Ingo Ruhmann / Christiane Schulzki-Haddouti

Kryptodebatten

Der Kampf um die Informationshoheit

1. Einleitung

Die Kryptopolitik dreht sich um die Frage, wer die Informationshoheit genießt: Wer kann Informationen anderer ausspähen? Wer darf seine Privatsphäre wirksam schützen? Die Kryptopolitik ist deshalb auch die Schlüsselfrage jeder Geheimdienstpolitik. Doch seitdem gute Verschlüsselungstechnologie auch Unternehmen und Bürgern preisgünstig zur Verfügung steht, ist die Kryptopolitik nicht nurmehr eine Angelegenheit der Geheimdienste, des Militärs und der Diplomaten, sondern auch der Zivilgesellschaft.

Schon vor der Zeit des römischen Feldherrn Cäsar sollten geheime Nachrichten übermittelt werden ohne dass sie von irgendjemanden mitgelesen werden konnten. Aus einfachsten Regeln, Nachrichten unleserlich zu machen, entstanden hochkomplizierte mathematische und technische Verfahren, die heute die Kryptologie – die Wissenschaft von der Ver- und Entschlüsselung, die Kryptografie – ausmachen.[1]

Kryptografie, also die Anwendung der Kryptologie, hat Kriege entschieden. Erst in den 70er-Jahren wurde bekannt, dass einer der entscheidendsten Erfolge der Alliierten im Zweiten Weltkrieg nicht auf dem Schlachtfeld erzielt wurde, sondern in einer Parklandschaft im Süden Englands. Im Kryptierzentrum »Bletchley Park« brachen polnische und britische Mathematiker mit Hilfe erster Computer den Code deutscher Verschlüsselungsgeräte (Enigma). Das Wissen um deutsche Truppenbewegungen und die Routen deutscher U-Boote sicherte das Überleben Großbritanniens als Brückenkopf der demokratischen Welt gegen die Bedrohung durch Deutschland.[2]

Auch nach dem Zweiten Weltkrieg sicherte den Briten das Know-How um Verschlüsselungsgeräte derselben Bauweise wie die Enigma der deutschen Wehrmacht zusätzliche Erfolge. Im Frühjahr 1956 spionierte der britische Inlandsgeheimdienst MI5 die ägyptische Botschaft in London aus, um während der Suez-Krise den verschlüsselten diplomatischen Funkverkehr zwischen London und Kairo mitlesen zu können.[3] Solche Neugier machte auch vor Freunden nicht Halt. In den Jahren 1960 bis 1963 entzifferte der MI5 den streng geheimen Funkverkehr zwischen der französischen Botschaft in Lon-

don und der Pariser Zentrale und las mit, wie sich Frankreich zur Aufnahme Großbritanniens in die Europäische Gemeinschaft stellen würde.[4]

Erst dreißig Jahre nach den Ereignissen des Zweiten Weltkrieges wurde nach und nach bekannt, was diese und ähnliche Erfolge der Entschlüsselung ausmachten. Dennoch hatten die Deutschen sich nach dem Zweiten Weltkrieg gegen einen weiteren Einsatz der Enigma entschieden. Die Briten ihrerseits übergaben Tausende erbeutete Enigmas ihren Partnern in den Commonwealth-Staaten.[5] Kryptografie – das lehrt die Geschichte – lebt nicht allein von überragenden technischen Kompetenzen oder den Spionagefähigkeiten der Beteiligten, sondern auch davon, andere möglichst lange unwissend über die eigenen Kompetenzen zu lassen, um aus den eigenen Entwicklungen den größten Nutzen zu ziehen.

Verschlüsselung kann die Arbeit der Geheimdienste deutlich erschweren. Deren Interesse besteht naturgemäß darin, den Umfang gut verschlüsselter Nachrichten so gering wie möglich zu halten, um ihre Informationsquellen nicht versiegen zu lassen. Kryptografie lebt vom Wissen, das wenige haben und anderen vorenthalten wird.

Wo der Einsatz der Verschlüsselung nicht zu verhindern ist, können Kenntnisse um die angebotene Technologie weiter helfen. Die Zeit ist vorüber, in der Kenntnisse über die Bauart von Verschlüsselungsmaschinen eine Entschlüsselung erlaubten. Heute sind die Geräte computergesteuert, doch wenige Produzenten sind in der Lage, leistungsfähige Kryptosysteme zu entwickeln. Die Produktion und Lizenzierung von Verschlüsselungsgeräten kommt daher einer »strategischen Kontrolle durch den Lizenzgeber gleich. Dasselbe gilt um so mehr für Software, eine immer mehr genutzte, aber weit weniger greifbare Komponente vieler moderner Systeme . . . Das Gleiche ist besonders stichhaltig für Verschlüsselungssysteme. Diese werden in wachsender Zahl in militärischer Kommunikationsausrüstung als eingebaute, als Ein- oder Aufsteckmodule angewandt und einige Systeme wurden nur nach Übersee verkauft unter der expliziten Vereinbarung der Regierung des Verkäuferlands, dass alle Codes, wenn nötig, durch die eigenen Sicherheitsdienste oder Militärs ›geknackt‹ werden können«.[6]

Groß war daher das Unbehagen der staatlichen Kryptologen, als sich in den 70er-Jahren ein ziviler Zweig der Kryptografie entwickelte. Ursache dieser Entwicklung waren immer leistungsfähigere Computer, die neue mathematische Verfahren in der Praxis möglich machten. Die schon zu dieser Zeit weltweite Computerkommunikation machte verschlüsselte Übertragungen dort notwendig, wo es beispielsweise um den Transfer von Geld zwischen Banken ging. Das Ergebnis waren neue mathematische Ansätze zur effektiven Verschlüsselung von Daten. Aus der militärischen Forschung kamen zusätzliche Impulse, die von dem Interesse getrieben waren, das Kernproblem der Verschlüsselung in den Griff zu bekommen: Die Verteilung und Verwaltung der geheimen Schlüssel, mit denen verschlüsselte Nachrichten durch die berechtigten Partner wieder entschlüsselt werden können. Je mehr Nachrich-

ten in der Zeit des Kalten Krieges verschlüsselt wurden, desto unbeherrschbarer wurde diese Aufgabe.

Die Antwort entstand wiederum in Großbritannien. Der Kryptologe James Ellis publizierte 1970 ein Papier, das den mathematischen Beweis für die Existenz eines Prozesses lieferte, in dem ein Schlüssel aus einem geheimen und einem öffentlichen Teil aufgebaut sein kann. Der öffentliche Teil liefert mit Hilfe einer mathematischen Funktion einen verschlüsselten Code, der nur von demjenigen zu lesen ist, der den geheimen Schlüssel besitzt. Jeder kann danach jedem Partner seinen öffentlichen – und für die Entschlüsselung wertlosen – Schlüssel geben, aber nur er selbst kann den erzeugten Code entschlüsseln.[7] Der Beweis für die Existenz der heute so genannten »Public Key-Verschlüsselung« war gefunden, die Idee musste nur in die Praxis umgesetzt werden.

