Politik der Chiffren

Verschleierte Seiten der Kryptographie-Debatte

Ingo Ruhmann

(aus: FIfF-Kommunikation 3/96)

Die Verschlüsselung von Nachrichten und ihre Wissenschft, die Kryptographie, wird derzeit in den Medien intensiv debattiert. Die Kurzformel der derzeitigen Kryptographie-Debatte lautet: Kryptographie ist die einzige effektive Möglichkeit zu vertraulicher elektronischer Kommunikation, sie wird aber durch Militärs und Geheimdienste behindert. Während hervorgehoben wird, wie nützlich kryptographische Verfahren für elektronische Transaktionen sind, bleibt dabei die Rolle der staatlichen Seite vage. Wilde Vermutungen werden abgelöst von immer wieder neuen Überraschungen über Aktivitäten des Gesetzgebers und der Exekutive. Die Rolle der Militärs und ihre Interessen bleiben verdeckt, was die Bewertung der Hintergründe staatlichen Handelns stark erschwert. In diesem Beitrag soll nun versucht werden zu analysieren, welche Interessen und aktuellen Ziele staatliche Stellen an der Kryptographie haben und was deren Bedeutung für diese Stellen ist.

Die Informatik gehört zu den Profiteuren des militärischen Interesses an der Kryptographie. Einer der drei historischen Ursprünge des Computers in den USA, Deutschland und Großbritannien ist die Arbeit an der maschinellen Entschlüsselung des ENIGMA-Codes der Wehrmacht durch Alan Turing und seine Kollegen in der britischen Chiffriereinrichtung Government Communications Headquarter (GCHQ). Auch in den Jahren nach dem Zweiten Weltkrieg brachten Chiffrier-Geheimdienste die Computerentwicklung maßgeblich voran. In den 50er Jahren gab die National Security Agency (NSA), Chiffriergeheimdienst der USA, über eine Milliarde Dollar für die Entwicklung von Hochleistungsrechnern aus. In ihrer gesamten Geschichte ist die NSA der größte Anwender von Supercomputern geblieben. Auch hierzulande, so wird berichtet, nutzten die Chiffrierexperten der heute zum Bundesamt für Sicherheit in der Informationstechnik (BSI) mutierten früheren Zentralstelle für das Chiffrierwesen (ZfCh) die ersten Supercomputer in der Bundesrepublik. Derzeit beschafft das BSI einen neuen Supercomputer für die Kryptoanalyse[1]. Alle genannten Geheimdienste waren und sind entweder eine militärische Organisation oder kooperierten innig mit Militärs.

[1] Antwort der Bundesregierung auf die Kleine Anfrage von Dr. Manuel Kiper "Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, auf Frage 5

Betriebsgeheimnisse und CyberCash

Seit Anfang der 80er Jahren ist die Kryptographie jedoch nicht länger alleinige Domäne der Militärs. Das zunehmende zivile Interesse an Kryptographie hat zu neuen Konflikten geführt. Der moderat als Kryptographie-Debatte umschriebene Konflikt ist einer zwischen kommerziellen Interessen und denen des Staates. Der Schutz der Privatsphäre durch Kryptierung wird zwar gern angeführt, hat aber bei der Bewertung keinen nennenswerten Einfluß.

Die kommerzielle Nutzung von elektronischer Kommunikation benötigt Kryptierverfahren bei der Verschlüsselung elektronischer Kommunikation zum Schutz von Betriebsgeheimnissen und zur Abwicklung von Geschäften, die elektronische Signatur zur Authentisierung von Geschäftsvorgängen und digital signierte elektronische Geldäquivalente zur Abwicklung elektronischer Zahlungen. Ohne diese Kryptierverfahren ist der Rationalisierungsgewinn vollelektronischer Kommunikation und Transaktion ohne Medienbrüche nicht zu erzielen: Allein die digitale Signatur für elektronische Kommunikation macht 250.000 Arbeitsplätze jener überflüssig, die bislang eingehende Papierdokumente gesichtet und vor-bearbeitet haben[2]. Die Absicht der Banken, einen großen Teil ihrer Zweigstellen durch elektronische Verfahren zu ersetzen und damit in den USA 450.000, hier 100.000 Arbeitsplätze abzubauen, ist nur durch den Einsatz von Kryptierverfahren bei Transaktionen zu erreichen[3]. Das Internet zum Warenhaus zu machen, setzt schließlich elektronisches Geld voraus, das mit kryptographischen Mitteln realisiert wird.

