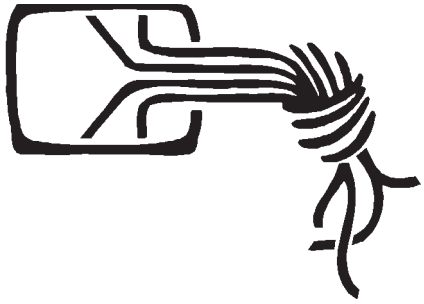
Stellungnahme des Chaos Computer Club e.V.

zu den Vorstellungen des Bundesministeriums des Innern zur Terrorismusbekämpfung



Berlin, 22. Oktober 2001

Bislang hat das Bundesinnenministerium die nach den Terroranschlägen des September 2001 ausgearbeiteten Vorschläge für Massnahmen bzw. Gesetzesänderungen und -ergänzungen nicht offiziell zur öffentlichen Diskussion gestellt. Trotzdem sind die entsprechenden Dokumente teilweise im freien Umlauf verfügbar [1].

In einem demokratischen Rechtsstaat muss jedoch auch das Gebot der Transparenz der für die Sicherheit zuständigen Behörden, der Gesetzgebers und letztlich der Regierung herrschen, damit der Bürger sich frei informieren und an der Diskussion beteiligen kann. Das Internet schafft hier eine Grundlage, die Kommunikation zwischen Staat und Bürger zu verbessern.

Die derzeitige Handlungsweise des Innenministers und seiner Behörde, im verborgenen Vorschläge und Gesetzesentwürfe auszuarbeiten, die weitreichende Einschränkungen bisheriger Grundrechte und eine starke Ausdehnung staatlicher Überwachungsmaßnahmen beinhalten, kritisieren wir daher aufs Schärfste.

Im folgenden möchten wir unseren Beitrag dazu leisten, die Diskussion um die Bekämpfung des Terrorismus zu versachlichen und die ausgearbeiteten Maßnahmen im Bezug auf ihre Zielgerichtetheit aber auch ihrer Schädlichkeit im Sinne einer auf Selbstbestimmungsrechten beruhenden Demokratie zu bewerten.

Angesichts der Fülle der vorgeschlagenen bzw. ausgearbeiteten Maßnahmen ließ es sich nicht vermeiden, sich in dieser ersten Stellungnahme zunächst auf die unmittelbar den Bereich Datenschutz, Telekommunikation und Überwachungstechnologien betreffenden Maßnahmen zu beschränken.

Ein Mehr an Überwachung bedeutet nicht mehr Sicherheit. Überwachungsmaßnahmen bringen immer auch die Frage nach der Überwachung derjenigen auf, denen Überwachungsmaßnahmen zugestanden werden. In der deutschen Geschichte gibt es genug Beispiele, wie mangelnde Kontrolle staatlicher Befugnisse letztlich demokratische Prinzipien ad absurdum führt.

- Erhebung biometrischer Merkmale in Personaldokumenten (Reisepass etc.)

Die öffentliche Aussage des Innenministers Schily, Fingerabdrücke in Personaldokumenten zur Erhöhung der Fälschungssicherheit einzuführen, vermag nicht über die praktischen Probleme und Gefährdungen einer solchen Massnahme hinwegzutäuschen.

Die erkennungsdienstliche Behandlung (aufgrund Pauschalverdächtigung) der Gesamtbevölkerung bringt nicht nur einen enormen organistorischen, technischen und somit auch finanziellen Aufwand mit sich, der von ihr hervorgebrachte Zugewinn an Sicherheit muss als fragwürdig bezeichnet werden:

- Fingerabdrücke scheiden als ein-eindeutige Merkmale ohnehin aus (nicht verwechslungssicher)

- andere biometrische Merkmale (Iris, Körper- & Gesichtsmerkmale) bringen wiederum die Frage nach dem technischen Aufwand der Erfassung und der Sicherheit gegenüber Verwechslung mit sich

- der Datenabgleich mit anderen Datenbeständen bringt - angesichts der technischen Unzulänglichkeiten biometrisch erfasster Merkmale entscheidende Probleme mit sich (Verdächtigungen aufgrund rein biometrisch erfasster Daten)

- die Speicherung von biometrischen Merkmalen im Personaldokument löst mitnichten das Problem der Verfälschbarkeit, sondern bringt es wiederum hervor. Holographische Bilder und Druckerzeugnisse sind - mit überschaubarem finanziellen Aufwand - ebenso verfälschbar und kopierbar wie sonstige Verfahren.

