

Vor- und Nachteile starker Kryptographie

<i>Pro- Argumente</i>
„Das Militär hat die Angewohnheit, andere zu beschuldigen, Fähigkeiten zu besitzen, die sie selbst schon im Griff haben.“ - Rosalie Bertell in „Planet Erde: Die neueste Kriegswaffe“
Datenflut heute gar nicht mehr zu bewältigen
Briefpost wird auch nicht einfach geöffnet
Steganographie ist viel wichtiger (parametrisierbar, nicht aufzuspüren)
oft technisches Unverständnis bei Kleinkriminellen
Deutschland verliert den Anschluss in kryptographischen Gebieten (deutsche Firmen können nicht mehr ihre Produkte verkaufen, Deutschland ist kein vertrauenswürdiger Investitionsstandort mehr)
Unternehmen und die Wirtschaft würden gegen Inustriespionage nicht mehr gewappnet sein
Terroristen sind selbst in der Lage sich Software zu beschaffen oder zu entwickeln zu lassen
Gedanken, die einmal gedacht worden sind, werden wieder gedacht
fast jede Erfindung des Menschen hat ihre Schattenseiten und wurde missbraucht (Pflanzenheilkunde, Chemie, Messer, Waffenproduktion, Kernspaltung, Fluchtautos)
Kriminalität wird immer einen anderen Weg finden
Kryptologie ist nicht die Ursache von Verbrechen
Verbote würden durch Terroristen nicht beachtet werden, nur der ehrliche Bürger würde entmündigt werden (Privatsphäre, Identitätsverlust, Spielball von Unternehmen), Bürgerrecht wird aberkannt
Gestellte Forderungen der Politik (Verbot von Kryptographie / Key Escrow) technisch nicht durchführbar, dienen nicht angestrebten Zielen
Gravierende Nachteile für informationelle Selbstbestimmung und Sicherheit der Bürger + Schutzinteressen der Wirtschaft
Key Escrow ist vom kosten-/ und sicherheitstechnischen Standpunkt im großen Rahmen eine absolute Katastrophe (CCC, US - Komitee) und würde Kriminalität und Missbrauch von Geheimnissen nur fördern, ob es überhaupt theoretisch möglich wäre, so etwas technisch zu implementieren, wird in Fachkreisen sehr angezweifelt
Um Geheimnisse eine lange Zeit zu schützen, müssen große Schlüssellängen genommen werden

<i>Pro- Argumente</i>
Durch die Verschlüsselung wichtiger Daten wird die kriminelle Szene behindert
Um mit dem kryptologischen Fachwissen von Verbrechern mithalten zu können, muss die Forschung in Deutschland noch verstärkt werden
Kryptographie ist die zentrale Voraussetzung für das Funktionieren der Informationsgesellschaft
Abhörmöglichkeit der Behörden wäre ein riesiges Angriffsziel für Kriminelle
Es ist fast unmöglich herauszufinden, ob und wie eine Nachricht verschlüsselt wurde (Mehrfachverschlüsselung, Kompressionen, variable Rundenanzahl)
Breite Bevölkerungsschichten sind gegen eine Regulierung
Politiker haben oft nicht das nötige Fachwissen um die Konsequenzen ihrer Forderungen zu durchschauen
Verschlüsselungstechniken sind geradezu ein Geschenk des Himmels, da es durch die Schaffung von Vertraulichkeit, Authentizität und Integrität ein wichtiges Instrument zum Schutz der Bürger darstellen, Dr. Helmut Bäumler, Datenschutzbeauftragter von Schleswig-Holstein
Nur durch die Nutzung von Kryptographie kann rechtsverbindlich über das Internet kommuniziert werden
Ein Verbot von Kryptographie wäre wettbewerbsfeindlich, da es Konsumenten die Wahlmöglichkeit nimmt und neue Innovationen verbietet
Kryptographie wahrt Berufsgeheimnisse (Journalisten, Ärzte, Rechtsanwälte, Psychologen, Steuerberater, Unternehmensberater, Geistliche ...)
Bei Verbot wäre das Ausweichen in andere Länder kein Problem
Strafandrohung nur wirksam, wenn sie höher wäre als das Delikt, was verschleiert werden soll
Verbot oder Einschränkung der Verschlüsselung ist verfassungsrechtlich verboten: Artikel 10 GG (vertrauliche, unbeobachtete Kommunikation ist unverletzlich)
Verbot würde folgende Regeln auch mit sich führen: alle Hausschlüssel bei Polizei hinterlegen, Safekombinationen und Geheimzahlen für EC Karte bei Polizei hinterlegen
Staat hat die Pflicht, die Verwirklichung der Grundrechte zu fördern (Bürger müssen in die Lage versetzt werden, sich selbst mit Kryptologie zu schützen)
Bürger ist wieder selbst in der Lage, sich vor Kriminalität zu schützen (Verschlankung des Staates)
Kostspielige Datenpolizei wäre für Deutschland nicht zu finanzieren
Andere Staaten (UK, OECD, USA) haben Verbot von Kryptographie auch bewogen, sind aber zum Entschluss gekommen, dies zu unterlassen

Pro- Argumente

Key Escrow würde zu einer nie dagewesenen Dimension von rechtlichen Eindringen in das tägliche Leben ausarten, ein Missbrauch ist vorprogrammiert

Agenten anderer Staaten sind oft im eigenen Geheimdienst, was bei nicht Verschlüsselung fatal wäre

Praxis, eigene Bevölkerung auszuhorchen war sehr weit im Ostblock verbreitet und hat nichts mit Demokratie, Rede- und Meinungsfreiheit zu tun

Terroristische Bedrohungen sind nicht so groß, dass alle Mitglieder der Gesellschaft ihre Privatsphäre aufgeben müssen

Kontraargumente

Kryptographie ist Werkzeug Terroristen um Angriffe zu planen und geheim zu halten

Staat verliert die Kontrolle über Bürger und ist der Kriminalität hoffnungslos ausgeliefert

unnötig, da vorhandene Mittel vollkommen ausreichen würden

andere Staaten könnten innerhalb des Landes Operationen planen

Verbot von Kryptierverfahren erleichtert die Strafverfolgung und schützt den ehrlichen Bürger vor Kriminalität

Die Aufbewahrung eines Nachschlüssels für alle kryptographisch abgesicherten Verbindungen für den Staat (Key Escrow) ist eine sehr gute Kompromisslösung im Vergleich zum Totalverbot

Vertrauen ist gut, Kontrolle ist besser

Abhörmöglichkeit im Verdachtsfall

„Transparenz und Ordnung“ sollen in das „chaotische“ Internet einziehen, das Netz soll bis in den letzten Winkel durchleuchtet werden

Kryptographie ist eine Domäne der Nachrichtendienste