Dem entgegen stehen auf staatlicher Seite Aufklärungswünsche der Strafverfolgungsbehörden, vor allem aber der Geheimdienste und Militärs. Hier wurde in den letzten Jahren das Abziehbild-artige Diskussionsmuster vom Mafiosi entwickelt, der durch nicht entschlüsselbare Kryptierverfahren seine finsteren Taten vorbereiten und koordinieren könne.

Von ENIGMA bis Information Warfare

Damit ist jedoch nur ein kleiner Teil der Bedeutung beschrieben, die Kryptographie für staatliche Stellen hat. Im staatlichen Bereich wird Kryptographie zum Schutz von Kommunikation vor allem gegen Kenntnisnahme durch Stellen anderer Staaten genutzt. Da es hierbei um weltweite diplomatische oder militärische Kommunikation mit Inhalten von hoher politischer Bedeutung geht, hat Kryptographie gerade im staatlichen Bereich

[2] Dirk Fox: Automatische Autogramme; in: c't 10/95, S. 278-284, S. 278

[3] Für die USA basiert dies auf einer Studie von Delotte & Touche LLP: 450.000 Banken-Jobs verschwinden in den USA; in: Süddeutsche Zeitung, 16.8.95, S. 20 und Eine Welt ohne Bankfilialen; in: ebd., 30.8.95. Die Entwicklung in der Bundesrepublik wurde analysiert von Arthur D. Little: Heißer Draht; in: Der Spiegel, 17/95, S. 121-125

den Status eines Hilfsmittels zur Wahrung staatlicher Autonomie. Diese staatliche Autonomie drückt sich gleichermaßen darin aus, die Kommunikation anderer - vor allem staatlicher Stellen - auszuspionieren, um daraus für eigene Zwecke einen Nutzen zu ziehen. Dabei werten Geheimdienste die elektronische Kommunikation anderer Länder aus, Militärs versuchen, Daten ihrer potentiellen Gegner zu nutzen. Doch es sind die Erfahrungen der Militärs, die die Furcht der Geheimdienste und Strafverfolger vor Kryptierung schüren.

Der Vergleich zwischen ziviler und militärischer Kommunikation macht deutlich, wie hoch die Bedeutung der Kryptographie im Militär ist. Während Polizeifunk, Telefon-Funkstrecken und alte analoge Funktelefone unverschlüsselt sensibelste Inhalte leicht abhörbar machten, verwenden Militärs schon für die Kommunikation auf dem Schlachtfeld und erst recht zwischen räumlich entfernten Stellen Kommunikationssysteme mit eingebauter Verschlüsselung.

Die letzte Schlacht zwischen hochtechnisierten Armeen, die entschieden wurde, weil bei der Kommunikation zwischen Kommandostellen eine Verschlüsselung fehlte, fand im Ersten Weltkrieg statt. Im Zweiten Weltkrieg entschied nicht zuletzt die Entschlüsselung der ENIGMA über den Kriegsausgang. Die Entwicklung der Verschlüsselungssysteme in der Zeit des Kalten Krieges schließlich gefährdete ernsthaft die Bedeutung der Entschlüsselung. Trotz Supercomputern begrenzte die erreichte hohe Qualität der Kryptiersysteme direkte Entschlüsselungserfolge. Das Speichern von abgefangenen Nachrichten und das Warten auf ausspionierte Schlüssel, bessere Computer oder besseres Wissen um gegnerische Codes wurde zum Schauplatz des einzigen seit 1945 konstant geführten Kampfes, der elektronischen Kriegsführung, die gegenwärtig zum Information Warfare weiterentwickelt wird.

Mangels Entschlüsselungserfolge ließen sich aus den Inhalten der Nachrichten keine Informationen mehr gewinnen. Stattdessen gewannen Strukturdaten darüber an Bedeutung, auf welcher Frequenz von welchem Ort aus in welchem Code gesendet wurde. Als Signals Intelligence hat diese Klasse von Spionagedaten eine eigene Bedeutung erlangt. Der nächste Schritt war das Verbergen von Nachrichten und Sender durch Frequenzsprungverfahren oder die Frequenzspreizung. Die Steganographie ist eine zivile Variante dieser Techniken eines Verbergens der Existenz einer Nachricht. Dies gilt - wie gesagt - nur für hochtechnisierte Armeen. Kleine Staaten haben dagegen nur sehr geringe Möglichkeiten, Kryptiersysteme zu entwickeln oder zu erwerben. Wie noch zu sehen sein wird, wirkt sich die staatliche Aufsicht über Anbieter von Chiffriergeräten als besonderer Bonus der Investitionen für Chiffrier-Geheimdienste aus.