In der geheimen britischen Chiffrierstelle, in der Ellis arbeitete, fand der Mathematiker Clifford Cocks 1973 eine Lösung.[8] Die beiden Papiere von Ellis und Cocks blieben jedoch bis 1997 geheim. Ohne Kenntnis davon gaben die zivilen Kryptologen Whitfield Diffie und Martin Hellman 1976 in ihrem bahnbrechenden Papier »New Directions in Cryptografy« eine den britischen Ideen entsprechende Methode an, die den Beginn der zivilen Karriere der Verschlüsselung markierte.[9] Zu einem für jeden programmierbaren Algorithmus wurde das Verfahren durch die drei Mathematiker Ronald Rivest, Adi Shamir und Leonard Adelman, die eine einfache Methode zur Generierung der notwendigen Bausteine entwickelten und deren Initialen heute in der Bezeichnung des RSA-Algorithmus an seine Urheber erinnert. RSA ist die Grundlage der heute weit verbreiteten zivilen Kryptosysteme.

2. Die Geburt ziviler Kryptografie

Die Arbeiten von Diffie und Hellmann waren ein Beleg dafür, dass Kryptografie nicht länger eine Domäne von Militärs und Geheimdiensten war, sondern auch in der zivilen Wissenschaft erforscht und in der Wirtschaft eingesetzt wurde. Finanziert wurde diese Forschung in den USA auch von der nationalen Forschungsstiftung der USA, der »National Science Foundation« (NSF). Am 20. April 1977 besuchten zwei Angestellte des Abhör- und Kryptier-Geheimdienstes »National Security Agency« (NSA) die NSF-Abteilung für Mathematik und Informatik.

Die NSA ist einer der geheimsten Nachrichtendienste der USA, der so geheim war, dass seine bloße Existenz jahrelang bestritten wurde. Die Aufgaben der NSA liegen im Sammeln von Informationen, der Entschlüsselung von militärischen, diplomatischen wie privaten Nachrichten aus dem Ausland, sowie der Verschlüsselung der gesamten Kommunikation der US-Regierung. Unterstellt ist der Dienst dem US-Verteidigungsminister.[10]

Der damalige Direktor der NSA, Admiral Bobby Inman, sah nach eigenen Worten große Gefahren für seine Spionagearbeit: »Aus der Perspektive der NSA betrachtet, liegt die Crux des Problems darin, dass ein Wachsen der Besorgnis über den Schutz von Telekommunikation im nicht-staatlichen Sektor ein Anwachsen der Diskussion und des Wissensstandes über den Schutz von Kommunikationssystemen in der Öffentlichkeit impliziert. Die wichtigste dieser Techniken ist natürlich die Kryptografie. Dabei existiert die sehr reale und kritische Gefahr, dass eine unbegrenzte öffentliche Diskussion kryptologischer Themen die Fähigkeiten der Regierung, Signalspionage zu betreiben und die Fähigkeit, Informationen zur nationalen Sicherheit vor fremdem Missbrauch zu schützen, ernsthaft schädigt«.[11]

Weil die Fähigkeiten der NSA zur Spionage und Überwachung der Kommunikation sehr erschwert würden, »versuchte die Regierung, Studien in der Kryptologie zu unterdrücken«,[12] stellte der Kryptologe David Kahn fest. Die beiden NSA-Agenten besuchten also die NSF, um bei der Forschungsstiftung einen größeren Einfluss auf die Vergabe von Arbeiten im Bereich der Kryptologie zu erreichen. Die NSA forderte die NSF auf, alle Arbeiten auf dem Gebiet der Kryptologie für a priori »geheim« oder »born classified« zu erklären.[13] Alle »born classified«-Forschungsarbeiten sind nämlich geheim und dürfen erst veröffentlicht werden, wenn eine staatliche Stelle die Freigabe gestattet hat. Vorbild dafür waren Bereiche der Atomphysik, in denen es um das Wissen um den Bau von Kernwaffen geht. Nach dem Wunsch der NSA sollte dasselbe nun auch für die zivile Kryptologie gelten, damit Wissen um effektive Verschlüsselung nicht unkontrolliert an die Öffentlichkeit käme.

Admiral Bobby Inman bestritt zwar, dass die NSA »unzulässigen Einfluss« auf die NSF ausüben wollte,[14] war aber allenfalls zu dem Kompromiss bereit, die Maximalforderung des »born classified« durch eine generelle Kontrolle der zivilen wissenschaftlichen Publikationen zu ersetzen.[15] Die wichtigen Wissenschaftsorganisationen wollten dieser Kontrolle von Wissenschaft durch Geheimdienste nicht nachgeben. Sie sahen darin den Versuch, ein ganzes Forschungsgebiet staatlicher Kontrolle zu unterwerfen und zivile Wissenschaft zu steuern.

Auch die Verwertung von Forschungsergebnissen wurde erschwert. 1978 wurden Patente von Entwicklungen der zivilen Forscher George Davida und David Wells zu einem Langcode und einer Gruppe um Carl Nicolai zu einem preisgünstigen Gerät zur Verschlüsselung von Sprachübermittlungen mit einer so genannten »Secrecy Order« versehen. Dadurch wurde jede Veröffentlichung über die zum Patent angemeldeten Forschungsergebnisse untersagt. Über beide Fälle wurde in den Medien breit berichtet. Beide Anordnungen mussten zurückgezogen werden, da sie nicht den Rechtsgrundlagen des Verfahrens entsprachen,[16] die nur dann eine »Secrecy Order« möglich machten, wenn vor der Anmeldung zum Patent keine Veröffentlichungen zu dieser Arbeit erschienen waren.

