Prof. Dr. iur. Bernd Lutterbeck
Technische Universität Berlin
Institut für Angewandte Informatik
25. April 1997

IT-SICHERHEIT ALS STAATSAUFGABE?

Einleitendes STATEMENT zu einer Podiumsdiskussion auf dem 5. IT-Sicherheitskongreß "Mit Sicherheit in die Informationsgesellschaft" in Bad-Godesberg am 29.4.1997.

TEILNEHMER:	**E. Lintner** (MdB, Parlamentarischer Staatssekretär beim BMI)
	H. J. Tauss (MdB (SPD))
	B. Lutterbeck
	A. Büllesbach (debis Systemhaus GmbH)
	H. Stöckert (DASA München)
MODERATION:	**D. Henze** (Präsident des Bundesamtes für Sicherheit in der Informationstechnik)

1. DIE IT-SICHERHEIT VERDIENT MEHR AUFMERKSAMKEIT ALS IN DER VERGANGENHEIT

Encryption technologies are the locks and the keys of the information age - aber was verbirgt sich hinter dem Verschlossenen ?

Dieser englische Satz hat mir gut gefallen. Ich fand ihn Ende März in meiner elektronischen Post. Mit diesem zusammenfassenden Satz protestierte eine amerikanische Bürgerbewegung gegen den neuerlichen Versuch der Clinton-Administration, diesmal durch einen "Data Security Act" ein gewisses Verbot der Verschlüsselung durchzusetzen. (http://www.crypto.com/clinton/)

In Wirklichkeit wird man sich über die grundlegende Aussage dieses Satzes nicht streiten müssen. Alle Beteiligten, wo immer sie stehen mögen, dürften verstanden haben, daß es sich bei dem Problem der Verschlüsselung schon lange nicht mehr um ein Thema handelt, welches gewisse Diplomaten, ganz

geheime Geheimdienstler und eher verrückte Mathematiker, die sowieso niemand verstehen kann, unter sich ausmachen.

Kryptographie ist eine Schlüsseltechnologie unser Zeit geworden.

Man kann natürlich darüber streiten, welchen Stellenwert Kryptographie innerhalb eines Konzepts von IT-Sicherheit hat. Sieht man sich allerdings den Gehalt der wichtigsten aktuellen Streitthemen an, so wird klar, daß der Satz "Encryption technologies are the locks and keys of the information age" schon ziemlich genau den Kern zu treffen scheint. In der einen oder anderen Form spielen diese Technologoien eine Rolle bei der staatlichen und privaten Behandlung von Schmuddelinhalten im Internet, bei allen geschäftlichen, insb. finanziellen Transaktionen, beim Streit um die urheberrechtliche Behandlung von Faktendatenbanken, bei dem Streit um Zensur im Netz.

Die vernetzte Informationstechnik ist ubiquitär, entsprechend ist auch das Bemühen um Sicherheitstechnik ubiquitär.

Die hier Versammelten und alle aktiv um die Gestalt der Informationgesellschaft Streitenden dürften auch darüber übereinstimmen, daß das erreichte Niveau von Sicherheit - einmal ganz intuitiv gesprochen - unbefriedigend ist. Bei manchen Anwendungen weniger, bei manchen mehr. Aber es ist weniger die einzelne Anwendung als das Gesamtkonzept, über das , übrigens nicht nur in Deutschland, gestritten wird.

Strittig ist, wer welche Maßnahmen aus welchem Interesse ergreifen muß.

Drei Typen von Akteuren und diverse Mischformen stehen zur Auswahl:

- der Staat, bzw. Staatenbünde wie die Europäische Union
- die Wirtschaft
- die Bürger und Bürgerinnen

Auch wenn sich hinter der Überschrift des Podiums noch schamhaft ein Fragezeichen verbirgt, so will es doch wohl die Dramaturgie der Tagung, daß wir IT-Sicherheit prinzipiell verorten. Die Fragestellung dieses Podiums kommt jedenfalls mit einiger Wucht daher. Dann aber muß man das Thema Sicherheit auch umfassend behandeln. Ohne das Thema "Information Warfare"

etwa , das gegenwärtig amerikanische Militärs in Angst und Bangen versetzt, ist das sicher nicht zu leisten.