Die Entwicklung der US-Streitkräfte für die Bedürfnisse von Information Warfare führt zu zwei gegenläufigen Tendenzen. Auf der einen Seite gewinnt der Schutz eigener Netze noch an Bedeutung. Für die Sicherheit aller sensitiven Netze hat die NSA die Multilevel

Information Security System Initiative (MISSI) begonnen. Als Teil von MISSI ist für die Beschaffung aller PCs in der US-Verwaltung genügend Platz für Kryptier-Erweiterungskarten wie die Fortezza-Karte vorgeschrieben. Bis zum Jahr 2000 sollen über 2 Millionen dieser Karten eingebaut und damit die Verschlüsselung des sensitiven zivilen und militärischen Behördenverkehrs in den USA erreicht sein[4]. Auf der anderen Seite steht die Nutzung möglichst vieler Daten eines potentiellen Gegners[5]:

> "Der Informationsvorteil kann helfen, traditionelle militärische Bedrohungen zu relativ geringen Kosten abzuschrecken oder abzuwehren. [...] Die USA kann ihre Informationsressourcen nutzen, um China, Rußland und andere machtvolle Staaten in einen Sicherheitsdialog zu verwickeln, um sie davon abzuhalten, eine feindliche Haltung zu entwickeln"[6].

Diese sich derzeit vollziehende Umstellung der Abschreckung von Atomwaffen auf Daten markiert nicht nur den Wechsel vom Nuklearen zum Nuntialen Zeitalter[7], sondern setzt den Zugang zu möglichst vielen Daten voraus. Kryptierung ist dabei der größte Hemmschuh. Der Eifer, Kryptiersysteme vom zivilen Markt und aus der zivilen Wissenschaft herauszuhalten oder so weit wie möglich zu behindern, ist begründet in der hohen Bedeutung, die einem gut lesbaren internationalen Datenverkehr bei Information Warfare zukommt.

Zusammengenommen bedeutet dies, daß die starke Nutzung der Kryptographie durch militärische Einheiten also zu der semiotischen Abwärtsspirale geführt hat, statt der Information aus Inhalten zunächst lediglich Struktur und Form der Signale zu erlauschen und nun auch diese immer schwerer detektieren zu können und damit immer weniger Informationen zu erhalten. Für die in militärischem wie geheimdienstlichem Auftrag gleichermaßen arbeitenden Chiffrier-Geheimdienste ist dies Warnung genug, um eine ähnliche Entwicklung in nichtmilitärischen Sektoren und vor allem bei gewöhnlichen Zivilisten so lange wie möglich zu verhindern. Für die Erreichung der Ziele von Information Warfare ist das Militär auf eine möglichst leicht zu verarbeitende, also unverschlüsselte Kommunikation potentieller Gegner angewiesen.

Neben Information Warfare ist zusätzlich die Ausweitung geheimdienstlicher Aufgaben getreten. Nicht nur beim Bundesnachrichtendienst (BND) hat das Organisierte Verbrechen den Warschauer Pakt als Hort des Bösen abgelöst. Hinter der bekannten Diskussionsfigur des Krypto-erfahrenen Mafiosi steckt also die Erfahrung mit den hochentwickelten militärischen Kryptosystemen vor allem der ehemaligen Sowjetunion.

---

[4] David Lawrence: Many Options for Implementing Fortezza is in the MISSI Framework; in: Defense Electronics, 11/95, S. S8-S10

[5] Dieser braucht weder Nationalstaat zu sein noch muß es sich bei militärischen Aktionen um einen bewaffneten Konflikt handeln, vgl.: Ingo Ruhmann: Netwar und Cyberwar - Kriegsführung in der Zukunft; in: FIFF-Kommunikation, Nr. 4, 1994, S. 39-42

[6] Josph Nye Jr, William A. Owens: America's Information Edge; in: Foreign Affairs, March/April 1996

[7] Ute Bernhardt, Ingo Ruhmann: Computer im Krieg - die elektronische Potenzmaschine; in: Norbert Bolz; Friedrich Kittler; Christoph Tholen (Hrsg.): Computer als Medium, München, 1994, S. 183-207

Bei den neuen Zielgruppen geheimdienstlicher Aufmerksamkeit läßt sich auch wesentlich einfacher an hochwertige Informationen kommen. Das neue Einsatzgebiet mit besonderer Bedeutung ist die Wirtschafts- und Industriespionage. Der US-Geheimdienst CIA begründete dies mit angeblichen französischen Aktivitäten. Auch der BND arbeitet auf diesem Gebiet.

