34/1986, S. 62 ff.

4. BEFÜRCHTUNGEN FÜR DIE BÜRGERSICHERHEIT

Das Bundesamt für Sicherheit in der Informationstechnik soll "Komponenten, die ... für die Verarbeitung oder Übertragung amtlich geheimgehaltener Informationen (Verschlußsachen) eingesetzt werden sollen" zulassen, "sowie die Herstellung der Schlüsseldaten, die für den Betrieb zugelassener Verschlüsselungsgeräte benötigt werden" übernehmen.[79] Das Bundesamt wird deshalb eine erheblichen Einfluß auf die Entwicklung und den Einsatz von Verschlüsselungsverfahren haben.[80]

Verschlüsselungsverfahren können in der Zukunft einen erheblichen Beitrag zur Sicherung der Freiheitsgrundrechte leisten. Um die Bedeutung des neuen Bundesamts für Sicherheit in der Informationstechnik richtig einschätzen zu können, müssen wir deshalb einen Blick in die Zukunft und auf mögliche künftig in einem solchen Zusammenhang auf dieses Amt zukommende Aufgabenstellungen werfen. Denn ein solches Amt soll nicht nur den derzeitigen, sondern auch den absehbaren künftigen Aufgaben gerecht werden. Hierzu sind allerdings noch keine Planungen der Bundesregierung bekannt geworden. Unbekannt ist sogar, ob überhaupt Planungen bestehen oder vorbereitet werden. Wir können daher in dieser Hinsicht nur Befürchtungen formulieren, die aus geschichtlichen Erfahrungen und parallelen Entwicklungen in den USA gespeist werden, und vor Entscheidungen warnen, die zu negativen gesellschaftlichen Veränderungen führen würden.

Zwei solcher künftiger Entwicklungsmöglichkeiten erscheinen uns in diesem Zusammenhang besonders relevant, weil sie Chancen für mehr Bürgersicherheit und Bürgerfreiheit beinhalten, die durch eine falsche organisatorische Behandlung aber leicht zerstört werden können: Die durch die IuK-Technik geschaffenen Möglichkeiten sicherer und anonymer Teletransaktionen und unausforschbarer Telekommunikation.

Zum einen könnte IuK-Technik eine Antwort auf die Probleme bieten, die hinsichtlich der Vertrauenswürdigkeit des Gegenüber, der Manipulationsgefährdung von elektronischen Nachrichten und Dokumenten und der Auswertbarkeit personenbezogener Daten durch die Informatisierung der Gesellschaft - die im folgenden unterstellt wird - hervorgerufen oder verschärft werden. Wie sicher kann man sein, daß derjenige, mit dem man telekommuniziert, auch der ist, der zu sein er vorgibt? Wie sicher kann man sein, daß die von ihm übermittelte Nachricht oder eine gespeicherte Urkunde nicht manipuliert ist? Wie sicher kann man sein, daß der Kommunikationspartner - ein Versandhandel, eine Bank, eine Versicherung, eine Behörde - die durch den Telekontakt bekannt gewordenen Daten nicht speichert und auswertet? Die erste Chance für einen freiheitserweiternden Einsatz von IuK-Technik ergibt sich aus der Möglichkeit, eine vertrauenswürdige Identifikation, eine Manipulationskontrolle und eine anonyme Kommunikation zugleich zu gewährleisten.

Zum anderen können digital übertragene Daten in den modernen Übertragungsnetzen und elektronisch übersandte oder gespeicherte Texte prinzpiell technisch leichter erfaßt und bei gleicher Personalausstattung mit größerem Technikeinsatz leichter ausgewertet werden. Für gesprochene Sprache ist dies noch sehr eingeschränkt möglich, aber auch dafür sind im Laufe der nächsten 20 Jahre erhebliche Fortschritte zu erwarten. Für Texte dagegen sind heute bereits alle erforderlichen Verfahren zur Auswertung - etwa Schlüsselwortanalyse - entwickelt. Die zweite Chance für einen freiheitserweiternden Einsatz von IuK-Technik liegt in der Möglichkeit, die Inhalte der Telekommunikation oder elektronisch gespeicherter Texte für Dritte, auch gegenüber staatlicher Überwachung, unausforschbar zu machen.