(Einen guten Überblick geben die Sourcen in http://www.infowar.com)

Das Bild von dem Schloß und dem Schlüssel des Informationszeitalters hat mir wie gesagt gut gefallen. Es führt zu der Frage, welchen Raum diese Technik denn erschließt. Man wünscht sich auf diese Frage eine politische, auch gesellschaftliche Antwort und nicht bloß eine technische.

Als Wissenschaftler darf ich mir vorstellen, daß das Podium das Sicherheitsproblem prinzipiell angeht. Ich hoffe dabei, daß sich Reden an die gebildeten Stände vermeiden lassen, das Podium also konkret wird. Ich will mich im Folgenden mit eigenen Wertungen zurückhalten. Ich will versuchen, solche Wege zu zeigen, die auf keinen Fall weiterführen. Ich bin mir auch sicher, daß wir um einige Einsichten nicht herumkommen, um in der Zukunft erfolgreich zu sein. Am Ende will ich dann doch noch etwas Kritik los werden.

2. IRRWEGE DER DISKUSSION

Staatsaufgaben sind alle Tätigkeitsbereiche, die der Staat für sich in Anspruch nimmt. Ist also IT-Sicherheit eine Staatsaufgabe?

"Gott waltet, aber er verwaltet nicht, der König waltet, der Beamte verwaltet."

Dieser in Lehrbüchern gerne zitierte Satz verweist auf die Herkunft unseres Wortes "verwalten" und seine spezifische Orientierung auf den Staat. Heute würde man vielleicht von Input-Orientierung sprechen. Klar war dieses Verständnis vom Verwalten und Regieren nur zu der Zeit, als der Monarch als außerhalb der Gesellschaft stehende Instanz die Kompetenz-Kompetenz für sich in Anspruch nehmen konnte. Diese Staatszentriertheit wirkt sich bis heute aus: "Wir verfügen über keinen verbindlichen oder wenigstens geklärten Begriff von Verwaltung, es ist bis heute unklar, was eine Staatsaufgabe ist und was nicht." Hierzu wird man auch heute nicht mehr sagen können als 1970 **Fritz Ossenbühl** in einem unter Juristen berühmten Vortrag vor den deutschen Staatsrechtslehrern:

"Staatliche Aufgaben sind solche, die der Staat nach der jeweils geltenden Verfassungsordnung zulässigerweise für sich in Anspruch nimmt."

Ob dies der Fall ist, sei eine Frage des Einzelfalls und der Grundrechtsauslegung.

Noch weniger aussagekräftig ist die Definition in einem juristischen Standardwerk wie dem Grundgesetz-Kommentar von **Maunz**, **Dürig** und **Herzog** (Art. 30 N. 5), wo es zum Begriff der Staatsaufgabe lapidar heißt:

"Staatsaufgaben sind alle Tätigkeitsbereiche, die der Staat für sich in Anspruch nimmt."

In dem gleichen Augenblick, wo es mißlingt, den Staat gewissermaßen auf den Begriff zu bringen, finden wir ein empirisches Gebilde vor, das man so kennzeichnen könnte:

- Ein politisch-administratives System, das sich in zahlreiche teils miteinander konkurrierende, teils um lose gekoppelten Einheiten gliedert. Die Vorstellung von einer Einheit des Staates bzw. der Verwaltung erweist sich als Mythos;

- An die Stelle des bipolaren Konzepts Staat-Gesellschaft oder öffentlich-privat sind Konzepte getreten, die den kontinuierlichen Übergang betonen.

Aus dieser Sicht, die von der deutschen und vor allem angelsächsischen Verwaltungswissenschaft weit überwiegend geteilt wird, ist es wenig aussichtsreich, mit dem Konzept der Staatsaufgaben irgend etwas von Belang aufzuzeigen. Der Begriff ist empirisch leer und verführt zu zirkulären Beweisketten.