Wozu US-Geheimdienste Industriespionage betreiben und dabei Schwächen in Kryptosystemen ausnutzen, zeigt sich derzeit im europäischen Rüstungsmarkt. Die US-Botschafter in Europa setzen sich vehement für ihre Rüstungsindustrie ein. Dabei geben US-Stellen an US-Unternehmen Daten über europäische Konkurrenzfirmen weiter, die sie gesammelt haben. In der Schweiz ging es um den Verkauf von Flugzeugen, in Griechenland um Phantom-Jets und Radaranlagen[8]. Nach dem Bombenanschlag auf das World Trade Center 1996 ermittelten US-Geheimdienste, daß Geld für die Attentäter per Banküberweisung aus Frankfurt gekommen war, wo es wiederum Mittelsmännern nahöstlicher Geheimdienste eingezahlt haben sollen. Die Überwachung internationaler Finanztransaktionen scheint also gut zu funktionieren.

Die nichtmilitärischen Quellen von Geheimdiensten - soweit es sich nicht um öffentliche Quellen handelt - sind nicht ernsthaft auf ein Ausspähen ihrer Daten und Kommunikation vorbereitet und weisen erhebliche Mängel in ihren Schutzvorkehrungen auf. Die Erfolge der Geheimdienste sind hier noch leicht zu erzielen. Ihnen droht Gefahr, wenn es zu einer weitverbreiteten Nutzung von Kryptosystemen kommt.

Wissen um Kryptographie wurde deshalb in den zurückliegenden Jahrzehnten gern als Geheimwissenschaft betrachtet und staatlicherseits monopolisiert. Es gab nur wenige Experten, die viele Staaten der Erde in meist nur einer staatlichen Einrichtungen zusammenzogen und dort unter Ausschluß der Öffentlichkeit arbeiten ließen. Die genutzten Kryptoverfahren ließen sich so gut unter Kontrolle halten. Diesem Hoheitswissen droht nun von ziviler Seite Gefahr.

Es ist deshalb interessant, den Fragen nachzugehen, welche Situation im Kryptierbereich erstens heute vorzufinden ist und zweitens, wie es überhaupt dazu kommen konnte, daß das Wissen um Kryptographie heute so weit verbreitet ist, daß es nur noch schwer zu kontrollieren ist.

[8] Craig Covault: U.S. Export Push Challenges Europeans; in: Aviation Week & Space Technology, May 27, 1996, S. 20-22

Strategische Kontrolle auf dem Krypto-Markt

In der Vergangenheit war kryptographisches Wissen und dessen Nutzung selbst ein wohlbehütetes Geheimnis, für das die strengsten Sicherheitsstufen galten. Kryptographie war militärischen Stellen zugeordnet und im militärischen Apparat auf besondere Weise abgekapselt. Die Arbeiten Alan Turings an der Entschlüsselung der ENIGMA wurden im Krieg von Großbritannien längere Zeit nicht einmal an die USA weitergegeben und blieben für die Öffentlichkeit bis in die 70er Jahre geheim. Zu dieser Zeit wurden auf dem ENIGMA-Prinzip arbeitende Verschlüsselungsmaschinen auch in Ländern der Dritten Welt kaum noch eingesetzt. Das Wissen um die eigenen wie die gegnerischen kryptographischen Verfahren gehört zu den Ultra-Geheimnissen jedes Staates, mit dem Politik gemacht wird.

Politisch bedeutsame Staaten wie die Atommächte USA, Großbritannien, Frankreich, China, die ehemalige Sowjetunion, aber auch die Bundesrepublik haben Verschlüsselungs-Verfahren entwickelt, die als sicher gelten. Ein Mitlesen ist bei ihnen nur durch unachtsame Nutzung, Verrat oder temporär beim Einsatz völlig neuer Abhör-Technologien möglich. Kleinere und weniger technisierte Staaten haben nicht die Kapazitäten zu Eigenentwicklungen und müssen eingekauftes Gerät nutzen. Weltweit gibt es nur fünf Anbieter für kryptographisches Gerät[9]. Die Anbieterländer sorgten bisher auch dafür, daß die Zahl der Unternehmen übersichtlich bleibt. Sie haben deshalb bei Verkäufen von Systemen in Drittländer die "strategische Kontrolle" über die geschützte Kommunikation ihrer Kunden[10].

