Die ersten Jahrzehnte der Public-Key-Cryptography

Über die widersprüchliche Durchsetzung der kryptologischen Erfindungen neuer Richtung

von Lambert Heller

2. Oktober 2003

Inhaltsverzeichnis

Einleitung

> „He must have said something wrong. One of the agents threatened to run him over in the parking lot, Bidzos said.
> 'He looked at me and very coldly said he would do me in,' Bidzos said. 'He clearly threatened me.'"[1]

Im Juni 1994 bekam Jim Bidzos, Chef des Privatunternehmens RSA Data Security, Inc., überraschend Besuch an seinem Arbeitsplatz. Vor seiner Tür standen drei Herren in Zivil, Agenten des US-Militärnachrichtendienstes National Security Agency (NSA).[2] Jim Bidzos wird selten überrascht – er überrascht vielmehr andere. Als aggressiver Verkäufer machte er im Laufe der neunziger Jahre praktisch allen großen Softwareunternehmen der Welt klar, dass sie eine Lizenz für sein Produkt benötigen, die RSA-Verschlüsselungstechnik. Die neue Verschlüsselungstechnik war revolutionär und einfach unwiderstehlich, und Bidzos wusste das an den Mann zu bringen. Heute ist RSA in jedem PC-Betriebssystem fest eingebaut – ob die Benutzer der PCs das nun wissen und RSA benutzen oder nicht. Man kann sich rasch davon überzeugen, indem man die eigene Festplatte nach Dateien mit „RSA" im Namen durchsucht – die meisten der so gefundenen Dateien enthalten vermutlich die von Bidzos und seinen Leuten damals lizensierte Verschlüsselungstechnik. Die RSA-Aktie wäre für Anleger in den neunziger Jahren ein ertragreicher Tipp gewesen; der Kurs der Firma explodierte förmlich. Aber an anderer Stelle konnte keine Freude aufkommen über diese sensationellen Erfolge. Nachrichtendienste wie die NSA hatten jahrzehntelang quasi ein Monopol auf gute Verschlüsselungstechniken gehabt. Was neu war und sich von niemandem knacken ließ, hatten nur die NSA und ihresgleichen gewusst; alles andere, was es an Verschlüsselung gegeben hatte, hatten *sie* hingegen knacken können. Die drei Herren in Bidzos Büro taten nun ihr Bestes, diese guten alten Zeiten zu verteidigen. Zwei Stunden lang wurde diskutiert, erklärt und gescherzt – Bidzos hätte einfach einsehen sollen, dass im Dienste der nationalen Sicherheit nun eine Rückrufaktion fällig war, dass es besser

---

1 David Bank: The Keys to the Kingdom – the government wants to be able to see private computer communications. San Jose Mercury News 27. Juni 1994 ⟨URL: `http://www.interesting-people.org/archives/interesting-people/199406/msg00078.html`⟩ – Zugriff am 3.4.2003.

2 Zu den Abkürzungen und Fachbegriffen siehe das Glossar am Ende des Textes.

wäre, Verschlüsselungstechniken wie RSA gänzlich zu verbieten, und dass es besser für alle wäre, wenn stattdessen die NSA Verschlüsselungsverfahren ausgäbe, die niemand knacken könnte – außer ihr selbst.

Ausgangspunkt dieser Arbeit ist eine Erfindung aus dem Jahr 1976, die dem RSA-Verschlüsselungssystem zugrunde liegt. Bei dieser Erfindung handelt es sich um die sogenannte Public-Key-Cryptography (PKC). PKC unterscheidet sich von allen vorangegangenen Verschlüsselungsverfahren darin, dass der Schlüssel hier stets aus zwei Teilen besteht. Mit dem einen, öffentlichen Teil kann eine Nachricht verschlüsselt werden, mit dem dazugehörigen anderen, geheimen Teil entschlüsselt. Wenn jemand eine Nachricht mit dem öffentlichen Schlüsselteil seines Kommunikationspartners verschlüsselt, kann also nur dieser die Nachricht wieder entschlüsseln, ohne dass die beiden insgeheim vorher einen gemeinsamen geheimen Schlüssel hätten verabreden müssen. Man spricht in diesem Zusammenhang auch von asymmetrischer Verschlüsselung, im Gegensatz zur symmetrischen Verschlüsselung bei allen vorangegangenen kryptographischen Systemen.[3] Diese Technologie lässt zum Beispiel eine spontane und dennoch abhörsichere Kommunikation zwischen Menschen zu, die sich nicht einmal persönlich zu kennen brauchen. Und mit derselben Technik ist noch mehr möglich: Elektronische Unterschriften, sogenannte digitale Signaturen, die noch fälschungssicherer sein können als Unterschriften von Hand. Angesichts dieser Potentiale sprachen die Erfinder der PKC im Titel ihres epochalen Aufsatzes von einer Kryptographie *neuer Richtung*.[4] Kryptographie, zuvor jahrzehntelang fast ausschließlich in den streng funktionalen, hierarchischen, abgeschotteten Kommunikationsnetzen der Regierungen, Militärs und Geheimdienste beheimatet, war auf einmal Mittel der Massenkommunikation geworden.

---

3 Eine ausführliche, leicht verständliche Einleitung in die den asymmetrischen Verschlüsselungsalgorithmen zugrundeliegende Mathematik in deutscher Sprache bietet Simon Singh: Geheime Botschaften. München, Wien, deutsch 2000, S. 311 ff; eine kompakte Darstellung auf dem Niveau der avancierten Kryptologie findet sich in Alfred J. Menezes, Paul C. van Oorschot und Scott A. Vanstone: Handbook of Applied Cryptography. Boca Raton, 1996 ⟨URL: `http://www.cacr.math.uwaterloo.ca/hac/`⟩ – Zugriff am 1.5.2003, S. 283 ff.

4 Wenn in dieser Arbeit von Kryptographie *neuer Richtung* die Rede ist, bezieht sich dies auf den Titel des Aufsatzes Whitfield Diffie und Martin E. Hellman: New Directions in Cryptography. IEEE Transactions on Information Theory IT-22 1976, Nr. 6 ⟨URL: `http://www.cs.rutgers.edu/~tdnguyen/classes/cs671/presentations/Arvind-NEWDIRS.pdf`⟩ – Zugriff am 1.5.2003; vgl. die nähere Diskussion der Erfindung und des Aufsatzes in 2.3 und 2.4.

Aber was hatte die NSA soweit gebracht, ausgerechnet dem Chef des aufstrebenden jungen Unternehmens RSA Data Security, Inc. damit zu drohen, ihn draußen auf dem Firmenparkplatz umzulegen? – Heute, zehn Jahre später, hat sich der politische Streit über die Nutzung von Kryptosystemen wie RSA so weit beruhigt, dass eine ähnliche Szene kaum noch vorstellbar wäre. Ist Geheimdiensten wie der NSA damit die Führungsrolle genommen worden, nicht nur als Kryptologen, sondern auch als Abhörern? Immerhin hatten sich die Erfinder der Public-Key-Cryptography vorgestellt, dass ihre Erfindung geradezu zwangsläufig in die Technik der Massenkommunikationsmittel Eingang finden werde – und sich dort nicht zuletzt bewähren werde als wirksamer technischer Schutz der privaten Individualkommunikation vor Überwachung. Wäre dies mit der Public-Key-Cryptography geschehen, wäre also die Wirklichkeit ihrer Anwendung identisch mit der Intention ihrer Erfinder, dann hätte die vorliegende Arbeit nicht geschrieben zu werden brauchen. Als so unproblematisch erscheint die Technik der asymmetrischen Verschlüsselung nur, wenn sie in einem der Lehrbücher für angewandte Mathematik, Kryptologie oder Informatik erklärt wird oder in den zahlreichen und auflagenstarken Handbüchern über Computer, Programme oder deren Anwendungsbereiche. Über ihre Funktionsweise hinaus werden dann vielleicht noch die Namen ihrer Erfinder, Diffie und Hellman, bzw. die Namensgeber des RSA-Verschlüsselungsalgorithmus, Rivest, Shamir und Adleman, und der Zeitpunkt der Erfindung, 1976 bzw. 1978, erwähnt. Und wenn es hoch kommt, werden die praktischen Hindernisse erwähnt, die dem Einsatz der Technik hier und da noch entgegenstehen, export- oder patentrechtliche Restriktionen.