Mehr Bürgersicherheit durch technischen Schutz der Privatsphäre bieten Verschlüsselungsverfahren[81], die in Kryptoprozessoren implementiert sind. Kryptoverfahren spielen in der Diskussion um die 'innere' wie 'äußere' Sicherheit und die Sicherheit von Geschäftsgeheimnissen von Banken und anderen Konzernen schon lange eine wichtige Rolle. Durch die elektronischen Medien und aufgrund der Ausweitung von elektronischen Dienstleistungen in alle Unternehmen und in die meisten Haushalte hinein werden Verschlüsselungsverfahren zwangsläufig auch in der allgemeinen geschäftlichen Telekommunikation gebräuchlich werden. Denn sie sind derzeit die einzige Möglichkeit, die Rechtssicherheit von Teletransaktionen in 'offenen' Netzen zu gewährlei-

---

[79] § 3 BSIG-E.

[80] siehe oben II.3 und Fn. 72.

[81] siehe dazu z.B. Denning, E. "Cryptography and Data security"; Addison Wesley, Reading 1982.

sten. Die sich zu dieser absehbaren Entwicklung aufdrängende Frage ist nun, ob die Verschlüsselung auch für die Bürger ein Mittel zur Sicherung ihrer Grundrechte sein könnte. Wie dies möglich wäre und welche Bedeutung hierfür das Bundesamt für Sicherheit in der Informationstechnik spielen könnte, sei im folgenden kurz angedeutet.

Das anzustrebende Verschlüsselungsverfahren müßte die Übertragung verschlüsselter Nachrichten zwischen beliebigen Personen und auch zu Institutionen ermöglichen. Klassische Verschlüsselungsverfahren erfordern jedoch immer einen geheimen Austausch des zu verwendenden - für beide Seiten gleichen - Schlüssels. Dies ist für eine gesellschaftsweite Nutzung nicht praktikabel.

Angewendet werden könnte jedoch ein asymmetrisches Verschlüsselungsverfahren. Die Verfahren arbeiten nur mit Schlüsselpaaren. Der Entschlüsselungsschlüssel läßt sich praktisch nicht aus dem Verschlüsselungsschlüssel ableiten. Weil deshalb einer der beiden Schlüssel veröffentlicht werden kann, werden sie auch als Public-Key-Systems bezeichnet. Wie in einem Telefonbuch kann jeder den Schlüssel des gewünschten Kommunikationspartners nachlesen, ohne daß vorher eine Absprache getroffen werden muß.

Eine technische Anwendung eines Public-Key-Systems wird beispielsweise von der Gesellschaft für Mathematik und Datenverarbeitung (GMD) entwickelt. Das technische und organisatorische Konzept, das unter dem Namen TeleTrusT[82] entsteht, soll einerseits den Austausch elektronischer Nachrichten in der Form unterstützen, daß Manipulationen sicher erkannt und die jeweiligen Absender einer Nachricht zuverlässig identifiziert werden können. Außerdem ermöglicht TeleTrusT, daß ein Teilnehmer unter einem Pseudonym handeln kann und seine Anonymität zumindest solange gewahrt wird, solange er dadurch niemanden schädigt.

Zugleich können die auf einer Chipkarte implementierten Funktionen für die Verschlüsselung von Nachrichteninhalten eingesetzt werden. Durch diese Abhörsicherung könnten Bürger vertrauliche Informationen vor Lauschern verbergen und ihre Schutzbedürfnisse hinsichtlich ihrer Persönlichkeitsrechte nach eigenem Empfinden befriedigen.

Werden allerdings sensible Transaktionen mit Hilfe von Verschlüsselungsverfahren abgewickelt und das Verfahren oder der Schlüssel sind nicht ausreichend sicher, könnten Lücken im Sicherungssystem zu hohen materiellen wie immateriellen Schäden für einzelne Bürger oder die gesamte Gesellschaft führen. Daher setzt jedes Public-Key-System zum einen voraus, daß der geheime Schlüssel vor möglichen Angreifern wirklich geheim gehalten wird. Wenn es einem Angreifer gelingt, den privaten Schlüssel auszuspähen, sind die Datenübermittlung von und an den Inhaber des ausgespähten geheimen Schlüssels nicht mehr gesichert. Seine Nachrichten können manipuliert werden. Dritte können seine Identität vortäuschen. Verschlüsselte Nachrichten an ihn können abgehört und in Klartext übersetzt werden.