Wer Kryptiersysteme kaufen möchte, sieht sich Exportregelungen gegenübergestellt, die denen von Massenvernichtungsmitteln gleichkommen. Die Exportregeln für alle westlichen Anbieter von Kryptiertechnologie entstammen der Zeit des Kalten Krieges und wurden im Exportkontroll-Gremium COCOM (für: Coordination Commitee) verbindlich festgelegt. Die USA haben das Verbot eines Exports von Kryptiersystemen in der International Traffic in Arms Regulation (ITAR) festgelegt, die Bundesrepublik in der Ausfuhrliste Teil I C Abschnitt 5 Teil 2 gemäß Außenwirtschaftsverordnung. Ausfuhren begutachten und damit genehmigen in allen westlichen Staaten die Chiffriergeheimdienste wie die NSA oder hier das BSI[11].

Trotz dieser Regelungen sind Kryptosysteme aus Europa in kleineren Ländern gefragt. Siemens entwickelte zusammen mit dem heutigen BSI verschiedene Geräte zur Sprach- und Datenverschlüsselung. Obwohl der Firma gute Kontakte zum Bundesnachrichtendienst (BND) nachgesagt werden, hat dies ihrem Absatz nicht geschadet. Beim Kauf der britischen Firma Plessey durch Siemens wurde der nationalen

[9] Erich Schmidt-Eenboom: Der BND. Schnüffler ohne Nase, Düsseldorf, 1993, S. 221
[10] Mike Witt: Tactical Communications; in: Military Technolgy, Nr 5, 1991, S. 19-25, S. 22
[11] vgl. Antwort der Bundesregierung auf die Kleine Anfrage von Dr. Manuel Kiper "Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, auf Frage 6

Sicherheit wegen der Unternehmensteil Plessey Crypto der britischen Firma General Electric zugeschlagen. Beide sind die wichtigsten Entwickler und Lieferanten von Kryptiersystemen im europäischen Bereich.

Das BSI und zuvor das ZfCh "arbeiten grundsätzlich mit allen deutschen Kryptoherstellern zusammen"[12]. Das BSI hat dabei ausschließlich für den staatlichen Bereich selbst entwickelt, aber auch zum Teil entwickeln lassen, wobei Aufträge an die Industrie vergeben wurden. Für Verkäufe solcher Geräte an Dritte wurden Lizenzen vergeben[13]. Nützlich für die Entschlüsselung der Kommunikation des Käufers solcher Geräte ist dabei, daß dem BSI der Aufbau der verkauften Systeme bekannt ist. Trotz aller Internationalisierung zeigt sich hier, daß Kryptographie aus klaren Interessen heraus eine strikt nationalstaatliche Angelegenheit geblieben ist.

Eine Besonderheit ist die seit 1959 in der Schweiz ansässige Crypto AG. Sie wurde von vielen jungen Staaten der Dritten Welt als Lieferant von Kryptogerät geschätzt, die sie für unabhängig von staatlicher Einflußnahme hielten. In den 70er Jahren wurde jedoch bekannt, daß die NSA seit 1957 offenbar über technologische Entwicklungen der Firma informiert wurde[14]. Auch die heute undurchsichtigen Besitzverhältnisse an der Crypto AG haben ihren Ruf als unabhängiger Lieferant von Kryptosystemen nicht schädigen können. Ihre Kunden müssen gewisse Fragwürdigkeiten in Kauf nehmen, da ihnen die Alternativen fehlen.

Die allgemeine Verbreitung von Kryptiersystemen durch einen freien Markt wäre daher ein erheblicher Rückschritt für die Wächter über dieses Wissen - die Chiffrierdienste der jeweiligen Länder. Sie alle eint das Interesse, es nicht zu einer unkontrollierten Ausbreitung von Kryptiersystemen kommen zu lassen.

Kryptographie als Wissenschaft - wie konnte es dazu kommen?

Nach dem Ende des Kalten Krieges besteht für die Chiffriergeheimdienste die Hauptgefahr nicht aus den arbeitslos gewordenen Krypto-Experten der ehemaligen Ostblockstaaten, die im Gegensatz zu den Nuklearphysikern offenbar geräuschlos in andere Beschäftigungsverhältnisse gewechselt sind, sondern die Verbreitung von Krypo-Know-How durch Wissenschaftler und neue Firmen. Dabei haben sie ihr bestes gegeben, um diese Verbreitung zu behindern.