Daneben gibt es einen seit den sechziger Jahren dahinrieselnden, in den neunziger Jahren dann anschwellenden Strom meist populärer, explizit kryptologiehistorischer Literatur. Diese erzählt die Erfindung des asymmetrischen Verschlüsselns als die Durchsetzung einer zunächst randständigen Idee gegen vielfältige Widerstände, gegen die ihre Erfinder als ungebrochene Sieger dastehen. Die Namensgebung von Steven Levys Werk über die Geschichte der Kryptographie neuer Richtung lässt keinen Zweifel darüber aufkommen, dass hier eine Erfolgsgeschichte zu erzählen ist.[5]

---

5 Steven Levy: Crypto. how the code rebels beat the government, saving privacy in the digital age. New York, 2001 – trotz des problematischen Titels handelt es sich um die einzige Mono-

Dieser Sieg wird von denjenigen, die schon immer für die Freiheit des individuellen Kryptographiegebrauch eintraten, ähnlich interpretiert wie von ordnungspolitischen Hardlinern, die diese Freiheit eingeschränkt sehen wollten durch die staatliche Aufsicht über die Massenkommunikation. Die eine Seite mag es freuen, die andere auch ein wenig bedauern, aber einig ist man sich darin, dass der Streit faktisch weitgehend für die eine Seite entschieden sei. Als offensichtlicher Beweis dafür gelten zwei unübersehbare neue Sachverhalte, die auf dem Schlachtfeld der Kryptographiedebatte übriggeblieben sind: Erstens die durchgesetzte öffentliche Verfügbarkeit neuartiger, starker kryptographischer Technologie und zweitens die massenhafter Nutzung bestimmter Kryptographieanwendungen. Wie der RSA-Verschlüsselungsalgorithmus funktioniert, ist in Fachbüchern nachzulesen, die in jeder Universitätsbibliothek öffentlich zugänglich sind; und auf der Festplatte jedes PCs ist der Algorithmus unmittelbar einsatzbereit.
Auch für die Deutung dieses Sieges hat man übereinstimmend eine Idee ausfindig gemacht, die es im politik- und sozialwissenschaftlichen Diskurs bereits anderweitig zu großer Beliebtheit gebracht hat. Der Sieg gilt als Fall des Bedeutungsverlustes der Nationalstaaten. „On the Information Highway, borders are just speed bumps“,[6] heisst es etwa bei Levy. Auch in der deutschen Fachöffentlichkeit wird so geurteilt:

> „[Solange] Cyberspace nationale Grenzen überwindet, die Verschlüsselung jedoch unüberwindbar ist, kann ein nationales elektronisches Vermummungsverbot schon gar nicht wirksam durchgesetzt werden.“[7]

In dieser Arbeit soll mit Gründen bezweifelt werden, dass die öffentliche Zugänglichkeit und massenhafte Nutzung von Kryptographie in ihrer derzeitigen gesellschaftlichen Gestalt tatsächlich die Sachlage weitgehend zugunsten einer Seite geklärt hat und dass dies exemplarischer Ausdruck des Bedeutungsverlustes der Nationalstaaten sei. Das asymmetrische Verschlüsseln hat in der Tat einen Siegeszug hinter sich – aber der lässt sich auch anders interpretieren. Diese Technologie, so die These meiner Arbeit, ist umfassend in den Dienst des nationalen Interesses gestellt worden. Wie das passierte und wie das Ergebnis aussieht soll in dieser

---

graphie, in der speziell die Geschichte der kryptologischen Innovationen neuer Richtung bis in die Ära der kryptopolitischen Liberalisierung behandelt wird.

6 Levy: Crypto. beat, S. 198.

7 Franz C. Mayer: Recht und Cyberspace. Neue Juristische Wochenschrift 1996, S. 1786.

Arbeit gezeigt werden. Vor allem jedoch soll gezeigt werden, wie sich im Verlauf dieser gesellschaftlichen Subsumtion der Public-Key-Cryptography herausgestellt hat, dass sich das nationale Interesse an ihr weitestgehend ausschließt mit dem individuellen Interesse daran, nicht abgehört oder anderweitig beaufsichtigt zu werden. Die Subsumtion der PKC unter das nationale Interesse fand in den USA früher und deutlicher statt als in allen anderen Ländern. Daher wird es manchmal nötig sein, besondere Entwicklungen in den USA auszuführen, um daran Allgemeines zu verdeutlichen; sachlich relevante Sonderentwicklungen in anderen Nationen werden jedoch keineswegs unterschlagen. Im Gegenteil, ausführliche Darstellungen zur Entwicklung des Umgangs mit der Kryptographie insbesondere in Deutschland und der EU sind notwendig, um die Ausrichtung des nationalen Interesses an der Standortkonkurrenz zu verdeutlichen, die je nach den unterschiedlichen Ausgangsbedingungen dieser Konkurrenz auch unterschiedliche Formen und Wege annimmt. In allen Industriestaaten wird PKC heute auf mannigfaltige Weise massenhaft genutzt. Stellen, an denen die Bürger solcher Länder im Alltag mit RSA und ähnlichen Algorithmen in Berührung kommen sind zum Beispiel Set-Top-Boxen für digitales Pay-TV und Spielekonsolen wie die Microsoft Xbox,[8] PC-Betriebssysteme wie Linux oder Windows XP und praktisch alle Internet-Browser, der Datenverkehr zwischen den Banken und zunehmend auch das Home Banking.[9] Im letztgenannten Bereich steht in Deutschland jetzt die massenhafte Verbreitung einer weiteren Anwendung bevor, die den Einsatzbereich der kryptographischen Erfindungen neuer Richtung spektakulär erweitern könnte: Die Spitzenverbände der deutschen Kreditwirtschaft bereiten die Herausgabe einer digitalen Signatur-Chipkarte für das

8 Der Bereich, in dem hier PKC zum Einsatz kommt, das Digital-Rights-Management (DRM), wird meistens einfach weggelassen, wenn die heute angewandte Kryptographie als solche diskutiert wird. Exemplarisch hierfür die komplette Weglassung des Thema DRM in verschiedenen ansonsten guten und aktuellen Überblicken zur angewandten Kryptographie. Vgl. Klaus Schmeh: Kryptografie und Public-Key-Infrastrukturen im Internet. 2. Auflage. Heidelberg, 2001, S. XV ff. und Reinhard Wobst: Abenteuer Kryptologie. Methoden, Risiken und Nutzen der Datenverschlüsselung. 3. Auflage. München, 2001, S. 5 ff. DRM als großer neuer Anwendungsbereich der Kryptographie lässt sich im engen Rahmen dieser Arbeit leider nicht angemessen diskutieren.

9 Einen beeindruckenden Versuch, viele weitere Anwendungsbereiche aufzuzählen, unternimmt Ross J. Anderson: Crypto in Europe – Markets, Law and Policy. Juli 1995 ⟨URL: `http://www.cl.cam.ac.uk/ftp/users/rja14/queensland.pdf`⟩ – Zugriff am 3.4.2003, S. 2 ff.

Homebanking.[10] Die digitale Signatur gilt als Anwendung im Schnittbereich von einerseits E-Commerce und andererseits E-Government.[11]
In welche Anwendungen asymmetrische Verschlüsselung und digitale Signatur implementiert worden sind, und wie diese Anwendungen große und wichtige informationstechnische Infrastrukturen ermöglicht und geprägt haben, wird in dieser Arbeit umrissen. Dabei muss in jedem Fall zwischen drei Ebenen differenziert werden:

1. Die Ebene der kryptographischen *Algorithmen* (zum Beispiel das PKC-Verschlüsselungsverfahren RSA)[12], und, allgemeiner, *Protokolle* (zum Beispiel Public-Key-Verschlüsselung nach dem PGP-Standard)[13], sowie

2. Die Ebene der *Anwendungen* im engeren Sinne von Einbettung der Algorithmen und Protokolle in Geräte und Computerprogramme (zum Beispiel das PC-Verschlüsselungsprogramm PGP).

3. Die Gestalt der *Nutzung* dieser Anwendungen (zum Beispiel PGP-verschlüsselte E-Mail-Kommunikation in einem Unternehmen, in dem stets alle geheimen Schlüssel bei der Geschäftsleitung hinterlegt sind).

Technisch ist jede Ebene in der darauffolgenden Ebene vorausgesetzt. Umgekehrt kann die Bedeutung kryptographischer Algorithmen und Anwendungen für Individuum und Gesellschaft nur in Hinblick auf die konkrete Gestalt ihrer Nutzung beurteilt werden. Erst von der Gestalt der realen Nutzung her können die technologischen Voraussetzungen als Determinanten oder Potentiale der Nutzung in die Beurteilung miteinbezogen werden.
Die Arbeit geht ungefähr chronologisch vor:

---

10 Auf den elektronischen Zahlungverkehr wird in dieser Arbeit nicht näher eingegangen; verschiedene Gestalten und die Entwicklung elektronischer Zahlungsweisen sind Gegenstand eingehender soziologischer Untersuchung in Arnd Weber: Soziale Alternativen in Zahlungsnetzen. Frankfurt/Main, New York, 1997.

11 Das Thema E-Government wird in dieser Arbeit unter 6.3 gestreift; ausführlich ist es Gegenstand kritischer Untersuchung bei Christoph Engemann: Electronic Government – vom User zum Bürger. Zur kritischen Theorie des Internet. Bielefeld, 2003.