Gleichzeitig musste die zivile Forschung Federn lassen: Einer mit Mitteln der NSF geförderten Forschungsarbeit von Leonard Adelman – einem der »Väter« des RSA-Algorithmus – wurde im August 1980 die Finanzierung von Forschungsbereichen, die sich mit kryptografischen Themen befassten, entzogen, weil durch diese Forschungsarbeiten die nationale Sicherheit gefährdet sei.[17]

Eine Diskussion um die Kontrolle ziviler Wissenschaft durch Geheimdienste fand im Frühjahr 1980 in der »Public Cryptografy Study Group« (PCSG) statt. Das Gremium setzte sich aus Militärs und Wissenschaftlern zusammen, nur einer der Beteiligten war jedoch ziviler Wissenschaftler. Das Ergebnis war der Vorschlag einer »freiwilligen« Kontrolle wissenschaftlicher Arbeiten durch den Geheimdienst NSA. Betroffen war aber nicht allein die Kryptologie. Nach den Wünschen der NSA in der Study Group sollten die Restriktionen gelten für: »Papiere in Mathematik, Ingenieurwissenschaften, Informatik, Statistik, Physik oder theoretische Forschung, die [...] angewandt werden kann auf Entwicklung, Design, Produktion oder Analyse von früheren, gegenwärtigen oder zukünftigen kryptologischen Systemen oder Programmen«.[18]

Damit waren die Grenzen nun so weit gefasst, dass fast jedes Gebiet der Informatik unter diese Regelung hätte fallen können. Entsprechend wuchs der Widerstand in der Informatik und in der Wirtschaft.

Einfacher hatte es die NSA 1979 dagegen damit, die Kryptologie als Wissenschaft und Technologie auf der Liste der »kritischen Technologien« bei der Neuregelung der Exportgesetzgebung, dem erstmals im Jahr 1949 erlassenen Exportkontrollgesetz (Export Control Act), unterzubringen.[19] Nach diesem Gesetz und seinen Nachfolgern, dem Export-Verwaltungsgesetz der USA, dem »Export Administration Act«, wird auch heute noch jedes Jahr eine Liste militärisch interessanter Technologiegüter zusammengestellt, die nicht aus den USA exportiert werden dürfen. Alle nicht exportierbaren Güter werden in einer Liste – der »International Traffic in Arms Regulation« (ITAR), also der »Regelung zum internationalen Waffenhandel« – zusammengefasst. 1979 wurde auch zum ersten Mal Computersoftware als expliziter Punkt im »Export Administration Act« aufgelistet. Verschlüsselungssoftware durfte danach für viele Jahre nicht aus den USA exportiert werden. Erst im Jahr 2001 wurde der »Export Administration Act« novelliert.[20]

Neu auf die ITAR-Liste kam 1979 auch die Weitergabe von Wissen über Chiffriersysteme. Ziel war das Verbot des Exports von wissenschaftlichem Know-How. Deswegen wurde untersagt, »jegliche nicht geheime Information«, die im Zusammenhang mit den aufgelisteten Kriegsgütern (also der Kryptologie) Verwendung finden könnte, zu exportieren. Ein Export lag bereits dann vor, wenn diese Informationen »Angehörigen einer fremden Nation zur Kenntnis gelangen (einschließlich Betriebsbesichtigungen und Teilnahme an Briefings und Symposien)«. Auch sei vor einer Veröffentlichung in einer Zeitschrift mit ausländischen Abonnenten eine staatliche Genehmigung einzuholen.[21]

Eine der zahlreichen Folgen war, dass das US-Verteidigungsministerium dafür sorgte, dass im August 1982 bei einer Konferenz zu optischen Instrumenten in San Diego über 150 nicht geheime Papiere von Referenten dieser Konferenz zurückgehalten wurden.[22] Die Regelungen hatten aber auch Konsequenzen für die Wissenschaft in Deutschland. Die Universität Dortmund bestellte Anfang der 80er-Jahre eine neue Version ihres Betriebssystems Unix. Da Dortmund schon seit längerem eine Lizenz für Unix hatte und die Auftragsbestätigung von AT&T kurze Zeit später per Telex in Dortmund ankam, deutete zunächst nichts auf mögliche Probleme hin. Am 15. 11. 1983 teilte AT&T jedoch mit: »Das US-Department of Commerce verhängte ein temporäres Embargo über die gesamte UNIX-Software, so dass es unglücklicherweise zu einer Verzögerung kommen wird«. [23]

Ähnliche Probleme hatten Forscher auf dem Gebiet der »Künstlichen Intelligenz«, wenn sie aus den USA neue Versionen ihrer Programmiersprachen, und Designer von Computerchips, wenn sie die Konstruktionssoftware aus den USA beziehen wollten. Mit der Ausweitung der Exportregelungen, vor allem aber der Publikationskontrolle auf die Informatik als Ganzes hatte die NSA jedoch deutlich überzogen. Statt sich auf das noch junge Gebiet der Kryptologie zu beschränken, brachte die NSA weite Teile der Informatik gegen sich auf, die den US-Kongress mobilisierten und eine Verfassungsklage zum Schutz der Freiheit von Wissenschaft und Forschung vorbereiteten. Erst durch diesen massiven politischen Gegendruck zog sich die NSA bis Mitte der 80er-Jahre davon zurück, wissenschaftliche Arbeiten einer Kontrolle zu unterwerfen und die Freiheit von Forschung und Wissenschaft auf dem Gebiet der Informatik einzuschränken. 1985 wurde denn auch das letzte ausschließlich militärisch genutzte Verschlüsselungsgerät, die elektro-mechanische KL-7, nach dem Auffliegen des Walker-Family-Spionagerings aus dem Verkehr gezogen, da die Sowjets damit definitiv über eine KL7-Maschine samt Schlüsselmaterial verfügten.[24] In den 80er- und 90er-Jahren drehte sich mit dem Siegeszug der IT-unterstützten Verfahren der Wind endgültig zugunsten der Zivilgesellschaft. Die wichtigste Rolle spielte hierbei anfangs ein Friedensaktivist, der ein kleines Softwareprogramm entwickelt hatte.

3. PGP

PGP ist heute das verbreitetste Verschlüsselungsprogramm im Netz. Jeder halbwegs aufgeklärte Netznutzer hat es auf seinem PC installiert. PGP gibt es für fast alle Rechner-Plattformen, es ist für die private Nutzung kostenlos. Die Verschlüsselungssoftware ist Kult und gilt seit Jahren als De-Facto-Standard für sichere Kommunikation im Internet. Sie war es schließlich auch, die das US-Kryptoexportverbot zu durchbrechen half: Ihr Code wurde per Buch exportiert – und in Europa wieder mühsam eingescannt. Denn der Buchexport war zu diesem Zeitpunkt nicht verboten.

Entwickelt wurde PGP vom Programmierer und ehemaligen Friedensaktivisten Phil Zimmermann.[25] Auslöser war im Januar 1991 ein Zeitungsbericht in der »New York Times«, der den Vorschlag für ein Anti-Terrorgesetz vorstellte. Er sah damals vor, dass alle Anbieter von sicheren Kommunikationsdiensten Hintertüren für die US-Regierung einbauen sollten. Darauf schrieb Zimmermann ein kleines Programm, das E-Mail und Dateien mit dem Public-Key-Verfahren verschlüsselte und nannte es »Pretty Good Privacy«, was man mit »ziemlich gute Privatsphäre« übersetzen kann.