[12] Antwort der Bundesregierung auf die Kleine Anfrage von Dr. Manuel Kiper "Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, auf Frage 3

[13] Antwort der Bundesregierung auf die Kleine Anfrage von Dr. Manuel Kiper und Manfred Such "Das Bundesamt für Sicherheit in der Informationstechnik", Drs. 13/3408, auf Frage 44

[14] James Bamford: The Puzzle Palace, New York, 1983, S. 407ff

Die heutige Krypto-Kontroverse ist ein Spiegelbild der Debatte, die vor über zehn Jahren in der USA ausgetragen wurde. Seit Mitte der 70er Jahre wurden kryptographische Verfahren zunehmend auch von zivilen Nutzern eingesetzt. Mit der Anwachsen der Kommunikation multinationaler Firmen und internationaler Bankgeschäfte wurden erstmals Chiffriergeräte von Privatfirmen eingesetzt.

1977 wurde für diese Nutzer der Data Encryption Standard (DES) ausgewählt und zum Standard erklärt, obwohl dessen Schlüssellänge als zu kurz kritisiert wurde[15]. Der DES war entwickelt worden, um Kryptierleistung auf einem Chip preiswert verfügbar zu machen und wurde 1984 für den US-Bankenverkehr vorgeschrieben[16]. Ende der 70er Jahre hatte die Kryptographie als Fachgebiet in den USA schließlich den Schwellwert für eine eigendynamische Entwicklung erreicht. Aus allenfalls zwei Patenten pro Jahr für Kryptosysteme waren ein halbes Dutzend pro Monat geworden[17].

Dies hielt die NSA für eine Gefährdung der nationalen Sicherheit, die sie nicht hinzunehmen gewillt war. Schon 1975 vertrat die NSA der National Science Foundation gegenüber einen Alleinvertretungsanspruch für die Vergabe von Forschungsunsunterstützung in der Kryptographie[18]. 1978 ging die NSA in die Offensive und versuchte, ausländische Teilnehmer von Konferenzen fernzuhalten, die Publikation von Forschungsergebnissen zu verhindern, ließ Patente für geheim erklären und versuchte sogar, die zivile Förderung für die Forschung an Kryptosystemen - ausgerechnet bei Leonard Adelman, einem der drei Erfinder des RSA-Verfahrens - zu unterbinden[19]. Der Höhepunkt aber war die Idee der NSA, die Kryptographie-Forschung als "born secret" zu klassifizieren. Eine solche, nur für Atomwaffen-relevante Forschung existierende Klassifikation als "geheim geboren" hätte bedeutet, alle zivilen und nichtzivilen Forschungsarbeiten für Geheim zu erklären und vor einer Veröffentlichung einer Kontrolle durch die NSA zu unterwerfen. Da viele Universitäten in den USA keine Geheimforschung dulden, wäre die Kryptographie-Forschung effektiv behindert worden[20].

Auf Vorschlag der NSA berief der Rat für Erziehung als Arbeitsgruppe die "Public Cryptography Study Group" ein, die 1981 ein System der Selbstzensur vorschlug, da eine gesetzliche Regelung ohnehin kaum mit der Verfassung vereinbar wäre[21]. Der damalige NSA-Chef Inman wollte dies sogar für Informatik allgemein angewandt wissen. In der Folge wurden die fraglichen Themengebiete ausgedehnt. Erst der Druck der National

[15] Whitfield Diffie, Martin Hellman: A Critique of the Proposed Data Encryption Standard; in: Communications of the ACM, March 1976, S. 164-165
[16] Edith Myers: Speaking in Codes; in: Datamation, Dec. 1, 1984, S. 40-45
[17] vgl.: David Kahn: The Public's Secrets; in: Cryptologia, Jan. 1981, S. 20-26
[18] Paul Wellich: Cryptography: voluntary control seems to work; in: IEEE Spectrum May, 1982, S.66
[19] Kahn, S. 23f
[20] vgl dazu: Ingo Ruhmann: Beeinträchtigung der wissenschaftlichen Freiheit durch die neue Wissenschaftspolitik der USA; in: J. Bickenbach, H. Genrich, R. Keil, W. Langenheder, M. Reisin: Informatik und Militär, Berlin, 1984, S. 61-66
[21] David Dickson: More secrecy on cryptography research; in: Nature, 19.2.1981, S. 621

Academy of Science[22] und der Boykott der Wissenschaftler, Forschungsaufträge des Pentagon unter derartigen Publikations-Bedingungen anzunehmen, führte zu einem ersten Umdenken im Pentagon ab 1984[23]. Dennoch gab es auch zwei Jahre später noch Probleme vor allem im Zusammenhang mit Exporten. Erst das Ende des Kalten Krieges und der Wechsel der US-Administration brachte einen grundlegenden Wandel in dieser Politik.