12 Benannt nach seinen Erfindern Rivest, Shamir und Adleman; näheres hierzu unter 2.3. und 2.4.

13 Pretty Good Privacy; näheres hierzu in 4.

Im ersten Kapitel soll – neben einigen Grundlagen der Kryptologie – aufgezeigt werden, dass es vor dem Zeitalter der modernen Nationalstaaten Kryptologie gab und diese bereits wesentlich von den Interessen hoheitlicher Machtentfaltung angetrieben wurde. Ereignisse wie vor allem der Zweite Weltkrieg veränderten jedoch die Haltung der Staaten zur Entwicklung und Anwendung von Kryptologie entscheidend. Statt den diplomatischen Nachrichtenverkehr der Gegner nach kaum mehr als gelegentlichen Bereicherungsmöglichkeiten zu durchsuchen, und die Gefahr des Ausgespähtwerdens durch den Gegner gleichzeitig stets zu unterschätzen, wurde die Kryptologie nun erstmals systematisch weiterentwickelt, für die eigenen Zwecke – zum Beispiel im großen Maßstab an der Front – eingesetzt, jedoch vor der eigenen Bevölkerung weitestgehend geheimgehalten.
Im zweiten Kapitel soll gezeigt werden, wie unter den Bedingungen der sich rasch entwickelnden Computer- und Netzwerktechnologie in den siebziger Jahren die Kryptographie – als Public-Key-Cryptography – neu erfunden wurde, nämlich als ein Mittel der digitalisierten Massenkommunikation. Die Erfinder sahen zwei Anwendungsspektren dieser neuen Technologie, den Schutz der privaten Individualkommunikation vor dem Abhören durch Dritte sowie einen möglichen zukünftigen E-Commerce. In diesem Stadium wurde die Erfindung vom US-Militärnachrichtendienst NSA total abgelehnt und dementsprechend behindert.
Im dritten Kapitel werden die achtziger Jahre als eine bleierne Zeit für die Verbreitung der Public-Key-Cryptography geschildert. Auf der einen Seite „zieht der PC zu Hause ein“ und steigert permanent seine Rechenleistung, bieten erste Computerprogramme fürs Büro integrierte asymmetrische Verschlüsselungsalgorithmen, zeigen weitere kryptographische Entwicklungen, wie sich die PKC auch zur Anonymisierung von Kommunikation und Zahlungsvorgängen nutzen ließe. Auf der anderen Seite lähmt ein scharfer Dissens zwischen Behörden des US-Handelsministeriums einerseits und des US-Militärs andererseits die reale Verbreitung und Nutzung der kryptographischen Innovationen. Ein modellhafter US-Gesetzgebungsakt über das Abhören elektronischer Individualkommunikation lässt allerdings bereits eine Prämisse jeder späteren Regulation dieses Bereichs nicht nur in den USA erkennen: Während die Individuen sich zwar nicht gegenseitig sollen abhören können, sollen Strafverfolger und Geheimdienste weiterhin die Bürger sowie Firmen ihre Angestellten abhören dürfen.

Im vierten Kapitel geht es vor allem darum, wie zu Beginn der neunziger Jahre der Impuls der Erfinder der PKC, die individuelle Privatsphäre schützen zu wollen, aufgegriffen wird. Vor allem Phil Zimmermann, der Erfinder des Verschlüsselungsprogramms PGP sowie die libertäre Bürgerrechtsbewegung der Cypherpunks, die rasch zur Avantgarde einer liberalen öffentlichen Meinung zu diesem Thema wird, versuchen den Schutz der Privatsphäre durch Technik praktisch voranzutreiben und als Wahrnehmung eines Rechts zu politisieren. Erfindungen wie PGP und das World Wide Web scheinen die Voraussetzung zu schaffen für einen vernetzten Umgang der Einzelnen mit Informationen, ohne jegliche zentrale Kontrollinstanz. Dem steht aber ein neuerdings harmonisches Vorgehen staatlicher Agenturen gegen einen allzu freien Gebrauch von Kryptographie gegenüber: Dieser soll nun zwar nicht mehr total verhindert werden, aber der Zugriff der Regierung auf alle verwendeten Schlüssel soll technisch garantiert werden.
Das fünfte Kapitel beginnt mit dem Boom der Kryptographieanwendungen ab 1994, einem Vorboten des E-Commerce. Es wird die These aufgestellt, dass staatliches Handeln mittelbar immer schon Voraussetzung für die Entstehung eines E-Commerce war – und es wird gefragt, wie und warum unter der Maxime der Standortpolitik der Einsatz der kryptographischen Innovationen zum staatlichen Programm geworden ist. Dieser Interpretationsversuch der schlagartigen kryptopolitischen Liberalisierung in den späten neunziger Jahren wird um eine eingehende Beschäftigung mit dem Sonderfall des Standortes Deutschland und der EU ergänzt, die gleichsam eine nachholende Entwicklung in Sachen Kryptographie neuer Richtung zurück zu legen hatten.
Ende der neunziger Jahre konnte man tatsächlich von einer massenhaften Anwendung der neuartigen kryptographischen Algorithmen und Protokolle durch die Bürger sprechen. Im sechsten Kapitel soll anhand von Modellen gezeigt werden, inwiefern die Fortentwicklung der Kryptographie, die Entwicklung von Anwendungen und Geräten sowie deren massenhafte Nutzung nun dem nationalen Interesse untergeordnet ist. Ferner sollen Gründe und Verlauf der Kryptoliberalisierung daraufhin untersucht werden, inwiefern diese für das inviduelle Interessse daran, nicht abgehört zu werden, nur bedingt und begrenzt ein Erfolg war, exemplarisch anhand des Zusammenhangs von nationalen Abhörvorschriften und Digitaltelefonie sowie der Wirkung der Krypto-Exportkontrollen nach dem Wassenaar Arrange-

ment. Danach wird anhand der digitalen Signatur die Kryptographie als ein Mittel untersucht, das in die Pflege kapitalistischer Geschäftsinteressen eingebunden ist. Wer in Kriminalromanen grundsätzlich die letzten zehn Seiten zuerst ließt um die Spannung besser zu ertragen, sollte diese Arbeit mit dem siebten Kapitel beginnen. In diesem Resümee liegt der Schwerpunkt auf der Konstellation des nationalen Interesses, nachdem die Subsumtion der kryptologischen Erfindungen neuer Richtung vollzogen war.

1 Kryptologie: Anfänge und Grundlagen

1.1 Kryptologie als Instrument hoheitlicher Machtausübung

Wer hat mit dem Verschlüsseln angefangen, und warum? Oft wird behauptet, dass die Kryptologie sich für den gesamten Zeitraum der Menschheitsgeschichte nachweisen lässt, der schriftlich bezeugt werden kann. Einen präziseren Eindruck vermittelt bereits, dass in der Geschichtsschreibung der Kryptologie vor allem von der Geschichte des Nachrichtenwesens im Kriege und in der Diplomatie die Rede ist. Die oben gestellte Frage lässt sich jedoch noch genauer beantworten: Die Kryptologie war bis Mitte des 19. Jahrhunderts. ein hoheitlich gehandhabtes Werkzeug, und hatte auch noch bis weit in die Zeit nach dem Zweiten Weltkrieg ihren Hauptantrieb in ihrem unmittelbaren Gebrauch durch die Nationalstaaten. Das lässt sich exemplarisch darlegen an der Biographie des schwedischen Kryptographiegeräte-Herstellers Boris Hagelin.

Sein Vater, K.W. Hagelin, war Manager eines Ölunternehmens und zeitweilig schwedischer Generalkonsul in St. Petersburg. Die kurz zuvor von ihm mitgegründete Aktiebolaget Cryptograph meldete 1916 einen neuen Typ handlicher Kryptographiemaschinen zum Patent an. Die Maschine erzeugt aus jedem eingetippten Klartext direkt eine chiffrierte Ausgabe, die dann per Funk weitergegeben wird. Dass 1925 ein Verkauf an interessierte Radiounternehmen scheiterte, lag nicht zuletzt an technischen Mängeln in einer der ersten Versionen des neuen Produkts – jedenfalls war es um das väterliche Geschäft nicht gut bestellt als es von Boris Hagelin nach abgeschlossenem Ingenieursstudium 1922 übernommen wurde. Der junge Hagelin war technisch sehr ambitioniert; als Hauptentwickler seiner eigenen Firma verbesserte er permanent das Konzept der Geräte. 1935 kam der Wende-

punkt in der Firmengeschichte, als die französische Armee 5.000 Exemplare einer verbesserten Geräteversion bestellte. David Kahn, dessen Werk *The Codebreakers* als der Klassiker der Kryptologiegeschichtsschreibung gilt, schreibt:

> „Looking back, Hagelin realized that [...] the other cipher machine companies had not failed because of any intrinsic flaws in their machines, but only because the time was not ripe for them in the 1920s. Not until the war-weariness of that decade had worn off and the rearmament of the 1930s had begun did a substantial market appear.“[14]

1937 bemerkt Hagelin, dass er das Geschäft seines Lebens mit der US-Armee abschließen kann. Nach mehreren Besuchen unter teils schwierigen Bedingungen kann er die amerikanischen Fachleute davon überzeugen, die Armee massenhaft mit seiner Hardware auszustatten. 1942 nimmt die L.C. Smith & Corona Tipewriters, Inc. eine bis dato beispiellose Massenproduktion der Hagelinschen Maschine auf. Ironischerweise, so bemerkt Kahn, werden ein Teil der insgesamt 140.000 produzierten Stück an die italienische Seestreitmacht verkauft. Noch vor Kriegsende ist Hagelin Junior Multimillionär.