Entscheidendes Problem ist aber der vom Bundesinnenminister offenbar favorisierte Vorschlag der Unterbringung von "verdeckten" bzw. "verschlüsselten" Merkmalen in den Personaldokumenten. Damit wird dem BürgerInnen und Bürgern die Möglichkeit entzogen, gegen etwaige Verwechslungen bzw. falsch erhobene bzw. fälschlich zugeordnete Merkmale vorzugehen.

- Erhebung von Sprachmerkmalen bzw. Sprachaufzeichnungen von Ausländern

Der Bundesbeauftragte für den Datenschutz hat zurecht angemerkt, dass zunächst einmal die Frage der Erfassung geklärt werden muss. Wenn Asylbewerber bzw. geduldete Ausländer im Rahmen einer Befragung aufgezeichnet werden, wird ja nicht nur ihre Sprache, sondern auch der Inhalt ihrer Antworten aufgezeichnet. Dieses Problem entfällt bei einer separaten Sprachaufzeichnung ("Sprechprobe").

Durch eine solche Sprachaufzeichnung kann aber nicht nur eine Stimmanalyse zur Bestimmung des Herkunftslandes durchgeführt werden, die Erhebung von Sprachaufzeichnungen zur Identifikation (sogenannte Sonagramme) hätte weitreichende Auswirkungen.

Auch wenn technisch die Identifikation von Personen beim weitflächigen Abgleich mit Aufzeichnungen aus der Telekommunikation möglich ist, so ist die Verwertung von Sonagrammen bereits 1986 vom Bundesgerichtshof als fragwürdig bezeichnet worden. Ebenso wie bei anderen biometrischen Merkmalen muß der Beweiswert aufgrund von Verwechslungsgefahr relativiert werden.

- Speicherung der Religionszugehörigkeit von Asylbewerbern und geduldeten Ausländern

Der Vorschlag einer Speicherung der Religionszugehörigkeit zur Verwendung als Verdachtsmerkmal im Rahmen der Rasterfahndung kollidiert mit Artikel 3 Grundgesetz, das Benachteiligung auf Grund von religiöser Anschauung verbietet:

GG, Artikel 3, Absatz 3:

Niemand darf wegen seines Geschlechtes, seiner Abstammung, seiner Rasse, seiner Sprache, seiner Heimat und Herkunft, seines Glaubens, seiner religiösen oder politischen Anschauungen benachteiligt oder bevorzugt werden. Niemand darf wegen seiner Behinderung benachteiligt werden.

Die Erhebung und Speicherung der Religionszugehörigkeit und die anschließende pauschale Verdächtigung aller z.B. muslimischen Studenten bzw. Mitbürger kann also kaum als verfassungskonform bezeichnet werden.

Zur Verdeutlichung des Missbrauchspotentials hätte das Innenministerium ebenso eine Tragepflicht eines äußeren Identifikationsmerkmals (gelber Stern an der Jacke o.ä.) bei einer Erfüllung der Rasterfahndungskriterien (muslimisch, studentisch, bisher nicht vorbestraft / aufgefallen) vorschlagen können.

- Originäre Ermittlungskompetenzen des BKA im Bereich der Hochtechologie-Kriminalität

Die Auflistung von Vorschlägen zur Bekämpfung von Computerkriminalität in einem Papier des Innenministeriums zur Terrorismusbekämpfung wirft zunächst die Frage nach dem Zusammenhang auf. Gerade die Terroranschläge der letzten Wochen sind dem Bereich der "low-tech" Kriminalität zuzuordnen und haben bislang genau keinen nachgewiesenen Bezug zu modernen Kommunikationsnetzen.

Die Zentralisierung der Ermittlungen zum Bundeskriminalamt ist schon aus technischer Sicht fragwürdig, da Beweissicherung und die technische Untersuchung von Anlagen in der Regel auch Vorortermittlungen benötigt.

Ein Zusammenhang zur Terrorismusbekämpfung ist für uns nicht erkennbar. Die zu einer zentralisierten Abwicklung der Ermittlungen nötigen automatisierten Schnittstellen bringen erhebliche Mißbrauchspotentiale mit sich. Die Sicherung von Computernetzwerken geschieht nicht durch Überwachung und die Erschaffung von staatlichen Zugangsmechanismen, sondern durch eine dezentrale und spezifische Absicherung der Systeme.