Zum anderen muß das Verschlüsselungsverfahren ausreichend sicher sein. Ist dieses gebrochen, können Teletransaktionen nur noch unter einem hohem Manipulationsrisiko ausgeführt werden. Ob ein Schlüssel oder ein Verschlüsselungsverfahren ausreichend sicher ist, kann nur in einer öffentlich geführten, unabhängigen Fachdiskussion geprüft werden. Nur so kann auch das Risiko eines auf Verschlüsselung basierenden Sicherungssystems abgeschätzt werden.

Im Gegensatz zu diesen Anforderungen haben die Behörden der inneren Sicherheit und die Nachrichtendienste ein erhebliches Interesse an Kommunikationsbeziehungen und -inhalten. Zu ihren Aufgaben gehört nicht nur die Sicherung staatlicher Informationsübertragung, sondern auch das Brechen gegnerischer Codes. Sie wollen deshalb verhindern, daß sichere Verschlüsselungsverfahren der organisierten Kriminalität oder gegnerischen Geheimdiensten zur Verfügung stehen. Sie argumentieren, daß ihr technologischer Vorsprung die Voraussetzung für den Erfolg gegen Terrorismus, Drogenhandel und fremde Geheimdienste ist. Sie sind daher daran interessiert, daß sie die technische Entwicklung von Verschlüsselungsverfahren beeinflussen, Verschlüsselung für den allgemeinen Gebrauch verhindern, oder zumindest dessen Normung hinterteiben oder sich jedenfalls den Erfolg von Brechnungsbemühungen durch eine Begrenzung der Schlüssellänge sichern.[83]

---

[82] Zur Beschreibung des Verfahrens siehe z.B. verschiedene Autoren in GMD-Speigel 1/86 und 1/88, siehe auch Hammer, V. "TeleTrusT: Verletzlichkeit und Verfassungsverträglichkeit eines Konzeptes für reschtssichere Transaktionen in der Informationsgesellschaft", DuD 8/1988 S. 391 ff.

[83] Vgl. beispielsweise Waidner, M./ Pfitzmann, B./ Pfitzmann, A.: "Über die Notwendigkeit genormter kryptographischer Verfahren" S. 294, DuD 6/1987, S. 294.

In diesem Feld sind Konflikte zwischen 'Staatssicherheit' und 'Bürgersicherheit' abzusehen. Welche Rolle in diesem Konflikt das Bundesamt für Sicherheit in der Informationstechnik spielt, wird durch seine Aufgabenbeschreibung, seine Organisationsform und seine personelle und organisatorische Kontiniutät mit der ZfCH weitgehend vorbestimmt. Daher ist auf diese Bestimmungsfaktoren besondere Aufmerksamkeit zu richten. Denn - wie bereits angedeutet - lassen parallele Entwicklungen in den USA befürchten, daß Verbesserungen der Bürgersicherheit verhindert werden.

So erreichte zum Beispiel die NSA, daß die Schlüssellänge des DES-Algorithmus, der 1977 von dem für Normierung im zivilen Bereich zuständigen National Bureau of Standards (NBS) zum Standard erklärt worden war, auf 56 statt auf 128 Bit begrenzt und die vollständige Veröffentlichung der Implementierung verboten wurde. Für die Verkürzung wurden von der NSA die nationalen Sicherheitsinteressen angeführt.[84] Durch die Längenbegrenzung der Schlüssel dürften Schlüsseltexte mit großem Aufwand entziffert werden können - ein erforderlicher Aufwand, der zwar vor privaten Brechungsversuchen schützt, nicht aber vor einem Geheimdienst wie der NSA.[85] Vermutet wird sogar, daß sich die NSA im Verfahren eine Geheimtür offen hält, um Nachrichten zu entschlüsseln.[86] Sie soll ihr bekanntgewordene Fehler in dem Kryptosystem verschwiegen haben.

Zusätzlich hat die NSA ihren Einfluß geltend gemacht, um die Internationale Normung von Kryproverfahren zu verhindern. Denn es ist offensichtlich, daß gute oder praktisch sichere Verschlüsselungssysteme wie Public-Key-Systeme eine "freie" Arbeit der Geheimdienste behindern wird.[87] Internationale Normen zuverlässiger Kryptoverfahren wären aber gerade erforderlich, um einen reibungslosen, unmanipulierbaren Nachrichtenaustausch zwischen Wirtschaftsunternehmen zu ermöglichen und eine einfache Handhabung und Vertrauenswürdigkeit für den Bürger zur Nutzung elektronischer Dienste zu garantiern.