> „‘With my earnings,’ [Hagelin] said, ‘I bought myself a 2.000-acre estate with a brick factory 30 miles south of Stockholm, outside Södertäge, as I thought that the cipher machine business was finished.’ How wrong he was! First came the cold war. As the two great powers built up their military might and those of their satellites in mutual fear and mistrust, a new market came into being for cipher machines. Then the old colonial empires broke up. The dozens of new nations that emerged from the ruins created a market for cipher machines far wider than any that had yet existed.“[15]

Der Einschätzung in Kahns Buch von 1967 zufolge hatte bis zum damaligen Zeitpunkt niemand einen größeren kommerziellen Erfolg mit der Kryptologie erzielt als Hagelin. Der Markt, auf dem sich dieser Erfolg erzielen ließ, war stets vor allem das Geschäft mit Nationen, die Kriege führen oder vorbereiten. Der Zweite Weltkrieg brachte diesen Markt erst zum Boomen, aber wie man sieht hatte Hagelin auch danach keinen Grund, seine Firma aufzulösen.

---

14 David Kahn: The Codebreakers. The Story of Secret Writing. New York, 1967, S. 426.

15 A. a. O., S. 432.

Die Behauptung, man habe verschlüsselt seit es unverschlüsselte Schriftzeichen gab, ist also zumindest ungeeignet, das doch sehr viel genauer angebbare Interesse an der Kryptologie zu erklären. Dennoch ist die Behauptung richtig in der Hinsicht auf die zeitliche Ausdehnung der Geschichte der Kryptologie. Daher soll im Folgenden umrissen werden, wovon die kryptologische Entwicklung angetrieben wurde, bevor das Zeitalter der modernen Nationalstaaten anbrach. Außerdem sollen einige kryptologische Grundbegriffe eingeführt werden.

1.2 Grundbegriffe und Einheit der Kryptologie

Als Beispiel für die 'alte' Kryptographie mag das Cäsar-Verschlüsselungsverfahren dienen, das in der kryptologischen Sekundärliteratur, wohl aufgrund seiner Überschaubarkeit, immer wieder als Urmodell kryptographischer Verfahren herhalten muss.[16]
Einem Boten wird eine Nachricht mit auf den Weg gegeben, die weder er selbst noch ein unbefugter Dritter unterwegs soll lesen können. Im Klartext soll diese Nachricht aus Buchstaben des lateinischen Alphabets bestehen. Zunächst wird Buchstabe für Buchstabe nach einem vorher zwischen Sender und Adressat vereinbarten Verfahren ersetzt. Dabei wird so vorgegangen, dass jeder Buchstabe durch denjenigen Buchstaben ersetzt wird, der ihm im Alphabet um drei Stellen folgt. Hieße der Klartext (*Plaintext*) beispielsweise

HALLO,

dann lautete der verschlüsselte Text (*Ciphertext*)

KDOOR.

Das verwendete Verschlüsselungsverfahren (*Cipher*) wäre die einmalige Ersetzung jedes Einzelbuchstabens durch einen Buchstaben, der ihm in gegebenem Abstand im Alphabet folgt, und der Schlüssel (*Code* oder *Key*) lautete drei, also die Zahl der Stellenverschiebung, die beim Ersetzen der Buchstaben verwendet wird.
Nun ließe sich dieses antike Verfahren der *monalphabetischen Substitution*, egal welcher Schlüssel verwendet wird, rasch von jedem brechen, der einigermaßen mit

16 Etwa in Schmeh, S. 54 f., welches zugleich Hauptquelle der Darstellungen dieses Abschnitts ist.

Schriftzeichen und Alphabet vertraut ist, selbst wenn er vorher keine Methode zum Brechen von Schlüsseln gekannt hat. Aber dennoch können alle komplexeren Verschlüsselungsverfahren als Erweiterungen dieses einen Verfahrens dargestellt werden. Immer besteht die Verschlüsselung darin, regelgesteuert Zeichen durch andere zu ersetzen oder Zeichen(gruppen) innerhalb des Klartext miteinander zu vertauschen. Meistens werden beide Verfahren in mehreren Runden hintereinander durchgeführt, und die verwendeten Regeln sind natürlich meistens komplizierter als beim Cäsar-Cipher. Doch was sind und wie kommt man auf 'gute' kryptographische Verfahren?

Kryptologie wird als die Einheit von *Kryptographie*, der Verschlüsselungslehre, und *Kryptanalyse*, dem Auffinden von Mängeln in Verschlüsselungsverfahren, bestimmt. Oft werden die Begriffe Kryptologie und Kryptographie allerdings auch synonym verwendet. Die Kryptanalyse muss als ein notwendiger Teil der Kryptologie als Ganzer aufgefasst werden. Das wird bei näherer Betrachtung des einzigen beweisbar sicheren Verschlüsselungsverfahrens klar. Hierbei handelt es sich um den One-Time-Pad (OTP), das heisst die einmalige Verschlüsselung eines Klartexts mit einer Reihe echter Zufallszahlen in der Länge des zu verschlüsselnden Texts. Es handelt sich beim OTP also um ein symmetrisches Verfahren, das prinzipiell als praktikabel gilt, zugleich jedoch für viele Kryptographieanwendungen im Alltag als ökonomisch ungeeignet. Der Aufwand, lange Zufallsreihen zu erstellen, sicher zu transportieren und aufzubewahren ist relativ hoch.[17] Jenseits des nur begrenzt nützlichen OTP kann es keine im strengen Sinne systematische Kryptographieentwicklung geben, sondern 'nur' den Zyklus, gute Einfälle zu haben, sie dem Versuch der Brechung auszusetzen, danach die Einfälle zu variieren oder zu verwerfen und von vorn anzufangen. Dieses Trial-and-Error-Spiel ist jedoch keine triviale Aufgabe. Vielmehr ist es nahezu ausgeschlossen, durch bloßes Drauflosprobieren, ohne kryptologische Vorkenntnisse, ein schwer zu knackendes Verschlüsselungsverfahren zu erfinden. Kryptologen schöpfen aus der reichhaltigen historischen Erfahrung mit unterschiedlichen Gestaltungsmerkmalen kryptographischer Verfahren. Auch die Methoden, kryptographische Verfahren auf Schwächen zu analysieren, sind entsprechend ausgefeilt.

17 Wobst, S. 60 ff.

Die Unverzichtbarkeit der Kryptanalyse ist in bis heute gültiger Form von Auguste Kerckhoffs von Nieuwenhof 1882 in seinem Aufsatz *La Cryptographie militaire* postuliert worden: Ohne methodisch ausgefeilte Versuche des Code-Brechens keine sichere Codierung.[18] Kerckhoffs, professioneller Kryptologe im Dienste der Grande Armée, ist der Wegbereiter der modernen Kryptologie. Er stellte hellsichtig klar, inwieweit die massenhafte Implementierung von Kryptographie in Geräte für den Gebrauch im Feld eine bedeutende Prämisse jeder künftigen Kryptologie sein wird. Die Anwendung müsse kompatibel zum technischen Kommunikationsmittel sein (zu Kerckhoffs' Zeit also zum Telegraphen); sie müsse einfach und auch durch Einzelne handhabbar sein; der Gebrauch verschiedener Schlüssel für die Kommunikation mit jeweils unterschiedlichen Partnern müsse möglich sein; vor allem jedoch dürfe die Sicherheit der Anwendungen nicht mehr von der Geheimhaltung der verwendeten Protokolle und Algorithmen abhängen.[19] Seine hohen und klar formulierten Anforderungen an die Implementierung der Algorithmen und Protokolle scheinen vom heutigen Stand der Geschichte aus betrachtet eine Vorbereitung der Kryptologie darauf zu sein, dass ein Jahrhundert später massenhaft verfügbare Universalrechenmaschinen in der Hand Einzelner, moderne Computer also, ihr eigentliches Medium sein würden. Zugleich ging mit diesen Anforderungen aber auch eine Schärfung des Blicks für das einher, was als Kerntätigkeit der kryptologischen Entwicklung bleibt, soweit man von allen Problemen der Einbettung in zuverlässige Anwendungen abstrahiert. Diese methodische Reduktion auf das kryptographisch Notwendige, den Cipher, dessen Unbrechbarkeit allgemeinen und bekannten Kriterien zu genügen hat, gibt der Kryptograhieentwicklung jene Fassung, in der sie neunzig Jahre später ihre großen Innovationen feiern konnte.