Die ersten Nutzer waren denn auch nicht Kriminelle, sondern Bürgerrechtler. Als es während des Bosnienkriegs zu Verhaftungen kam, wollten die staatlichen Behörden die Herausgabe des PGP-Passphrase erzwingen. Auf dem Computer lagen die Daten von Dissidenten, die im Falle der Entschlüsselung um ihr Leben hätten fürchten müssen.[26] Zimmermann erhält noch heute Dankesbriefe aus Osteuropa, Mittelamerika und Burma.

Von PGP gibt es inzwischen viele Versionen. Kritische Experten empfehlen die spartanische Version von PGP 2.6. Das ist die letzte Version, bevor Phil Zimmermann seine Firma PGP Inc. 1997 an den Sicherheitskonzern Network Associates (NAI) verkaufte. Bei ihr kann man davon ausgehen, dass keine Hintertüren eingebaut sind. Sie ist im Netz zusammen mit einer grafischen Oberfläche wie dem Programm MailPGP (für Windows 95, 98, NT) kostenlos erhältlich.[27] Bequem benutzen lässt sie sich beispielsweise mit dem Mail-Programm »The Bat«, wo sie direkt eingebunden ist oder auch mit dem Mail-Programm Crosspoint. Zu den jüngeren Versionen ist die PGP-Version 2.6 allerdings nur eingeschränkt kompatibel – was viele Nutzer abschreckt.

Noch immer soll es Polizei und Nachrichtendiensten nicht möglich sein, PGP-verschlüsselte E-Mails zu dechiffrieren – vorausgesetzt der Nutzer wendet es sauber an. Der Angriff auf das Endgerät kann allerdings zum Erfolg führen, denn auf der Festplatte des PC befindet sich der geheime Schlüssel. Die Fahnder müssen deshalb nur noch das geheime Passwort herausfinden. Das ist mit Hilfe des »Großen Lauschangriffs« theoretisch kein Problem – Tastaturwanzen können die Eingaben in die Tastatur protokollieren.[28]

Zehn Millionen Internetnutzer sollen das Programm installiert haben. Es wäre jedoch ein Irrtum davon auszugehen, dass es ebenso häufig genutzt wird. Phil Zimmermann: »Wenn man sich die Internetbevölkerung als Tortengrafik vorstellt, dann nutzt nur ein kleiner Teil davon Verschlüsselung. Die Menschen in diesem kleinen Tortenstück sind aber fast alle Nutzer von PGP«. Wann der Einsatz von PGP sinnvoll ist, lässt sich mit einer einfachen Daumenregel beurteilen: Alles, was Nutzer lieber nicht per Postkarte mitteilen, sondern im Umschlag verschicken möchten, sollten sie im Internet verschlüsseln. Denn die E-Mail läuft über viele Rechner, bevor sie beim Computer des Empfängers ankommt. Auf jedem dieser Rechner kann die Nachricht gelesen und auch verändert werden, ohne dass der Absender oder der Empfänger es merken.

4. Bollwerk Deutschland

Die Exportbeschränkungen für Verschlüsselungs-Know-How überlebten sogar den Kalten Krieg und wurden erst im Januar 2000 nach langen, harten Auseinandersetzungen gelockert. Die Schlüsselfigur der politischen Debatte war David Aaron. Der ehemalige US-Sonderbotschafter in Sachen Kryptopolitik verabschiedete sich wenige Wochen nach der Liberalisierung aus dem Staatsdienst, um im Auftrag der Anwaltskanzlei Dorsey & Whitney für US-Firmen im Ausland »Troubleshooting« zu betreiben. Mit Aaron war der letzte große Kryptohardliner von der Bühne gegangen.

Aaron hatte in den 90er-Jahren hartnäckig versucht, andere Staaten von der Key-Recovery-Politik zu überzeugen. Er führte für die USA die OECD-Verhandlungen, konnte sich jedoch trotz massiven Drucks bei wichtigen europäischen Partnern wie Deutschland nicht durchsetzen. Dennoch wurde er im Juni 1997 auf seinen Posten berufen. Im November 1997 übernahm er dann die Leitung der »International Trade Administration« (ITA), die mit 2000 Angestellten dem US-Handelsministerium untersteht. Sie ist zuständig für internationale Handelsabkommen und Exportkontrolle und gilt als Eiserne Faust der US-Handelspolitik. Hier war Aaron auch für die Exportkontrolle von kryptografischen Systemen verantwortlich.

Allen damals Beteiligten ist sein Auftritt vor dem Deutschen Industrie- und Handelstag im Oktober 1998 noch heute in bester Erinnerung, als er in einer emphatisch-aggressiven Rede »die Wahrheit über die US-Kryptopolitik« enthüllte.[29] Zuvor hatten die Deutschen den Amerikanern unterstellt, mit Hilfe von »Key Recovery« auch Zugriff auf ausländische Systeme erlangen zu wollen. Der schwelende Dissens zwischen Deutschland und den USA in der Kryptofrage hatte sich zu einem kleinen Feuer entfacht: Nachdem sich im Sommer die Enquêtekommission des Deutschen Bundestags »Neue Medien« gegen eine Adaption der US-Kryptopolitik, insbesondere ihres Konzepts der »Key Recovery Agents«, als einer Bedrohung von nationaler Souveränität und Sicherheit ausgesprochen hatte, sorgte Mitte September der damalige deutsche Wirtschaftsminister Günther Rexrodt mit einer Rede für Aufruhr, in der er die US-Politik als »inakzeptabel« bezeichnete.[30]

Deutschland spielte in den Augen der USA das »Bollwerk in Europa«, so damals EPIC-Sprecher Marc Rotenberg.[31] Würden die Deutschen kippen, würden auch andere liberale Länder wie Kanada folgen. Der Zeitpunkt für Aarons Besuch war geschickt gewählt: Die Entscheidung über eine Kryptoregulierung in Deutschland hatte die alte konservativ-liberale Regierung per Kabinettsbeschluss bis zum Ende der Legislaturperiode verschoben. Die von der FDP geführten Ministerien hatten zuletzt eine Regulierung blockiert. Unter Rot-Grün wurden unter dem Vorzeichen internationaler Zusammenarbeit in der Strafverfolgung die Karten neu gemischt.