Mein hoffentlich hier unverdächtiger Speyerer Kollege **Carl Böhret** hat den empirisch vorfindlichen Staat einmal als Funktionalen Staat bezeichnet, der sich allein von den gesellschaftlich notwendigen Funktionen her bestimmt und immer aufs neue legitimiert. Er leitet das entsprechende Buch mit den Sätzen ein:

"Der Staat ist nicht mehr, was er früher einmal war."

Der tradierte Staat als besonderes Wesen ist am Ende."

Man gewinnt mit einem solchen Verständnis neue Handlungsspielräume.

Zum Beispiel wären die Erfolge des New Public Management in zahlreichen Ländern ohne ein solches Verständnis des Staates überhaupt nicht denkbar. Man muß sich aber andererseits an eine neue Form der Austragung öffentlicher Konflikte gewöhnen.

Unsere Podiumsdiskussion wird diesen Befund zur Kenntnis nehmen müssen. In unserem Fall müssen wir die Frage klären:

Welche Funktion hat IT-Sicherheit für unsere Gesellschaft? Was spricht dafür, daß die Gesellschaft diese Funktion dem Staat zuweist?

Der Staat, so meine These, wird sich einreihen müssen, in die Reihe derer, die Interessen am Gegenstand IT-Sicherheit angemeldet haben. Je besser er argumentiert, um so aussichtsreicher seine Chancen auf Belohnung. Seine Chancen werden steigen, wenn es ihm gelingt, die notwendige Debatte nicht als ausschließlich juristische zu führen. Ich jedenfalls halte eine fachliche Debatte, die mit Titeln daherkommt wie

- Grundrecht auf Verschlüsselung

für eher kontraproduktiv - jedenfalls im Augenblick.

3. WOVON WIR ABSCHIED NEHMEN MÜSSEN

Dampfmaschinen explodieren. Das Netz der Netze hält wahrscheinlich einen Atomschlag aus.

Vor Bundesgerichten in Washington D. C. wird gegenwärtig einer der interessantesten Streitfälle um IT-Sicherheitsprobleme entschieden, die mir bekannt geworden sind. Der Fall macht nämlich einen Bruch sichtbar - eine Reihe von Wissenschaftlern würden das Wort "Epochenbruch" benutzen:

Karn v. Department of State

1994 haben die amerikanischen Informatiker **Bruce Schneier** und **Phil Karn** ein Buch über Kryptographie veröffentlicht:

Aplied Cryptography: Protocolls, Algorithms, and Source Code in C. John Wiley and Sons 1994.

Das Buch enthält über 100 Seiten Source-Code für unterschiedliche Algorithmen. Drucktechnisch ist der Code so dargestellt, daß er jederzeit mit einem handelsüblichen Skanner in eine elektronische Form überführt werden kann.

Nach amerikanischen Rechtsvorstellungen fällt Software, die, wie es heißt, "confidelity features" enthält, unter das Exportverbot für Kriegswaffen.

Anfang 1995 beantragten die Autoren eine Exporterlaubnis für das Buch, die ihnen gewährt wurde. Ende 1995 waren weltweit 17.000 Exemplare des Buches verkauft.

Wenige Monate später beantragten sie bei der gleichen Stelle des Department of State eine Exporterlaubnis für das Buch in einer Diskettenversion. Diese wurde ihnen verweigert, mit der bemerkenswerten Begründung, daß die Diskettenversion nicht dem besonderen Schutz der amerikanischen Verfassung unterliege.

Karns Klage vor einem Washingtoner Gericht blieb erfolglos.

(http://venable.com/oracle/oracle7.htm v. 22.3.1996)

Am 21. Januar 1997 hat das Berufungsgericht die Sache wieder an die erste Instanz zurückverwiesen.