Die durch Universitätsbeschlüsse untermauerte Drohung der US-Wissenschaftsgemeinde, nicht länger Aufträge des Militärs anzunehmen und die zusätzliche Drohung mit einer Verfassungsklage[24] brachte das Pentagon und die NSA nach zähem Ringen schließlich dazu, die Kontrolle der zivilen Forschung wieder zurückzuschrauben, nachdem ein neuer Präsident keinen Rückhalt mehr bot. Diesem harten Konflikt, den Militärs um die Freiheit der Forschung in der Kryptographie begonnen hatten, entspringt der heutige Entwicklungsstand in diesem Fachgebiet. Daß wir über zivile sehr widerstandsfähige Kryptiersysteme verfügen können, ist nicht mit Zustimmung der Militärs und Geheimdienste geschehen. Sie waren bereit, das System wissenschaftlicher Öffentlichkeit auf Spiel zu setzen, um die zivile Kryptographie zu behindern. Es ist allein der Hartnäckigkeit der betroffenen Forscher zu verdanken und dem taktischen Fehler der Militärs, rasch möglichst viele Forschungsgebiete einer Kontrolle zu unterwerfen, damit aber auch eine entsprechend große Zahl von Forschern gegen sich aufzubringen.

Wie wenig Krypto ist noch möglich?

Die heutige politische Bewertung der Kryptographie ist zwar entspannter, aber keineswegs problemlos. Die Clinton-Administration kam zu ihrer durch die Clipper-Initiative[25] bekannten Position durch eine Beratung durch NSA und FBI noch vor der Amtseinführung[26]. Seither koppelt die Clinton-Administration - entgegen ihrer ansonsten sehr unternehmensnahen Wirtschaftspolitik - Kryptierung mit einer bedarfsweisen Überwachung durch staatliche Stellen. Auf der Pariser OECD-Konferenz zu Kryptierung Ende Dezember 1995 vertraten US-Abgesandte die Position, verfügbare - also exportierbare - Kryptosysteme müßten eine Entschlüsselung des von einer Person eingehenden wie ausgehenden Verkehrs ermöglichen.

Kennern asymmetrischer Kryptierverfahren wird dies deswegen verdächtig vorkommen, da die Kenntnis des privaten Schlüssels einer Zielperson nur ihren eingehenden Verkehr

[22] Mitchel B. Wallerstein: Scientific Communication and National Security in 1984; in: Science, May 4, 1984, S. 460-466
[23] John Walsh: DOD Springs Surprise on Secrecy Rules; in: Science, June 8, 1984, S. 1081
[24] James R. Ferguson: Scientific Freedom, National Security and the First Amendment; in: Science, Vol 221, S. 620
[25] Als Clipper-Initiative wird der Versuch der Clinton-Adminsitration bezeichnet, einen sog. Clipper-Chip zu entwickeln und zu verbreiten, mit dem Daten in einer Art verschlüsselt werden, durch die eine Identifikation des Urhebers und über die Clipper ausgebende Stelle dessen geheimer Schlüssel für Geheimdienste und Strafverfolger verfügbar wird.
[26] Steven Levy: Scared Bitless; in: Newsweek, June 10, 1996, S. 38-40, S. 38

lesbar macht. Erst die Kenntnis der privaten Schlüssel aller Adressaten jedoch ermöglicht das Mitlesen des *ausgegehenden* Verkehrs. Eine Überwachung hieße damit entweder eine Freigabe privater Schlüssel in großer Zahl oder die generelle Einigung auf Kryptosysteme, die schwach genug sind, um auch ohne Kenntnis der privaten Schüssel leicht brechbar zu sein.

Die Position der Bundesregierung ist seit etwa 1993 zurückhaltend. Seit dieser Zeit läßt sie sich über die Clipper-Initiative berichten und von Experten beraten, welche Probleme sie sich mit einem solchen Verfahren einhandelt. 1995 wurde dann ein Entwurf zu einer gesetzlichen Regelung einer digitalen Signatur bekannt. Dies ist ein auf einem asymmetrischen Kryptierverfahren basierendes Verfahren, bei dem ein staatliches Entschlüsseln durch die Schlüsselverwaltung durch "vertrauenswürdige Dritte" (trusted third parties) ermöglicht wird. Diese Regelung findet sich nun im Informations- und Kommunikationstechnik-Dienstegesetz (IuK-Dienstegesetz) wieder. Gleichzeitig hält sich das Gerücht, im Bundes-Innenministerium liege ein fertiger Entwurf des Verbots anderer Kryptierverfahren in der Schublade, bis sich die geeignete Situation ergebe.