1.3 Die 'Geheimen Kabinettskanzleien'

Zwischen dem 17. und der Mitte des 19. Jahrhunderts war es ein offenes Geheimnis, dass die Könige und Fürsten der großen europäischen Höfe systematisch die Post auswärtiger Diplomaten am Hofe in Geheimen Kabinettskanzleien mitlesen und auswerten ließen. Da diese Post regelmäßig kryptographisch verschlüsselt

18 Hier wiedergegeben nach Kahn, S. 234 f.

19 Diffie und Hellman, S. 39.

war, gehörte das Brechen von Verschlüsselungsverfahren notwendigerweise zum Geschäft der Geheimen Kabinettskanzleien. Hatte die Nutzung der Kryptologie zuvor fast ausschließlich davon abgehangen, ob Einzelne Interesse und Talent für sie entwickelten und damit ihren lokalen Fürsten oder Königen einen Konkurrenzvorsprung verschafften, war die Kryptologie nun zu einer Institutionen geworden. Vielerorts durchliefen Kryptologen dank der Geheimen Kabinettskanzleien eine Beamtenlaufbahn mit hohem Ansehen und Einkommen. Auch wenn die Bezahlung größtenteils aus Erfolgsprämien bestand, minderte das die Annehmlichkeiten dieses Berufs kaum, denn die Erfolge stellten sich regelmäßig ein. Die Grenze der Kompliziertheit der benutzten kryptographischen Verfahren war de facto die Grenze der Alltagserfahrungen von Offizieren und Diplomaten der jeweiligen Zeit. Es ist dokumentiert, wie auffallend wenig Bewusstsein die 'politische Klasse' dieser Zeit von der Schwäche ihrer Verschlüsselungen hatte. Die Unverhältnismäßigkeit zwischen aufwändiger professioneller Kryptanalyse einerseits und stümperhafter Kryptographie andererseits mag kurios erscheinen. Aber dennoch hatte die politische Gewalt nun damit begonnen, sich in Gestalt der Geheimen Kabinettskanzleien die Kryptologie systematisch zum Mittel zu machen – auch wenn die Art und Weise, in der sie das tat, noch Widersprüche hatte, die aus der Sicht von Bürgern moderner Nationalstaaten geradezu eklatant sind.
Charakteristisch für ihre Zeit war der rasche, totale Zusammenbruch des Systems der Geheimen Kabinettskanzleien. Dazu heisst es bei Kahn:

> „[The] political gales of the 1840s [...] blew down most of Europe's remaining absolutism and the totalitarian agencies that propped it up. Europe's new birth of freedom tolerated no government opening of mail. In England, a tremendous public and parliamentary outcry over the surreptious opening of letters forced the government to discontinue the interception of diplomatic correspondence in June of 1844. That October the government dissolved the Decyphering Branch [...]. In Austria, the Geheime Kabinets-Kanzlei closed its doors in 1848. In France, the Cabinet Noir, which had been withering ever since the Revolution, passed away as well in that convulsive year."[20]

Die Geheimen Kabinettskanzleien waren im Angesicht der bürgerlichen Revolution institutioneller Ausdruck für alles, was eine moderne Staatsgewalt *nicht* sein sollte.

20 Kahn, S. 188.

Der ideellen Gesamtheit der Geschäfte ihrer Bürger, dem bürgerlichen 'Gemeinwohl', sollten und konnten sie offenkundig nicht dienen. Im Gegenteil, die Geheimen Kabinettskanzleien waren ein typischer Ausdruck der unbeaufsichtigten Begaunerei zugunsten des Partikularinteresses der Höfe. Im Anfang hatte die neue Gestalt der nationalstaatlichen Gewalt keine besondere neue Verwendung für die Kryptographie, sondern war damit beschäftigt, eine spezifische Gestalt der staatlichen Kryptographienutzung abzuwickeln, die von den politisch-ökonomischen Zeitläufen überholt worden war.

1.4 Kryptologie im modernen Nationalstaat

Das monotone metallische Klicken des eletrischen Telegrafen war das Geräusch, mit dem die moderne, bürgerliche Anwendung der Kryptographie begann.[21] Im England der industriellen Revolution, Mitte des 19. Jahrhunderts, hatten sich schnell Interessenten dafür gefunden. Verträge ließen sich telegrafisch abschließen, und das eigene Geschäft ließ sich zentral verzögerungsfrei lenken. Industriespionage hatte es zwar schon vor dem Telegrafen gegeben, aber nun lag ihr Material auf dem Präsentierteller, genauer: Auf dem Telegrafenmast.
Angesichts des ökonomische Nutzenkalküls, dem die Telegrafie als Geschäftsmedium unterworfen war und durch die sie erst Verbreitung gefunden hatte, lag zum Greifen nahe, welchen Nutzen Verschlüsselung in einer Welt der Konkurrenz hat. Die wichtigste Triebfeder zur Fortentwicklung der kryptologischen Methoden lag seit dem 19. Jahrhundert jedoch bei den Nationalstaaten. Der Zweite Weltkrieg machte deutlicher als je zuvor, wie abhängig moderne Staaten von der Diskretion ihrer Nachrichtenübermittlung sind – insbesondere der telegrafischen und erst recht derjenigen per Radiowellen. Im amerikanischen Bürgerkrieg und im deutsch-französischen Krieg waren es noch lediglich Diplomaten, Staatsmänner und Feldherren, die sich gegenseitig verschlüsselt Briefe schrieben. Immerhin machten sie vom gesellschaftlich vorhandenen Wissensstand der Kryptologie bereits weitgehend Gebrauch. Während des Ersten Weltkriegs machte die Mechanisierung der Kryptographieanwendung große Fortschritte, und im Zweiten Weltkrieg hatten die Kriegsschiffe bereits eigene Kryptographiemaschinen an Bord, ebenso zahllose

21 Vgl. Kahn, S. 189 f., zugleich Hauptquelle der Darstellungen dieses Abschnitts.

Bataillone.[22] Auch in der Forschung hatte die Kryptographie den Diplomatendünkel endgültig abgestreift. Weitab von der heissen Front focht nun ein Heer von mathematischen Spezialisten den Krieg mit aus. Vor allem Großbritannien und die USA machten mitten während des Krieges kriegsstrategisch äußerst relevante technische Erfindungen, darunter die mit großem materiellen und personellen Aufwand betriebenen Projekte zur Entschlüsselung mitgehörter deutscher und japanischer Funksprüche. Ein charakteristisches Merkmal dieser Projekte war die strikte Geheimhaltung, unter der sie stattfanden. Noch Jahre nach Kriegsende verbreiteten die USA an Staaten des Nahen Ostens kryptographische Verfahren, die sich in Wahrheit bereits während des Krieges als unsicher erwiesen hatten. Und die Geschichte des Siegs polnischer und britischer Kryptologen über die deutsche Verschlüsselungsmaschine Enigma kam erst 1974 ans Licht der Öffentlichkeit – so lange galten die Akten darüber noch im nachhinein als *confidential*.

Die nach dem Zweiten Weltkrieg übrig gebliebenen Supermächte trieben ihre kryptologische Entwicklungen nun erst recht voran. Sie verfolgten das Ziel, durch ihre Nachrichtendienste ihre eigene staatliche Kommunikation zu schützen und an Informationen (sowohl staatliche als auch private) anderer Staaten zu gelangen. Etwas Schutz für die Geschäftswelt im eigenen Land fiel bei alledem bestenfalls gelegentlich und zufällig ab, denn nicht nur vor den konkurrierenden Staaten, sondern auch vor den eigenen Bürgern bemühte man sich konsequent, diesen Fortschritt geheim zu halten.

Die USA vereinte nach dem Zweiten Weltkrieg ihre vormals nach Waffengattungen getrennten Auslandsgeheimdienste unter einem gemeinsamen Dach als eine neue Behörde, die NSA (National Security Agency). In den ersten Jahren ihres Bestehens war selbst die Existenz dieser Einrichtung eine Geheimsache. Als die Weltmacht Nummer Eins der Nachkriegsära verfolgte man konsequent das Ziel, auch in Sachen Ver- und Entschlüsselung unangefochten spitze zu sein. Bis heute wird über die NSA behauptet, sie sei sowohl der weltgrößte Arbeitgeber von Mathematikern als auch der größte Käufer von Computern. In zwei Abteilungen verfolgt die Agency ihre beiden Hauptziele: In der Abteilung Sigint (Signal Interception) elektronisch und per Funk übertragene Daten weltweit abzuhören, in der

22 Vgl. auch Hagelins Produktionszahlen im ersten Abschnitt dieses Kapitels.

Abteilung Comsec (Communications Security) den eigenen Nachrichtenverkehr vor dem Abhören durch Dritte zu schützen.