(http://www.epic.org/crypto/export_controls/karn_decision_1_97.html)

Mich interessiert hier nicht so sehr, ob man der Gleichung **Software = Waffe** zustimmen kann. Insofern wird in Deutschland oft übersehen, daß auch in Deutschland der Export von Software schon verboten ist, soweit die Software unter die Dual Use Verordnung der Europäischen Union v. 19. 12.1994 fällt (ABL EG L 367/1 und die Allgemeine Software-Anmerkung unter L 367/10). Interessanter und von allgemeinen Interesse scheint mir die unterschiedliche Behandlung des Mediums durch die Behörde. Was oberflächlich betrachtet wie ein Kuriosum aussieht, macht bei näherer Betrachtung durchaus Sinn.

Man kann unterstellen, daß das Department of State sich der Tragweite seiner Entscheidungen bewußt war. Man darf unterstellen, daß den Beamten bekannt war, daß die Software trotz ihres Verbotes weltweit zur Verfügung steht. Spätestens seit ihrer Niederlage gegen die Verbreitung von **Phil Zimmermanns** Pretty Good Privacy dürften die Beamten erfahren haben, daß

ihr Verbot weder im Innern der USA noch außerhalb durchsetzbar ist. Trotzdem diese Entscheidungen. Warum?

Meine Erklärung setzt auf die Vernunft der Beamten. Sie haben einerseits eine Entscheidung für eine Gesellschaftsstruktur getroffen, die sich auf Papier und Bücher gründet. In dieser Gesellschaft ist die freie Meinungsäußerung jedenfalls nach amerikanischen Vorstellungen einer der allerhöchsten Werte, der sich auch gegenüber den Interessen des Staates durchsetzen kann. Indem sie einer Diskette den gleichen Schutz wie einem Buch verweigern, machen sie sichtbar, daß wir es nicht nur mit einem Bruch des technischen Hilfsmittels zu tun haben, sondern mit einem fundamentalen Bruch in den Werten. Das State Department hat sich geweigert, diesen Bruch durch eilige Analogien zu überbrücken. Etwa wie die Richterin in dem parallelen Fall **Bernstein gegen Department of State** in einer Entscheidung von 1996, in dem sie die Gleichung **Algorithmus = Freie Meinungsäußerung** aufstellt.

(http://www.eff.org/pub/Legal/Cases/Bernstein_v_DoS/Legal/960415.decision und http://eff.org/pub/Legal/Cases/Bernstein_v_DoS/Legal/961206.decision)

Eine solche Haltung klärt sicher noch nichts. Sie ist aber aus meiner Sicht ehrlicher und klarer als die Haltung deutscher Staatsanwaltschaften, die seit längerem versuchen, den Service-Provider Compuserve/München und den holländischen Internet-Provider XS4ALL (Access for All) in unterschiedlichen Verfahren auf den Weg des Gesetzes zu bringen. Anfang letzter Woche mußte der DFN die Sperrung des Zugangs zur Internet-Adresse von XS4ALL wieder aufheben. Die Begründung des Sprechers des DFN spricht für sich: "Eine wirksame Sperrung des rechtswidrigen Inhalts des niederländischen Internet-Rechners XS4ALL war nicht möglich."

(vgl. die Presseerklärungen unter http://www.xs4all.nl/spotlight/index_e.html)

Die seriöse **Neue Zürcher Zeitung** hat am 18. April diesen und andere Zensurfälle im Netz folgendermaßen kommentiert:

"Was immer man von diesen Maßnahmen hält, sie verkennen eines: Das Internet, das daraufhin angelegt wurde, einem Atomschlag standzuhalten, wird auch dem Angriff der Zensoren widerstehen. In einem globalen Medium lassen sich nationale Zensurgesetze nicht durchsetzen."

Wir alle, der Staat ebenso wie die Bürger, müssen uns anscheinend Ohnmachtserfahrungen gewöhnen, wie es **Alexander Roßnagel** jüngst

formuliert hat. Ein Staat, eine Rechts- und Sozialordnung, die mit Dampfmaschinen hantieren mußten, hatten es vergleichsweise noch einfach: Man kannte die gefährdeten Rechtsgüter, nämlich Leben, Gesundheit und in neuester Zeit die Umweltqualität. Man konnte davon ausgehen, daß sich das spezifische Risiko einer Technik immer in einem punktartigen Ereignis, in einem Unfall realisieren, bei dem die gebändigten Naturkräfte plötzlich außer Kontrolle geraten können und Energie bzw. Emissionen freisetzen. Davon kann bei der vernetzten Informationstechnik nicht mehr die Rede sein. Der Unfall spielt überhaupt keine Rolle, die gefährdeten Rechtsgüter sind andere. Insoweit ist eine Analogie zwischen alter und neuer Technik nicht möglich.