- Schaffung einer Initiativ-Ermittlungskompetenz des BKA

Die Schaffung einer Initiativ-Ermittlungskompetenz für das BKA legitimiert implizit auch jedwede Überwachungsmaßnahmen des BKA. Eine breitgefächerte, verdachtsunabhängige und pauschale Überwachung von Datennetzen, Bewegungsprofilen, Zahlungsvorgängen, Grenzübertritten und anderen menschlichen Aktivitäten (durch Videoüberwachung etc.) kehrt so die Unschuldsvmermutung um und stellt quasi die Gesamtbevölkerung unter Verdacht.

Die zudem zu erwartenden Nachteile durch abweichendes Verhalten (durch Erschwernisse bei Reisen, Bank-Transaktionen, der Bewerbung um einen Arbeitsplatz etc) hätte weitreichende Folgen auf die Wahrnehmung von Grundrechten durch die Bevölkerung.

Bereits in der Begründung des Volkszählungsurteil vom Dezember 1983 leitet das Bundesverfassungsgericht aus den im Grundgesetz verankerten Grundrechten ein Recht auf informationelle Selbstbestimmung ab. Wörtlich heisst es dort (Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 - 1 BvR 209/83):

"Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermassen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

Mit dem Recht auf Informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiss. Wer unsicher ist, ob abweichende Verhaltensweisen dauerhaft gespeichert, verwendet, oder weitergegeben werden, wird versuchen nicht durch solche Verhaltensweisen aufzufallen.

Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbstimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

- Auskunftspflicht von Banken / Geldinstituten, Postdienstleistern, Luftverkehrsunternehmen gegenüber dem Verfassungsschutz zur Erforschung von Geldströmen, Postverkehr, Reisetätigkeiten

Anbetracht des zu bewertenden Verhältnisses zwischen Mittel und Zweck der vorgeschlagenen Maßnahmen ist die Unterrichtungspflicht privater Stellen über privatrechtliche Rechtsbeziehungen im Rahmen nachrichtendienstlicher Arbeit abzulehnen.

Die Ermittlungsbehörden sind bereits jetzt bei entsprechenden Ermittlungsverfahren aufgrund von dokumentierten Anfangsverdachten (teils nach Einholung eines richterlichen Beschlusses) befugt, entsprechende Unterlagen bei derartigen Unternehmen anzufordern.

Eine vollständige Offenlegung des Bank-, Brief- und Transportverkehrs gegenüber den bundesdeutschen Sicherheitsbehörden entspräche einer neuen Qualität der staatlichen Einmischung in die Beziehung der Bürger untereinander.

- Pauschale Überwachung von Telekommunikationsflüssen

Die vom BMI zur Terrorismusabwehr entworfenen Maßnahmen des

- pauschalen Zugriffs von Ermittlungsbehörden und Geheimdiensten auf Verbindungsdaten

- Einsatzes des sogenannten IMSI-Catchers GA 090 zur Ermittlung von Geräte- und Kartennummer von (GSM-) Mobiltelefonen

- Erlasses einer Mindestspeicherung für Verbindungs- und Nutzungsdaten für Telekommunikationsbetreiber

sind allesamt altbekannte Forderungen der Geheimdienste, ohne daß ein Bezug zu terroristischen Aktivitäten bzw. zur Bekämpfung des Terrorismus vorliegt.

Die aufgeführten Maßnahmen lehnen wir grundsätzlich ab, da es sich um pauschale Zugriffsrechte handelt, bei denen immer auch unbeteiligte Dritte in ihren Grundrechten beschnitten werden.

Die in diesem Zusammenhang aufgestellte Forderung nach dem

- Erlasses einer Telekommunikationsüberwachungsverordnung (TKÜV) nach § 88 TKG

ist zwar grundsätzlich verständlich, in den vorliegenden Form des Entwurfes eines TKÜV allerdings ebenfalls ein Pauschalinstrument zur Verpflichtung der Provider, staatlichen Zugriff zu ermöglichen. Die Überprüfung eines entsprechenden richterlichen Beschlusses und die der rechtsstaatlichkeit einer Maßnahme muß auch im Internet-Zeitalter gewährt sein.

[1] BMI-Sicherheitspaket zur Terrorismusbekämpfung Darstellung der gesetzlichen Maßnahmen. Datum und Quelle unbekannt, http://www.ccc.de/CRD/schilyterror1.pdf