Ob sich die OECD-Staaten auf eine gemeinsame Kryptierpolitik und die dazu geeignete Situation einigen können, ist ungewiß. In den USA gab der Nationale Forschungsrat NRC im Juni einen Bericht heraus, dessen Kernaussage ist, auf lange Sicht überwiegen die Vorteile einer Freigabe von Kryptoverfahren deren Nachteile[27]. Auf Clipper und Exportrestriktionen könne daher verzichtet werden.

Behinderungen

Auch heute bleibt die Kryptographie-Forschung nicht frei von Behinderungen. Zu deren interessanten Facetten gehört bezeichnenderweise das Verhindern weiterer Normungsbemühungen auf internationaler Ebene. Der Sinn ist, die Etablierung eines neuen einheitlichen Systems so lange wie möglich zu behindern, da derzeit nicht mit der Etablierung eines "Industriestandards" zu rechnen ist.

Schon beim DES hatte sich die NSA lange Zeit geweigert, Softwarelösungen des DES zu zertifizieren. Der Grund war die Furcht, softwaregestützte Systeme könnten leicht modifiziert werden, um längere Schlüssel zu nutzen. Der NSA wurde nachgesagt, DES mit vier Cray 1 in weniger als einem Tag brechen zu können[28]. Jede Verlängerung des Schlüssels würde dies behindern.

Heute geht es um die Bemühungen der internationalen Standardisierungsorganisation ISO, Normen für Kryptosysteme zu entwickeln. Aussagen Beteiligter zufolge hat die ISO

[27] NRC: Cryptography's Role in Securing the Information Society, Washington, June 1996
[28] C.A. Devours: The Black Chamber; in: Cryptologhia, Jan 1981, S. 43-45, S. 44

ihren Technical Committees die Normung von Kryptieralgorithmen verboten. Während die Bundesregierung jegliche Einflußnahme abstreitet[29], berichten Insider, daß sie wie auch andere Regierungen erheblichen Druck auf die ISO ausgeübt hat. Damit wurde jedoch die Verbreitung eines Kryptier-Programms wie PGP keineswegs aufgehalten, sondern eher befördert.

Fazit

Die verbreitete Nutzung von Kryptiersystemen steht einerseits den militärischen Zielen bei der Umstellung der Atomaren Abschreckung auf die durch Information Warfare und andererseits den Aufgaben der Geheimdienste in diametraler Weise entgegen. Die bisher als praktisch empfundene übersichtliche Aufteilung des Marktes für Kryptiersysteme gerät ins Wanken durch Entwicklungen auf wissenschaftlichem Gebiet. Dabei ist es Chiffrier-Geheimdiensten trotz erheblicher Anstrengungen nicht gelungen, die Publikation des Erkenntniszuwachses zu verhindern. Erfolge wurden von ihnen allenfalls durch ein Verlangsamen der Verbreitung von Kryptiersystemen erzielt.

Die Regierungen der OECD-Staaten und vor allem ihre Geheimdienste sehen sich nun vor einer Zäsur. Ihre internationalen Abstimmungsbemühungen sind vorerst gescheitert. Die von ihnen forcierte Entwicklung der Informationsgesellschaft benötigt dringend die verbreitete Nutzung von Chiffriersystemen zum Schutz der Kommunikation und zur digitalen Signatur. Bisher hat sich jeder Versuch, sichere, aber brechbare Chiffriersysteme zu verbreiten, als undurchführbar erwiesen. Die nächsten Monate werden zeigen, ob einige dieser Staaten nicht nur neue Chiffriersysteme wie die digitale Signatur einführen, sondern damit auch Verbote anderer Systeme durchzusetzen versuchen und wie Öffentlichkeit und Unternehmen darauf reagieren. Damit wird sich auch entscheiden, ob sich die Informationsgesellschaft als eine Zivilgesellschaft entwickelt oder nicht.

[29] vgl. Antwort der Bundesregierung auf die Kleine Anfrage "Sicherheit der Informationstechnik und Kryptierung", Drs. 13/4105, Frage 11