Die Bundesregierung sah die US-Richtlinien für Krypto-Produkte in einer Linie mit der US-Exportpolitik. Demnach durften bestimmte Verschlüsse-

lungsprodukte nur dann ins Ausland exportiert werden, wenn amerikanische Sicherheitsbehörden mit Hilfe der so genannten »Key Recovery Agents« innerhalb von zwei Stunden auf den Klartext der chiffrierten Daten zugreifen konnten. Die Entwicklung eines Standards für »Key Recovery«-Produkte durch die »Key Recovery Alliance« sollte zusammen mit einer restriktiven Exportpolitik für Nicht-Recovery-Produkte die Verschlüsselungssysteme mit Schlüsselhinterlegungsfunktion qua Marktmacht weltweit durchsetzen. Doch die Allianz, der ursprünglich um die 60 internationale Unternehmen angehörten, bröckelte: Zuerst verabschiedete sich der deutsche Konzern Siemens, dann folgte das französische Unternehmen Bull.

Die klare Haltung Deutschlands drohte weltweit einen Flächenbrand auszulösen. David Aaron musste daher in die Offensive gehen: Er kündigte an, nichts als die Wahrheit, die ganze »Wahrheit über die US-Kryptopolitik« zu enthüllen.[32] Aaron versuchte zu vermitteln, dass künftig die Möglichkeiten polizeilicher Überwachung gefährdet würden, wenn der Klartext nicht entschlüsselt werden könne. Er warnte auch vor Attentaten, die möglicherweise nicht rechtzeitig entdeckt werden könnten. Auch werde die deutsch-amerikanische Freundschaft belastet, ein Handelsdisput möglich. Der Kern seiner Rede bezog sich jedoch auf den Vorwurf der Wirtschaftsspionage durch die Hintertür, der durch das »Key Recovery Agent«-Konzept aufgekommen war. Diesen konnte Aaron dadurch entkräften, dass er die jüngsten Kursänderungen in der US-Politik vorstellte. Das Weiße Haus hatte kurz vor seiner Deutschlandreise 56-Bit-Produkte nach einer einmaligen Überprüfung von den Exportkontrollen befreit. Die Firmen mussten auch keine Pläne für die spätere Implementation von Key-Recovery-Funktionen vorlegen.[33]

Für Experten war dies allerdings nicht sehr beeindruckend. Denn mit 56-Bit-Produkten verschlüsselte Daten konnten schon seit längerem mühelos geknackt werden. Wichtig war allerdings, auf die Regelungen im Bereich der »Key Recovery Agents« komplett zu verzichten. Damit hatte Aaron den Argumenten der Bundesregierung den Teppich unter den Füßen weggezogen. Denn gerade diese Frage hatte hierzulande für eine einheitliche Frontlinie gesorgt. Selbst das zurückhaltende Bundesinnenministerium hatte grünes Licht gegeben: Eine Key-Recovery-Politik nach US-Vorstellungen sei als Gefährdung der nationalen Sicherheit zu verstehen.

5. Wassenaar

Die internationale Front gegen die US-Kryptopolitik drohte jedoch bereits bei den Wassenaar-Verhandlungen zu bröckeln. Im November 1998 trafen sich die 33 Wassenaar-Mitgliedstaaten, darunter auch die USA und Deutschland, in Wien zu Verhandlungen.[34] Das Wassenaar-Abkommen, ein Nachfolger des Exportkontrollabkommens COCOM, wurde im Juli 1996 unterschrieben. In regelmäßigen Abständen unterrichten sich die Unterzeichnerstaaten über ab-

gelehnte Exportanträge, um zu verhindern, dass eine Ausfuhr über ein anderes Land genehmigt wird. Auf der Liste des Abkommens werden neben Rüstungsgütern auch Kryptoprodukte als zivil und militärisch nutzbare, also Dual-Use-Produkte geführt, die eine Exportgenehmigung benötigen. Eine Ausnahme gab es damals: Software, die »öffentlich frei verfügbar« und für »den Massenmarkt bestimmt« ist.[35] Für die USA war dies eine Chance, auf einem unpolitischen Weg ihre Verschlüsselungsprodukte mit der Hintertür doch noch auf den Weltmarkt zu bringen. Das Wassenaar-Abkommen stellt allerdings lediglich eine Mindestharmonisierung der Güter und Technologien dar, die überhaupt von einer Exportkontrolle erfasst werden – jeder Staat kann das dabei angewandte Verfahren aber frei gestalten. Die Entscheidung, ob und unter welchen Bedingungen ein Produkt exportiert werden darf, liegt einzig in der jeweiligen nationalen Verantwortung der Unterzeichnerstaaten.

Im Ergebnis werden seit 1998 Hardware- und Softwareprodukte gleich behandelt. Alle Exportkontrollen für Krypto-Produkte mit weniger als 56-Bit-Schlüssellänge entfielen. Im Gegenzug wurde die Exportkontrolle auch auf starke Kryptografie »über 64 Bit« erweitert, die für den Massenmarkt bestimmt ist. Die so genannte Ladentisch-Software, also Programme für den Massenmarkt, oder »allgemein zugängliche« Software (Public Domain), sind generell von den Kontrolllisten freigestellt. Hierunter versteht das Wassenaar-Abkommen Software, die »ohne Einschränkungen bezüglich ihrer weiteren Verbreitung« verfügbar gemacht wurde. Ausgenommen von der Exportkontrolle wurden zudem Verfahren zur Digitalen Signatur und Authentifizierung für Banking, Pay-TV und Copyright-Schutz sowie schnurlose Telefone und Handys, die keine Verschlüsselung zwischen den Endstellen erlauben.[36]

US-Sonderbotschafter David Aaron begrüßte damals den Beschluss der Wassenaar-Mitgliedstaaten noch als »Bekräftigung« der US-Krypto-Politik, obwohl sich die USA mit ihrem Plan, Key-Recovery-Systeme zu begünstigen, nicht durchsetzen konnten.[37] Tatsächlich war dies jedoch eine entscheidende Niederlage für die US-Kryptopolitik. Die Beschränkung galt zunächst für zwei Jahre und wurde 2000 verlängert. Ende 2002 stehen erneut Verhandlungen an, wobei die Amerikaner hier unter dem Vorzeichen der Terrorismusbekämpfung die Zügel wieder etwas enger anziehen wollen. Das erste Vorzeichen war im März 2002 der Vorschlag des US-Verteidigungsministeriums, ausländische Experten aus Verteidigungsprojekten künftig auszuschließen.[38]

6. Liberalisierung

Generell geht es in der internationalen US-Kryptopolitik seit Wassenaar nicht mehr um »Key Recovery« (Schlüsselwiederherstellung), »Key Escrow« (Schlüsselhinterlegung) oder sonstige Schlüsselmanagementsysteme, sondern nur noch um eine beliebige Möglichkeit, den Klartext chiffrierter Nachrich-

ten wiederherzustellen. In den USA verfolgte die US-Regierung noch am »National Institute of Standards and Technology« (NIST) einige technische Pilotprojekte, die letztlich zeigten, dass eine staatliche Schlüsselhinterlegung nicht realisierbar war. Eine politische Kurskorrektur war daher nur noch eine Frage der Zeit. Mit den weitreichenden Lockerungen der Exportpolitik gaben die USA schließlich dem weltweiten Liberalisierungstrend nach, in dem vor allem Deutschland den Vorreiter gespielt hatte.