2 1969-1980: Eine neue kryptologische Idee

2.1 Das Jahrzehnt der Computer-Pioniere

Ende der sechziger bis Anfang der achtziger Jahre spielte sich die Vorgeschichte des PCs und des Internets zugleich ab. Ihre Bühne waren eine Hand voll Labors US-amerikanischer Großunternehmen wie Xerox PARC, AT&T's Bell Laboratories und IBM, sowie Hochschulen wie das MIT in Cambridge, die University of California in Berkeley und die Stanford University. Die häufig anzutreffende Aussage über die Geschichte des Internets, im Anfang sei es ein Versuch des US-Militärs gewesen, durch Dezentralisierung der Datenströme seine Informations-Infrastruktur darauf vorzubereiten, einen atomaren Weltkrieg zu überstehen, ist nur die halbe Wahrheit – und verfehlt damit das Eigentümliche der computernetzwerk-bezogenen Erfindungen in den siebziger Jahren ums Ganze. Ermöglicht durch eine Praxis der großzügigen privaten und öffentlichen Förderung wurde der computerwissenschaftliche Forschungs- und Entwicklungsprozess weitgehend in den akademischen Bereich verlagert. Das Argument, das Internet nütze im Kriegsfall der Nation, eignete sich zwar, um benötigte Fördermittel zu erhalten – die konkrete Steuerung, und letztlich erst recht die naturwüchsige Dynamik des ganzen Entwicklungsprozesses hatte das Militär aber nicht in der Hand.[23] So waren die ersten integrierten Halbleiterschaltkreise, in denen sich ein kompletter Rechner unterbringen ließ, 1970 bereits kommerzielle Entwicklungen von Intel und Texas Instruments für den freien Markt. Die *Request for Comments* (RFC) waren 1969 als Modell einer Entwicklung von technischen Standards für Computernetzwerke entstanden, in dem die allgemeine Öffentlichkeit in den Entwicklungsprozess eingebunden wurde – durch jedermann zugängliche Informationen über alle Standards selbst in frühen Stadien ihrer Vorbereitung und Entwicklung.[24] Mehr noch, die Entwicklungstätigkeit vollzieht sich

23 Katie Hafner und Matthew Lyon: Die Geschichte des Internet. Heidelberg, 2000, S. 9 f.

24 Vgl. A. a. O., S. 166 f.; in Hafners und Lyons Buch wird die 'Frühgeschichte' des Internets, die in der vorliegenden Arbeit lediglich anhand des Modells der RFCs charakterisiert wird, ausführlich und materialreich erörtert.

nach dem Modell der RFCs nicht nur vor den Augen einer ansonsten passiven Öffentlichkeit, sondern die Öffentlichkeit wird virtuell selbst zur Entwicklergemeinde, die, wie der Name RFC schon sagt, kommentiert, verändert und verbessert. Aus der Selbstbeschreibung der RFCs:

> „The Internet, a loosely-organized international collaboration of autonomous, interconnected networks, supports host-to-host communication through voluntary adherence to open protocols and procedures defined by Internet Standards. [...] In outline, the process of creating an Internet Standard is straightforward: a specification undergoes a period of development and several iterations of review by the Internet community and revision based upon experience, is adopted as a Standard by the appropriate body [...]. [...] During the development of a specification, draft versions of the document are made available for informal review and comment [...].“[25]

Die Beispiele der ungebundenen kommerziellen Entwicklung von Halbleiterschaltkreisen und der freien RFCs vermitteln einen Eindruck davon, wie sehr Anfang der siebziger Jahre die Dynamik der Computerwissenschaften und der Netzwerksysteme an Eigenständigkeit gewonnen hatte. Im Bereich der Kryptologie kulminierten die kommerziell beauftragte Entwicklungstätigkeit sowie die individualistischen Zielsetzungen junger Wissenschaftler 1976 in zwei epochalen Ereignissen.

2.2 1976 – Ein Epochenjahr der Kryptologie

1976 entwickelte das seinerzeit weltgrößte IT-Unternehmen IBM im Auftrag des Londonder Bankhauses Lloyds das symmetrische Verschlüsselungsverfahren *Digital Encryption Standard* (DES).[26] Kein Verschlüsselungsverfahren hat bis heute auch nur annähernd den Verbreitungsgrad von DES erreicht, keines ist seitdem so gründlich erforscht worden. DES sollte eine für kommerzielle Ansprüche hinreichend sichere Verschlüsselung bieten. IBM nahm sich dieses äußerst anspruchsvollen Ziels an, weil man das Resultat zur Einbindung in kommerzielle Anwendungen frei verbreiten wollte. Der Algorithmus von DES – und dieser aus heutiger Sicht

25 S. Bradner: The Internet Standards Process – Revision 3, RFC 2026. 1996 ⟨URL: `ftp://ftp.isi.edu/in-notes/rfc2026.txt`⟩ – Zugriff am 1.5.2003, S. 2 ff.

26 Ausführlich und kritisch dargestellt in Levy: Crypto. beat, S. 37 ff.

banale Schritt war revolutionär – wurde deshalb veröffentlicht. Der ganze Vorgang blieb nicht ohne aktive staatliche Begleitung. NSA und IBM einigten sich auf einen Deal. Die NSA stellte ihr Know How zur Überprüfung und Verbesserung der Entwicklungsergebnisse zur Verfügung, und durfte im Gegenzug die Kriterien dieser Verbesserung geheim halten. IBM verzichtete auf die Lizensierung des Verfahrens, und der Algorithmus wurde zum nationalen Verschlüsselungsstandard erklärt. Die akademische Kryptologie-Gemeinde quittierte den Vorgang mit äusserster Skepsis, der NSA wurde eine gezielte Unterwanderung des Verschlüsselungsstandards unterstellt – und das Ziel, eigene, bessere Algorithmen zu entwickeln und öffentlich zu machen, war in die Welt gekommen.
Das zweite epochale Ereignis war die Erfindung der asymmetrischen Verschlüsselung – jener Art kryptographischer Verfahren, um die es in dieser Arbeit hauptsächlich geht. Der historischen Genauigkeit halber wäre von einer Neuerfindung zu sprechen, denn das Konzept einer asymmetrischen Verschlüsselung war bereits mindestens einmal zuvor entwickelt worden – von einem Mitarbeiter des britischen Nachrichtendienstes, der es jedoch nie veröffentlichte.[27]

2.3 Was ist das Neue an der Public-Key-Cryptography?

Vor der Erfindung der asymmetrischen Verschlüsselung beruhten alle Verschlüsselungsverfahren auf einem vorgängigen Geheimnis zwischen Sender und Empfänger einer Nachricht.[28] Oberstes Prinzip war: Sollen sich Nachrichten über unsichere Kanäle so austauschen lassen, dass sie vor dem Zugriff Dritter geschützt bleiben, dann muss zuvor über einen sicheren Kanal ein Schlüssel ausgetauscht worden sein. Geschieht dies nicht, kann auch der Schlüssel selbst nicht vor dem Zugriff Dritter geschützt werden, und die Verschlüsselung einer Nachricht wäre überflüssig. Dieses Problem ist in der Kryptologie auch als das Schlüsselaustauschproblem bekannt; alle 'alten' kryptographischen Algorithmen, vor der Erfindung der asymmetrischen Verschlüsselung, die mit jenem Problem zu kämpfen hatten, werden symmetrische Verschlüsselungsverfahren genannt. In der Praxis war das Schlüsselaustauschpro-

27 Vgl. Boris Gröndahl: Die Entdeckung der Public-Key-Kryptographie. telepolis 1998 ⟨URL: `http://www.heise.de/tp/deutsch/special/krypto/1381/1.html`⟩ – Zugriff am 1.5.2003.

28 Eine ausführliche vom Schlüsselaustauschproblem ausgehende Erklärung der PKC bietet Schmeh, S. 93 ff.

blem nicht zuletzt auch ökonomischer Natur. Für die Kommunikation zwischen nur zwei Partner reicht ein gemeinsamer geheimgehaltener Schlüssel. Bei insgesamt drei Partnern ergeben sich bereits drei mögliche Kommunikationspaarungen, und dementsprechend müssen es drei solcher Schlüssel sein, für vier Partner sechs und entsprechend mit geometrischer Steigerung weiter. Es liegt auf der Hand, dass solche Verschlüsselungsverfahren in den Größenordnungen von Massenkommunikationsmitteln rasch auf ihre Grenzen stoßen. Vor dem Hintergrund der rasch voranschreitenden Entwicklung von Computern und Netzwerken im nicht-militärischen Bereich stand die Idee eines massenhaften Zugangs zu computergestützter Kommmunikation gleichsam 'im Raum' – und damit potentiell auch eine Zuspitzung des Problems der Diskretion von elektronischer Individualkommunikation. Diese hatte bislang praktisch nur am Telefon stattgefunden – einem System, bei dem die jeweiligen Kommunikationspartner für die Dauer ihres Gesprächs eine technisch exklusive Verbindung miteinander teilen. Telefongespräche können immer nur an einer zentralen Vermittlungsstelle mitgehört werden oder durch Angriffe auf die Hardware der Telefonverbindung, die jedoch verhältnismäßig aufwendig sind und nur ausgewählte Opfer treffen. Das Protokoll des Datenaustauschs per Internet sieht hingegen eine permanent offene Verbindung zwischen allen Beteiligten vor. Vor diesem Hintergrund war es nicht bloßer Zufall, dass das asymmetrischer Verschlüsselungsverfahren, das im folgenden beschrieben werden soll, von mindestens drei Personen unabhängig voneinander erfunden worden war – die Zeit war reif dafür.[29] Ganz zu schweigen von dem anderen Aspekt des komplexen Schlüsselaustauschproblems, 'sichere Kanäle' zu finden. Diese sind in der gesellschaftlichen Realität rar, und ihr Gebrauch setzt zudem ein gemeinschaftliches Vorgehen der Kommunikationspartner voraus. Doch auch wenn es unvertraut klingen mag: Es ist möglich, dass auch zwei einander ansonsten vollkommen fremde Personen eine verschlüsselte Kommunikation miteinander eingehen. Jedoch, soviel dürfte die Ausführung des Schlüsselaustauschproblems verdeutlicht haben, nie und nimmer mit den Mitteln der symmetrischen Verschlüsselung.