Zwischenzeitlich beabsichtigte die NSA sogar, die Entwicklung von Verschlüsselungsverfahren und die Schlüsselverteilung selbst zu übernehmen. So sollte der DES-Algorithmus durch drei andere, von der NSA geheimgehaltene Verfahren abgelöst werden.[88] Die NSA wäre dann in der Lage gewesen, mühelos jede für sensitiv gehaltene Nachricht trotz Verschlüsselung mitzuhören.[89]

Gegen diese Entwicklung wurden jedoch rechtsstaatliche Bedenken und wirtschaftliche Interessen geltend gemacht. So wurde etwa kritisiert, die Übernahme der Standardisierung der öffentlichen wie auch der geheimen Verschlüsselungsverfahren sowie die Kontrolle über das Schlüsselmanagement würden dem Prinzip der Gewaltenteilung widersprechen und der NSA einen unangemessenen Einfluß geben.[90] Außerdem wurde die einseitige Orientierung der NSA an staatlichen Interessen bemängelt, die den industriellen Erfordernissen nicht gerecht werde. Sie würde das Innovationspotential im Kryptobereich und den internationalen Datenaustausch behindern und in die Wettbewerbsfreiheit im Telekommunikationssektor eingreifen.[91]

Dieser Widerstand - unter anderem der American Bankers Association - führte zwar dazu, daß durch den Computer Security Act dem NBS im Zuge seiner Umstrukturierung zum National Institute of Standards and Technology (NIST) wieder die Festlegung von Verschlüsselungsstandards für zivile Behörden übertragen

---

[84] Vgl. Coy, W.: "Geheime Schriften, geheime Dienste" S. 89, in: Michel, K./ Spengler, T. (Hrsg.): "Kursbuch 66" S. 83 ff.; Kursbuchverlag, Berlin 1981.

[85] Vgl. Coy, W.: "Geheime Schriften, geheime Dienste" S. 88 f. und dort auch Fn. 8.

[86] Fölsing, A.: "Die hohe Schule der Kryptologie", S. 103, in: Michel, K./ Spengler, T. (Hrsg.): "Kursbuch 66" S. 92 ff.; Kursbuchverlag, Berlin 1981.

[87] Vgl. Fölsing, A.: "Die hohe Schule der Kryptologie", S. 105.

[88] Schreiben der Botschaft der Bundesrepublik an das Auswärtige Amt vom 7.1.1987. Rihaczek, K.: "Datensicherheit amerikanisch", DuD Heft 5/1987, S. 240 ff.

[89] "Ein solches System wäre dann die offizielle Installation eines 'großen Bruders'." Waidner/Pfitzmann/Pfitzmann, DuD 6/87, S. 298; Vgl. hierzu auch näher unten II.4.

[90] Aussagen des OTA Berichts-Entwurf "The Integrity and Confidetially of electronic Informations" nach: Schreiben der Botschaft der Bundesrepublik an das Auswärtige Amt vom 7.1.1987, S. 10 f.

[91] Vgl. Computerworld vom 11.1.1988, S. 13; Aussagen des OTA Berichts-Entwurfs "The Integrity and Confidetially of Electronic Informations" nach: Schreiben der Botschaft der Bundesrepublik an das Auswärtige Amt vom 7.1.1987, S. 10 f.

wurde.[92] Ein erheblicher Einfluß der NSA wird aber weiterhin zu erwarten sein. Ein grundsätzlicher Umschwung in der internationalen Normung von Kryptostandards ist nicht erkennbar.

Möglicherweise sind die Sicherungsbemühungen nationaler Sicherheitsbehörden für Wirtschaftsunternehmen ausreichend, auch wenn durch unterschiedliche Ziele und Anwendungen Defizite zu erwarten sind. Daß sich eine sichere Infrastruktur mit Verschlüsselungsdiensten zur vertraulichen Kommunikation von Bürgern unter den beschriebenen Voraussetzungen entwickeln wird, ist nicht zu erwarten. Im Interesse der Freiheitsgrundrechte des Bürgers und somit als Grundlage der Demokratie muß deshalb die Unabhängigkeit der zuständigen Behörden sichergestellt werden. Diese würde eine Voraussetzung schaffen, um die unterschiedlichen politischen Interessen in einem demokratischen Prozeß auszugleichen.

[92] Vgl. "Computer Security Act of 1987"; siehe auch Computerworld vom 11.1.1988, S. 13.