Ein weiterer wichtiger Schritt hin zu einer Liberalisierung war die Haltung der Europäischen Union, die vor allem von den Positionen Deutschlands und Frankreichs geprägt wurde. Wenige Monate nach Wassenaar beschloss die Europäische Union, jegliche Exportbeschränkungen innerhalb der Union aufzuheben.[39] Einzelheiten des Exportverfahrens werden in der deutschen Außenwirtschaftsverordnung festgelegt, die für Verschlüsselungsprodukte Anträge auf Individual-Ausfuhrgenehmigung beim Bundesausfuhramt (BAFA) vorschreibt. In der Mehrheit werden solche Anträge mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) abgestimmt. Verwendungszweck, Endempfänger und Empfängerland sind von entscheidender Bedeutung. In der Praxis wurden Einzelgenehmigungen für zivil nutzbare Krypto-Produkte nur in wenigen Ausnahmefällen abgelehnt. Im Zweifel konnten die Hersteller einen »Nullbescheid« beantragen, der bestätigte, dass für ein bestimmtes Ausfuhrvorhaben keine Exportgenehmigung erforderlich ist.

Weitere Schritte in Deutschland besiegelten den liberalen Kurs. Das Regierungskabinett beschloss am 2. Juni 1999 die liberalen Kryptoeckwerte.[40] Im November schließlich machte das Bundeswirtschaftsministerium Nägel mit Köpfen und gab die öffentliche Förderung des »Gnu Privacy Guard« (GnuPG)[41], der Open-Source-Variante von »Pretty Good Privacy«, den Segen.[42] Diese Meldung schaffte es sogar in die US-Presse, woraus deutlich wird, welche Signalwirkung ihr zugemessen wurde. Denn mit der öffentlichen Förderung war klar, dass Verbreitung und Entwicklung der so lange bekämpften Software nicht mehr zu kontrollieren war – weder per Exportrestriktionen, noch durch die Entwicklungskontrolle bei der US-Firma Network Associates, die das Programm von Entwickler Phil Zimmermann gekauft hatte. Die Open-Source-Variante würde sich nicht kompromittieren lassen.

PGP wurde seit der Version 2.5 nicht mehr unter der GNU-General-Public-License vertrieben. Im Mai 1996 gründete Philip Zimmermann mit anderen für die Weiterentwicklung von PGP die Firma PGP Inc. Das erste von dieser Firma veröffentlichte Programm war die Windows-Version von PGP 5.0. Damit hatten die freien Entwickler jedoch ein großes Problem: Die Lizenzbestimmungen der Freeware-Version gestatteten zwar explizit den Vertrieb des Programm-Quelltextes und auch die Modifizierung für den eigenen Gebrauch. Aber weder durften die geänderten Quelltexte noch die Änderungen selbst veröffentlicht werden. Nach dem Verkauf von PGP Inc. an Network Associates befürchteten Experten, dass sich die Situation auf Druck der US-Regierung verschärfen würde. So wäre es möglich gewesen, auch die Einsicht

in den Quelltext selbst zu verhindern. Angesichts dessen, dass PGP zu diesem Zeitpunkt längst Standard war, hätte dies ein erhebliches Sicherheitsproblem bedeutet: Denn warum soll man einer Software vertrauen, die man nicht mehr überprüfen kann? Tatsächlich haben sich die Befürchtungen von damals inzwischen bewahrheitet: Phil Zimmermann hat Network Associates verlassen. Der Hauptgrund waren wohl die zunehmenden Streitereien um die Offenlegung des PGP-Quellcodes. Die letzte Version 7 weigerte sich das neue Management von Network Associates offen zu legen. Zimmermann war der letzte Garant dafür, dass es in PGP keine Hintertüren geben würde. Inzwischen hat die Firma gar die Weiterentwicklung eingestellt, angeblich lohne sich das Geschäft nicht mehr.

Schon 1997 hatte jedoch Phil Zimmermann die PGP-Spezifikationen frei gegeben. Im internationalen Standardisierungsgremium der »Internet Engineering Task Force« (IETF) erarbeitete eine Arbeitsgruppe die Spezifikationen für einen offenen Verschlüsselungsstandard, den OpenPGP-Standard. Im November 1998 wurde er als IETF-Standard vorgeschlagen. Mit finanzieller Unterstützung des Bundeswirtschaftsministeriums wurden seither einige Programme entwickelt, um das ursprünglich nur für Unix-Nutzer entwickelte GnuPG auch Anwendern von Windows-Betriebssytemen zur Verfügung zu stellen.[43] Der freie Entwickler Werner Koch hätte nämlich von sich aus die Windows-Varianten nicht entwickelt. Erst seit dem Frühjahr 2001 sind GnuPG-Werkzeuge fertig: Sylpheed ist ein grafisches E-Mail-Programm für unterschiedliche Betriebssysteme[44], das mit GnuPG direkt zusammenarbeitet. Damit ist es möglich, E-Mail direkt im Mail-Programm zu verschlüsseln beziehungsweise verschlüsselte Mail zu öffnen und zu lesen. Der Nachteil ist dabei, dass man auf ein neues E-Mail-Programm umsteigen muss. Falls man davor zurückschreckt, kann man WinPT benutzen. Es ist ein Taskleistenwerkzeug, mit dem man über die Zwischenablage[45] Mail ver- und entschlüsseln kann. WinPT ist eine grafische Benutzeroberfläche für GnuPG. Noch bequemer verschlüsselt GnuPG über GEAM[46]. Der Nutzer verschlüsselt und entschlüsselt automatisch über den GEAM-Server, der in das Firmennetzwerk eingebunden ist. Der Server läuft unter Linux sowie verschiedenen Unix-Varianten und kann in jede Netzwerkinfrastuktur integriert werden.[47] Vor allem die Datenschützer wollen GnuPG aktiv fördern und auch die Bundesbehörden wie das Bundesinnenministerium denken über den Einsatz der kostenlosen Software nach.