Die neue Technik ist ausfallsicher, dezentral, nicht hierarchisch.

Wer dieses nicht verstanden hat, wird Schwierigkeiten haben, die Funktionalität von Sicherheit in der Informationsgesellschaft zu bestimmen.

Wahrscheinlich muß man das Selbstbewußtsein einer Großmacht besitzen, um trotz dieser Ausgangssituation mit geradezu offensiven Optimismus in die Zukunft zu blicken. In der angesehenen Zeitschrift Foreign Affairs verweisen **Joseph Nye** und **William Owens**, zwei langjährige Berater der Clinton-Administration, auf einen Aspekt des Sicherheitsproblems, der nun wirklich die Grenzen eines engen Sicherheitsverständnisses sprengt:

"Wissen ist mehr denn je Macht. Das Land, das die Informationsrevolution am besten anführen kann, wird auch mächtiger als andere sein. Auf absehbare Zukunft sind dieses Land die Vereinigten Staaten. Amerika hat seine offensichtliche Stärke in militärischer Macht und seiner ökonomischen Produktion. Aber seine wirkliche Stärke, mit der sie anderen Nationen überlegen ist, ist die Fähigkeit, Informationen zu verarbeiten und darauf Entscheidungen zu stützen....

Dieser Vorsprung ist ein wichtiges Moment amerikanischer Diplomatie, including soft power, das ist die Attraktivität amerikanischer Demokratie und freier Märkte." (S.20, Übersetzung vom Verf.)

Ich bin mir nicht sicher, wie weit das "Soft Power-Konzept" in der internationalen Diplomatie reicht. Ich möchte nur darauf hinweisen, daß es einen außenpolitischen Aspekt des Sicherheitsproblems gibt, zu dem man in der amerikanischen Literatur schon Stimmen findet. Natürlich muß ein solches Konzept davon ausgehen, daß bestimmte Regularien im Netz der Netze nicht mehr möglich sind.

4. MEIN PETITUM

Die Technik **hat sich entscheidend verändert.**

Die Gesellschaft **hat sich sehr verändert.**

Auch *der Staat* ist nicht mehr, was er einmal war.

Viele Unsicherheiten. Wir müssen uns auf die demokratischen Tugenden rückbesinnen!

Ich persönlich sehe einen einschneidenden Wandel in unseren Gesellschaften. Deshalb gehöre ich zu dem Personenkreis, der die Rede vom Epochenbruch für gerechtfertigt hält. Das, was wir mit der Rede von der Informationsgesellschaft manchmal zudecken, ist in Vielem neu. Ich bin mit anderen der Überzeugung, daß die Bundesrepublik bei der Entdeckung des Neuen einen falschen Weg geht. Die Debatte um die IT-Sicherheit ist hierfür vielleicht ein Beispiel:

Es gibt reihenweise Probleme, die die Fachleute lösen müssen. Ein Kongreß wie dieser gibt dazu viele Möglichkeiten.

Es gibt aber auch eine Dimension des Sicherheitsproblems, die weit über den hier anwesenden Expertenkreis hinausweist. Diese Dimension verweist auf viele Unsicherheiten und auf ein Wissen jenseits unseres Expertentums.