Die Erfindung der asymmetrischen Verschlüsselung gilt als der Durchbruch zur Lösung des Schlüsselaustauschproblems. Für einen asymmetrischen Schlüsselaus-

29 Vgl. zur Erfindung des britischen Militärgeheimdienstes den Abschnitt 2.2 und zur Erfindung Ralph Merkles 2.4.

tausch benötigt jeder Einzelne – trotz beliebig vieler Kommunikationsteilnehmer – nur noch ein einziges Schlüsselpaar. Der eine Teil dieses Paars dient der Verschlüsselung von Nachrichten an seinen Besitzer, und nur der andere Teil des jeweiligen Schlüsselpaars erlaubt es, diese Verschlüsselung wieder rückgängig zu machen. Dementsprechend ist der erste Schlüsselteil öffentlich bekannt, das dazugehörige Gegenstück braucht hingegen ausschließlich sein Besitzer zu kennen. Indem er diesen *Private Key* vor Dritten geheim hält, haben diese keine Chance, eine einmal vorgenommene Verschlüsselung einer Nachricht an den Schlüsselpaarbesitzer rückgängig zu machen, selbst wenn diese Verschlüsselung von ihnen selbst vorgenommen worden wäre. Die öffentliche Verfügbarkeit des einen Schlüsselteils gibt dem ganzen Verfahren seinen Namen, *Public-Key-Cryptography.*

Im umgekehrter Weise lassen sich nun auch digitale Unterschriften anfertigen. Eine Kopie der Nachricht[30] wird vom Sender quasi mit seinem geheimen Schlüsselteil verschlüsselt. Nun kann jeder, der einen bestimmten öffentlichen Schlüssel besitzt, mit Gewissheit nachvollziehen, dass nur mit Hilfe des dazugehörigen geheimen Schlüsselteils die korrekte 'unterschreibende' Verschlüsselung der Kopie oder Prüfsumme vorgenommen worden sein kann. Damit verlagert sich das Problem von der Authentifizierung der Nachrichten zur Authentifizierung öffentlicher Schlüssel. Da das Problem der Authentifizierung ganz unabhängig von der Verschlüsselung gelöst wird, eröffnet die PKC einen ganz neuen Einsatzbereich der Kryptographie. Jede Nachricht, ob verschlüsselt oder nicht, lässt sich nun signieren.

Wenn sich die Kommunikationspartner nicht persönlich kennen, kann es auch sinnvoll sein, einen öffentlichen Schlüssel zu signieren. Man spricht in diesem Zusammenhang auch von einem Zertifikat. Der Aussteller des Zertifikats hat sich davon überzeugt, wer tatsächlich Besitzer eines bestimmten Schlüssels ist. Damit kann er Dritten, die ihm vertrauen, die Arbeit abnehmen, sich jeweils individuell davon zu überzeugen.

Aus dem strukturell nicht mehr notwendig hierarchischen Vertrauensmodell der neuartigen asymmetrischen Kryptographie ergeben sich verschiedene mögliche Zertifizierungsmodelle. Als die beiden einfachsten Grundstrukturen hierfür wären zu nennen: 1. Eine tendenziell unendliche Kette von Zertifikaten, in der jeder Schlüs-

30 in der Praxis stattdessen meistens eine unverwechselbare Prüfsumme der Nachricht; in die Mathematik der digitalen Signaturen führt anschaulich ein: Wobst, S. 288 ff.

selbesitzer andere Schlüssel zertifizieren kann und ebenso seinen Schlüssel von beliebigen (auch mehreren) anderen Schlüsselbesitzern zertifizieren lassen kann. 2. Ein traditionelles hierarchisches Vertrauensmodell. Hier bürgt ein Dritter durch zentrale Zertifizierung. Zentrale Zertifizierung impliziert zwar nicht mehr, 'wie früher', eine ebenso zentrale Verfügungsmacht über alle geheimen Schlüssel, jedoch schließt sie sich damit auch nicht aus. Die Subsumtion unter eine solches zentrales, technisch nicht mehr notwendiges Vertrauensmodell kann lediglich durch das massenhafte Vertrauen aller Kommunikationspartner in die gewissenhafte Aufgabenerfüllung der Zertifizierungsinstanz erfolgen; oder, und dies spielt in der realen Welt die entscheidende Rolle, es wirken ökonomische Hebel. Das kann beginnen mit dem Angewiesensein auf von anderen anerkannte Zertifikate, eventuell kombiniert mit zivilrechtlich einklagbaren Garantien über die genaue Funktionsweise (certification policy) und den 'Grad der Zuverlässigkeit' einer Zertifizierungsinstanz. Gegebenfalls kann diese Zuverlässigkeit auch staatlicherseits sanktioniert werden – bis hin zur gewaltsamen Anordnung an bestimmte Personen, sich auf bestimmte Zertifikate und die Methoden ihrer Vergabe zu verlassen.[31]

2.4 Was war mit der Public-Key-Cryptography beabsichtigt?

Bis hier dürfte deutlich geworden sein, dass Diffie und Hellman mit dem Titel ihres epochalen Aufsatzes von 1976 *New Directions in Cryptography*[32] keineswegs übertrieben haben. Dabei hatten beide Wissenschaftler bis zur Veröffentlichung nahezu unbemerkt von der Öffentlichkeit am Problem der asymmetrischen Verschlüsselung gearbeitet, nicht einmal Forschungsteams oder gar ganze Fakultäten können sich dieses Forschungsresultat auf die Fahne schreiben. Auch Diffies und Hellmans offizielle Stipendien bzw. Lehrstühle hatten thematisch nur am Rande etwas mit ihrer Haupttätigkeit in den Jahren vor 1976 zu tun, ihrer Entdeckung einer *neuen Richtung* von Kryptographie. Kurz, es handelte sich um eine kaum beachtete Erfindung eines kleinen, informellen Netzwerks junger Forscher.
Der Widerspruch zwischen der großen inhaltlichen Bedeutung und der zunächst

31 Die weit gehenden gesellschaftlichen Implikationen der Vertrauensmodelle, die sich durch asymmetrische Verschlüsselung und vor allem ihren Zwillingsbruder, die digitale Signatur, ergeben, werden unter 6.3 behandelt.

32 Diffie und Hellman.

randständigen Gestalt dieser Erfindung wird erklärlich vor ihrem historischen Hintergrund. Die siebziger Jahre waren weder das Post-Cold-War- noch das Internet-Age. Auch wenn E-Mail und computernetzwerk-gestützte Geschäfte wie selbstverständlich in Diffies und Hellmans Aufsatz vorkommen: Die E-Mail war erst drei Jahre vorher erfunden worden; außer ein paar tausend amerikanischer Informatiker und technikbegeisterter Studenten kannte dieses Medium niemand. Und E-Business existierte ausschließlich in den Köpfen einiger mit öffentlichen Geldern bezahlter Visionäre.

New Directions selbst liest sich für den heutigen Betrachter, der die Geschichte der jahrzehntelangen staatlichen Behinderung der massenhaften Kryptographieanwendung bereits kennt, vor allem als eine erstaunlich wenig politische, jedenfalls sehr nüchterne Darstellung einer Erfindung nebst einer kurzen kryptologiehistorischen Einordnung.

Einen kryptographischen Algorithmus zu veröffentlichen, der nachvollziehbar beansprucht, selbst gezielten Versuchen seiner Brechung zu widerstehen, war in den siebziger Jahren keineswegs üblich, ganz zu schweigen davon, eine breite Öffentlichkeit als potentielle Nutzerin eines neuen kryptographischen Konzeptes ins Auge zu fassen. Der US-Nachrichtendienst las mit, und mischte sich in die Veröffentlichung und Nichtveröffentlichung kryptographischer Ideen regelmäßig und massiv ein.[33] Diffie und Hellman gelang ihre Publikation durch eine Nacht-und-Nebel-Aktion in Gemeinschaft mit dem Verleger der Fachzeitschrift. Allein der Akt dieser unabgesprochenen Veröffentlichung war unter dem geltenden Reglement ein offener Bruch des Souveränitätsanspruchs, den der US-amerikanische Militärnachrichtendienst NSA jahrzehntelang über die Fortentwicklung und auch die Anwendung der Kryptographie gehabt hatte. Diesen Souveränitätsanspruch fechten die Autoren nicht einmal explizit an, sondern ignorieren ihn. Kryptologie und der Fortschritt der Kryptographieanwendung werden von Diffie und Hellman selbstverständlich vor den Augen der Öffentlichkeit vollzogen, und das in einem strikten Sinne. Sie fassen ihre Öffentlichkeit bruchlos entsprechend dem Ideal einer weltweiten, formal offenen scientific community als ideeller Urheberin technischer Standards auf, wie es sich auch im Modell des *Request for Comments* ausdrückt. Dabei handelt es sich

33 Eine emphatische, umfassende Schilderung dieser Repression findet sich bei Levy: Crypto. beat, S. 109 ff.

jedoch nicht um eine abstrakte Überzeugung, sondern es geht ihnen um einen konkreten Nutzen für die Massen im Sinne zahlreicher Individuen. Nicht nur der Akt der Veröffentlichung selbst, sondern auch die Rolle der breiten Öffentlichkeit selbst in der Public-Key-Cryptography lag quer zur Konzeption einer Kryptographie, die ausschließlich in den geschlossenen Hierarchien von Militär und Geheimdiensten angewendet wird.