7. Kryptopolitik als Sicherheitspolitik

Die Beziehungen zwischen Deutschland und den USA haben sich im Sicherheitsbereich seither deutlich abgekühlt. Die liberale Kryptopolitik war für die Deutschen und die Europäer angesichts der über das Echelon-Netzwerk betriebenen Wirtschaftsspionage die einzige Verteidigungsmöglichkeit. Der

Schutz von Unternehmen gegen die elektronische Ausspähung kann nur mit Hilfe von guten Verschlüsselungswerkzeugen wirksam sein – die Gegenspionage-Abteilungen der Geheimdienste sind hier weitgehend machtlos. Wohl auch deshalb darf es nicht überraschen, dass Frankreich, das selbst lange eine äußerst restriktive Politik betrieb, kurz nach dem deutschen Liberalisierungsschritt ebenfalls Lockerungen einführte. Deutsche und Franzosen hatten hier ihre Politik aufeinander abgestimmt. Diesen Kurs bekräftigte die Arbeit des Echelon-Untersuchungsausschusses des Europäischen Parlaments. Er forderte Kommission, Rat und die Mitgliedstaaten auf, eine effektive und aktive IT-Sicherheitspolitik zu betreiben. Dies betrifft auch die Entwicklung wirksamer Sicherheitsprodukte, wobei vor allem Projekte unterstützt werden sollen, die nutzerfreundliche Open-Source Verschlüsselungssoftware entwickeln. Softwareprodukte, die ihren Quelltext nicht offen legen, sollten in einem künftigen europäischen Sicherheitsstandard in die am wenigsten verlässliche Kategorie herabgestuft werden.

Ein Jahr lang hatte der Echelon-Untersuchungsausschuss zahlreiche internationale Experten befragt, bevor er Anfang Juli 2001 seinen Abschlussbericht verabschiedete. Auf einen Nenner gebracht kam er zu dem Schluss: Echelon existiert, aber es gibt nicht viel, was man dagegen tun kann. Die Abgeordneten empfahlen diplomatische Verhandlungen mit den USA, mehr Rechtssicherheit für europäische Bürger – und Selbstschutz durch Verschlüsselung. In der strittigen Frage, ob das globale Überwachungssystem auch zur Konkurrenzspionage verwendet werde, kam der Ausschuss zu der Ansicht, dass dies zweifellos der Fall sei, auch wenn es keinen einzelnen, klar bewiesenen Fall gäbe. Seriöse Quellen hätten den Brown-Bericht des US-Kongresses bestätigt, wonach fünf Prozent des Aufklärungsmaterials aus nicht-offenen Quellen für Wirtschaftsspionage benutzt wird. Dieselben Quellen schätzen, dass diese Aufklärungsarbeit die US-Industrie in die Lage versetze, bis zu 7 Milliarden US-Dollar über Verträge einzuspielen. Dass die USA gezielt die Kommunikation einzelner Unternehmen überwachen, um »Marktverzerrungen durch Bestechung zu Ungunsten von US-Firmen zu verhindern«, gab Ex-CIA-Direktor James Woolsey gegenüber dem europäischen Untersuchungsausschuss zu.[48]

Die US-Station in Bad Aibling sollte im Herbst 2002 ihren Betrieb einstellen. Dieser Plan wurde jedoch nach den Terroranschlägen vom 11. September wieder ad acta gelegt. Die Episode zeigt, dass die USA in Europa eine neue sicherheitspolitische Konstellation aufbauen: Wohl aus Verärgerung wegen der eigenständigen Krypto- und Geheimdienstpolitik Deutschlands und Frankreichs in der Europäischen Union setzen die USA verstärkt auf Spanien. Schon in den ersten Monaten der Bush-Regierung konnten die Spanier wichtige Rüstungsaufträge gewinnen und die begehrte US-amerikanische Aufklärungstechnik für den Kampf gegen die baskische Terrororganisation ETA benutzen. Auch Italien und Griechenland bot die Bush-Regierung geheimdienstliche Unterstützung im Kampf gegen Terroristen an. Die geheimdienstliche Zusammenarbeit wurde zudem auch mit Norwegen, Däne-

mark und der Schweiz intensiviert. Ziel unter anderem ist auch, Großbritanniens Isolation langfristig zu beenden.

8. Praxisausblick

Zwar stimmt es optimistisch, dass die Verschlüsselung derzeit in Europa weitgehend keiner Kontrolle unterworfen ist. Doch nur die wenigsten Firmen, Bürger und Bürgerinnen verschlüsseln ihre Daten tatsächlich. Entweder weil ihre Bedienung zu mühsam und zeitintensiv ist, oder weil man kaum Partner findet, die ebenfalls damit umgehen können. Für die Misere gibt es vor allem zwei Gründe: Die Nutzer sind einerseits zu bequem, zwei, drei zusätzliche Mausklicks für die Sicherheit in Kauf zu nehmen – immer mit der Frage im Hinterkopf: Was kann mir kleinem Nutzer denn schon passieren? Andererseits sind die Schutzwerkzeuge selbst bei gutem Willen nur umständlich zu bedienen. Die IT-Sicherheitsbranche ist immer noch zu sehr auf die Technik selbst fixiert und kümmert sich zu wenig um das Marketing. Die Frage, ob eine Schlüssellänge zu kurz oder zu lang ist, ist für die Techniker wichtiger als die Frage, ob ihr Produkt denn tatsächlich verwendet wird. Die heutige Kryptopolitik kümmert sich deshalb nach den politischen Schlachten der Vergangenheit vor allem um die Frage, wie man die Kryptografie unter die Leute bekommt. Eine Schlüsselrolle kommt hier den Kryptoherstellern zu, die eine nahezu unsichtbare Sicherheitstechnologie schaffen müssen.

Anmerkungen

1 Kryptografie von kryptos (griech.: κρυπτοσ): geheim und graphikos (griech.: γραφι κοσ): schreibkundig bezeichnet den Vorgang des geheimen Schreibens selbst. Kryptos in Verbindung mit logos (griech.: λογοσ): Rede, Vernunft, bezeichnet die Wissenschaft von den Geheimschriften.
2 Diese und weitere Hintergründe beschreibt Richard Overy, Die Wurzeln des Sieges. Warum die Alliierten den Zweiten Weltkrieg gewannen, Stuttgart 2000.
3 Peter Wright/Paul Greengrass, Spy Catcher, Frankfurt 1989, S. 89 ff.
4 Ebd. S. 116 ff.
5 Christiane Schulzki-Haddouti, Elektriktrick, Chiffriermaschinen des 20. Jahrhunderts, in: c't 3/2000.
6 Mike Witt, Tactical Communications, in: Military Technology, Nr. 5, 1991, S. 19-25, S. 22.
7 J. H. Ellis, The Possibility of Secure Non-Secret Digital Encryption, Januar 1970, http://www.cesg.gov.uk/publications/media/nsecret/possne.pdf
8 C.C. Cocks, A Note on Non-Secret Encryption, CESG Report, 20th Nov. 1973.
9 Whitfield Diffie/Martin E. Hellman, New Directions in Cryptografy, in: IEEE Transactions on Informations Theory, Nov. 1976, S. 644-654, verfügbar unter: http://cne.gmu.edu/modules/acmpkp/security/texts/NEWDIRS.PDF
10 Bobby Inman, The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector, in: Cryptologia, July 1979, S. 129-135, S. 129.