Bei Unsicherheiten verfallen unsere bundesrepublikanischen Institutionen leicht in alten hierarchischen Schlendrian. Statt eine Kryptodebatte offen zu führen, wird sie, wie der Berliner Datenschutzbeauftragte in seinem letzten Tätigkeitsbericht anmerkt (S.47), "geradezu konspirativ angegangen". Und die Regulierungsdebatte um das Internet wird noch zu häufig von Männern geführt, die keine Sekunde Erfahrung mit dem Medium haben, wie die frühere Parlamentarische Staatssekretärin Yzer neulich einmal bemerkt hat. Statt offen darüber zu reden, ob IT-Sicherheit eine Aufgabe des Wirtschaftsministeriums oder des Innenministeriums oder wem auch immer ist, bestimmen Bonner Ressort-Egoismen die Tagesordnung. Der grundlegende Fehler, der ausstrahlt auf viele Politikbereiche, aber auch die Wirtschaft, besteht darin, daß noch nicht in der nötigen Breite verstanden ist, daß Top Down-Strategien nicht erfolgreich sein können. Es ist mir ein Rätsel, wie man ohne Mitwirkung der Bevölkerung jemals in der Informationsgesellschaft landen will.

Ich möchte mir eine mögliche Option dieser falschen Strategie lieber nicht

genauer ausdenken:

Wir Experten schmieden emsig die Schlüssel und Schlösser.

Sind wir fertig, stellen wir fest, daß kaum einer Lust hat, den neuen Raum zu betreten.

LITERATURVERZEICHNIS

Bizer, Johann, Rieß, Joachim, Roßnagel, Alexander (1997):
Beschränkungen kryptographischer Verfahren sind verfassungswidrig. In: Jahrbuch Telekommunikation und Gesellschaft 1997, S. 421 f.

Berliner Datenschutzbeauftragter (1997):
Bericht des Berliner Datenschutzbeauftragten für 1996. Berlin 1997.

Bundesbeauftragter für den Datenschutz (1997):
Tätigkeitsbericht 1995-1996. Bonn 1997.

Crypto Law Survey (1997):
Erstellt von Bert-Jaap Koops. In: http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm (Stand April 1997).

Jahrbuch Telekommunikation und Gesellschaft 1997 (1997):
Jahrbuch Telekommunikation und Gesellschaft 1997: Die Ware Information - Auf dem Weg zu einer Informationsökonomie. Hg. von H. Kubicek e.a. Heidelberg: R. v. Decker's Verlag 1997.

Koch, Alexander (1997):
Grundrecht auf Verschlüsselung? In: Computer und Recht 1997, S. 106 ff.

Lutterbeck, Bernd (1995):
Funktionswandel des Staates. Die Out-Sourcing-Problematik aus staatstheoretischer Sicht. In: Büllesbach, A. (Hg.), Staat im Wandel - mehr Dienstleistung, weniger Verwaltung. Köln: Datakontext-Verlag 1995, S. 7 ff.

Lutterbeck, Bernd (1996):

Konturen der Informationsgesellschaft. Über Cyberspace, Globalisierung und den Marktplatz der Ideen. Vortrag, in Veröffentlichung begriffen. In: http://ig.cs.tu-berlin.de/bl/013/index.html.

Möller, Ulf (1997):
Kryptographie: Rechtliche Situation, politische Diskussion. In: http://www.thur.de/ulf/krypto/verbot.html (Stand: 19.4.1997).

Nye, Joseph F., Owens, William A. (1996):
Americas Information Edge. In: Foreign Affairs Vol. 75 No. 2 (March/April 1996), pp. 20 ff.

Roßnagel, Alexander (1997):
Globale Datennetze: Ohnmacht des Staates - Selbstschutz der Bürger. In: Zeitschrift für Rechtspolitik 1997, S. 26 ff.

Spinner, Helmut F. (1994):
Die Wissensordnung. Ein Leitkonzept für die dritte Grundordnung des Informationszeitalters. Opladen: Leske und Budrich 1994.

Spinner, Helmut F. (1997):
Wissensregime der Informationsgesellschaft - Wissen aller Arten, in jeder Menge und Güte als Gegenstand der Rechts-, Wirtschafts-, und Wissensordnung. In: Jahrbuch für Telekommunikation und Gesellschaft 1997, S.65 ff.

Ohne Verfasser (1997):
Stecker raus! Auch Zensoren surfen im Internet - mit wechselnden Erfolg. In: Neue Zürcher Zeitung v. 18.4.1997.