11 Ebd., S. 130.
12 David Kahn, The Public's Secrets, in: Cryptologia, Jan 1981,S. 20-26, S. 20.
13 The House Committee on Government Operations: The Government Classification of Privat Ideas, House Report No. 96 1540 (Union Calendar No. 908), 96th Congress, 2nd Session, Washington 1980, in: Cryptologia, April 1981, S. 24-93, S. 88 f.
14 Inman, vgl. Anm. 10, S. 133.
15 Ebd, S. 134.
16 Deborah Shapley, Intelligence Agency Chief seeks »Dialogue« with Academics, in: Science, Vol. 202, 2 Oct. 78, S. 407-410, S. 410; The House Committee on Government Operations, vgl. Anm. 13, S. 87.
17 Kahn, vgl. Anm. 12, S. 24.
18 PCSG: Report of the Public Cryptografy Study Group, in: Communications of the ACM , July 81, Vol. 24, No. 9, S. 434-445.
19 Kahn, vgl. Anm. 12, S. 23 f.
20 Ian F. Fergusson, The Export Administration Act: Controversy and Prospects, 26. 3. 2001, http://www.cnie.org/nle/crsreports/economics/econ-74.cfm
21 Kahn, vgl. Anm. 12, S. 24.
22 William Carey, Handcuffing Science, in: Science, Vol. 217, Sept 24, 1982, S. 1233; Colin Norman, Administration Grapples with Export Controls, in: Science, Vol. 220, 3. June 1983, S. 1021-1024, S. 1021.
23 Telex, AT&T an Uni Dortmund, 15. 11. 83.
24 Jerry Proc, KL7, http://webhome.idirect.com/~jproc/crypto/kl7.html
25 Mehr Details in: Ralf Bendrath, PGP – die ersten zehn Jahre, in: Telepolis, 19. 03. 2001, http://www.heise.de/tp/deutsch/inhalt/te/7175/1.html
26 http://www.fitug.de/debate/9709/msg00031.html und auch http://inf2.pira.co.uk/top012.htm
27 Das Programm ist für den privaten Einsatz lizenzfrei erhältlich und kann zum Beispiel über den PGP-Server ftp://ftp.de.pgpi.com/pub/pgp oder über Network Associates, Inc. (http://www.pgpinternational.com) bezogen werden. Hier finden sich auch Hinweise zur Installation und zur Bedienung des Programms.
28 Vgl. Kai Raven, Spion in der Tastatur, in: Spiegel Netzwelt vom 27. Juni 2000, http://www.spiegel.de/netzwelt/technologie/0,1518,82775,00.html
29 Christiane Schulzki-Haddouti, Update Kryptopolitik, in: Telepolis, 29. 10. 1998, http://www.heise.de/tp/deutsch/inhalt/te/1615/1.html
30 Christiane Schulzki-Haddouti, Hintertür für Spione, in: Die Zeit, 17. 9. 1998.
31 Dies., vgl. Anm. 29.
32 Ebd.
33 Christiane Schulzki-Haddouti, »Wir wollen verhindern, daß starke Verschlüsselung in die Hände der falschen Regierungen, Organisationen und Individuen gerät«, Ein Interview mit David Aaron, dem Krypto-Experten der amerikanischen Regierung, in: Telepolis, 29. 10. 1998, http://www.heise.de/tp/deutsch/inhalt/te/1616/1.html
34 Dies., Umrüstung. Kryptografie gilt weiterhin als Waffe, in: c't 26/1998. http://www.heise.de/ct/98/26/052/
35 Dies., vgl. Anm. 29.
36 Ebd.
37 Ebd.
38 Florian Rötzer, Pentagon: Keine Ausländer mehr im IT-Bereich, in: Telepolis, 7. 3. 2002, http://www.heise.de/tp/deutsch/inhalt/co/12028/1.html
39 Christiane Schulzki-Haddouti, Lockerungen für Kryptoexporte innerhalb der EU, in: Telepolis, 7. 4. 1999, http://www.heise.de/tp/deutsch/inhalt/te/2718/1.html

40 Eckpunkte der deutschen Kryptopolitik, Pressemitteilung des Bundesministerium für Wirtschaft und Technologie und des Bundesministerium des Innern, 2. Juni 1999, http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=4&tsid=100&tdid=116&page=0

41 http://www.gnupg.de/, Homepage von GnuPG.

42 Presseerklärung über Förderung des Projektes »Open Source und IT- Sicherheit: Weiterentwicklung und Vermarktung des GNU Privacy Guards (GnuPG)«, 18. 11. 1999, http://www.sicherheit-im-internet.de/themes/themes.phtml?ttid=2&tdid=121&page=0

43 Neben GnuPG gibt es auch andere OpenPGP-Varianten von PGP: Cryptoex arbeitet ebenfalls auf Basis von OpenPGP und kann zusammen mit dem E-Mail-Programm Outlook Express benutzt werden. Für Macintosh-Rechner gibt es ein PGP-kompatibles Programm namens MacCTC.

44 MS Windows 2000, NT, 98 und GNU/Linux.

45 Alle Texte, die man unter Windows erst markiert und dann mit der Tastenkombination Strg+C kopiert, landen in der Zwischenablage. Mit der Tastenkombination Strg+V werden sie aus der Zwischenablage wieder herausgeholt und können an beliebigen Stellen eingefügt werden.

46 GEAM ist die Abkürzung für Geam Encrypts All Mail.

47 Einzige Voraussetzung ist die Verwendung von TCP/IP als Netzwerkprotokoll und SMTP als Mail-Protokoll.

48 Christiane Schulzki-Haddouti, Außer Spesen nichts gewesen?, in: Telepolis, 10. 05. 2001, http://www.heise.de/tp/deutsch/special/ech/7601/1.html, siehe auch Duncan Campbell, Ehemaliger CIA-Direktor, sagt, die Wirtschaftsspionage der USA würde auf »Bestechungsaktionen der Europäer« zielen, in: Telepolis, 12. 03. 2000, http://www.heise.de/tp/deutsch/special/ech/6663/1.html