Die Einzelnen werden vorausgesetzt als autonome 'Endanwender' der zukünftigen, neuartigen Kryptographie. Die Masse der potentiellen Kryptographie-Anwender entsteht bei Diffie und Hellman jedoch nicht in abwehrender Entgegensetzung zu einem überwachenden Staat,[34] sondern ihr gemeinsamer Nenner ist zuallererst eine Maxime: Kein Dritter soll mithören oder -lesen können, was eine Person einer anderen mitzuteilen hat. Damit machen Diffie und Hellman implizit einen höchst gesellschaftlichen Sachverhalt stark: Den allgemeinen und notwendig konkurrierenden Bezug der Individuen aufeinander. Jeder könnte ein Interesse daran haben, in die Privatsphäre jedes anderen einzugreifen, und da dieses Interesse so absehbar und so stark ist, dass es sich möglichwerweise selbst über soziale Normen oder gesetzliche Regeln hinwegsetzt, die die Privatsphäre schützen sollen, bedarf diese Sphäre eines technischen Schutzes. PKC soll nicht zuletzt ein technischer Schutz privater Informationen sein. Dieses konkrete Interesse aller Einzelnen lässt sich scheinbar unproblematisch mit dem Geschäftsinteresse an einem zukünftigen E-Commerce zu summieren. Hier lauern erst recht Konkurrenten aufeinander, und ohne weitere Reflexionen auf gesellschaftliche Verhältnisse sind auch Angestellter und Chef, Kunde und Händler lediglich eine Reihe von untereinander Konkurrierenden.

Warum auch hätten Diffie und Hellman die Gefahren für die Informationen jedes Einzelnen konkret bestimmen sollen? Die Setzungen, unter denen die Funktionsweise der kryptographischen Verfahren erklärt werden, werden in der Erklärung des Nutzens dieser Verfahren für die Einzelnen einfach wörtlich genommen: Jeder wird in der Privatsphäre seiner Informationen potentiell und real von 'jedem Dritten' bedroht! Die kryptographischen Verfahren erscheinen so als die technisch adäquate Lösung von Problemen, die von den Autoren stillschweigend als bekannt

34 – und somit noch ganz anders als beim ersten populären Computerprogramm, das PKC integrierte, PGP. Vgl. Kapitel 4.

vorausgesetzt werden; das Verhältnis des Staates zu diesem Bezug der Einzelnen aufeinander erscheint als die einer Gewalt, die bisher bestenfalls die gegenseitige Verteidigung der Privatsphäre erschwert hat, ansonsten jedenfalls keinen nennenswerten Bezug zum Verhältnis der Einzelnen zueinander hat.
Die Erfahrung, dass im realen Leben tatsächlich abgehört wird, liegt dem ganzen Vorstoß zur PKC zugrunde, hier liegt das Problem, das sie lösen helfen soll – allerdings in einem abstrakten Verständnis, ohne einen Begriff von gesellschaftlich notwendiger Konkurrenz zwischen den Individuen, und ohne einen Staat, der für diese Konkurrenz sorgt oder einfach selbst abhört. Dieses abstrakte Verständnis passt als Ausgangsproblem zu einer impliziten *technischen Utopie*. Diffie und Hellman haben eine große Erfindung gemacht, um ein politisches und soziales Problem technisch zu lösen.
Unter der Voraussetzung, dass das Problem selbst vor allem durch Technik lösbar ist, ist es nur konsequent, dass die öffentlich gemachte Erfindung dieser technischen Lösung Anlass zu großem Optimismus gibt. So schreibt Whitfield Diffie selbst zehn Jahre nach seiner Erfindung, als bereits hemmende Faktoren der Durchsetzung von PKC ans Tageslicht getreten waren:[35]

> „[PKC] is soon to be implemented in hundreds of thousands of secure telephones and efforts are under way to apply the same mechanisms to data communication on a similar scale. The outlook in the commercial world is equally bright.“[36]

In *New Directions* beziehen Diffie und Hellman abschließend Kahns Begriff des Amateurs auf sich und ihre Veröffentlichung.

> „It was the amateurs of cryptology who created the species. The professionals, who almost certainly surpassed them in cryptanalytic expertise, concentrated on down-to-earth problems of the systems that were then in use but are now outdated. The amateurs, unfettered to those realities, soared into the empyrean of theory.“[37]

---

35 Vgl. 3.2.

36 Whitfield Diffie: The First Ten Years of Public-Key Cryptography. Proceedings of the IEEE 76 1988, Nr. 5, S. 574
Warum es zu den hunderttausenden sicheren Telefonen nicht gekommen ist wird unter 6.1 und 6.2 erörert.

37 Kahn, S. 125 f.

Die Leistungsbilanz der Amateure für den kryptologischen Fortschritt ‘als solchen’ legitimiert am Ende von Diffies und Hellmans Aufsatz geradezu den Bruch mit dem staatlichen Monopolanspruch auf die Kryptographieentwicklung. Ihre Erfindung erscheint gewissermassen als von der wissenschaftlichen Qualität der Entwicklungstätigkeit früherer ‘Amateure’ in der Kryptologiegeschichte gedeckt. Der sich abzeichnende politische Konflikt um öffentliche Kryptographieentwicklung im akademischen Bereich wird so zwar nicht offen angesprochen, aber die Legitimität der eigenen Entwicklungstätigkeit unterstrichen – letztlich mit dem Argument der erfinderischen Leistung.

Der Nachdruck auf dem Kahnschen Begriff des Amateurs steht freilich im Widerspruch zu Diffies und Hellmans Selbsteinordnung der PKC in die Kryptographieentwicklung nach Kerckhoffs.[38] Es ist sehr gut nachvollziehbar, die Entdeckung der PKC in Zusammenhang zu bringen mit Kerckhoffs’ erster Maxime, Kryptographie sei so zu gestalten, dass möglichst wenige Elemente und Prozesse geheim gehalten zu werden brauchen. Allerdings war die historische Figur Kerckhoffs vollberuflicher Militärkryptograph, und insofern gerade eine der Figuren in Kahns Buch, die man zumindest als große Ausnahme von der Regel der entscheidenden Rolle des Amateurkryptographen anerkennen muss.

Weber stellt in seiner Schilderung der Entwicklung der PKC die These auf, dass Diffie diese Erfindung vor anderen machte, die sich mit dem Thema beschäftigt hatten, weil er im Gegensatz zu diesen „durch libertarian traditions, student movement, Kritik an der Regierung“ geprägt war.[39]

Zwei Jahre nach der Veröffentlichung von *New Directions*[40] sollte sich zeigen, dass Diffies und Hellmans Erfindung nur ein Meilenstein auf dem Weg zum anwendungsgerechten asymmetrischen Algorithmus gewesen sein sollte. Diffie und Hell-

38 Vgl. die Fußnote zu Diffie und Hellman unter 1.2.

39 Weber, S. 171 – insbesondere auf die „libertarian traditions“ und die „Kritik an der Regierung“ wird in 4.4 dieser Arbeit eingegangen. So umfassend und nachvollziehbar Webers Darstellung der Erfindung der PKC ist, so problematisch ist allerdings die Einordnung dieser Erfindung in seinem Buch. Er behandelt die PKC ausschließlich als technologische Voraussetzung möglicher anonymer digitaler Zahlungsmittel, und unterschlägt dabei, dass PKC auch in anderen Konzepten des elektronischen Zahlungsverkehrs eingesetzt wird, in denen die individuelle Privatsphäre der Kunden weitaus weniger berücksichtigt wird. Als Beispiel hierfür sei etwa die vorantreibende Rolle der Kreditinstitute bei der Einführung digitaler Signatur-Karten in Deutschland genannt; vgl. hierzu auch 6.3 in dieser Arbeit.

40 Diffie und Hellman.

man selbst hatten bereits weniger berühmte Vorgänger und Vorbereiter gehabt. Hellman kannte bereits Ralph Merkles Knapsack-Algorithmus – einen kurz zuvor veröffentlichten Versuch, einen asymmetrischen Schlüsselaustausch zu bewerkstelligen, dessen kryptographische Defizite bereits aufgefallen waren, bevor dieser Ansatz von sich hätte reden machen können. Im Jahre 1978 jedoch veröffentlichten die am MIT arbeitenden Kryptologen Ronald Rivest, Adi Shamir und Richard Adleman den nach ihnen benannten RSA-Algorithmus.[41] Der RSA-Algorithmus war nach seiner Veröffentlichung in den USA patentiert worden; dieses Patent lief im Jahr 2000 aus. Der Schlüsselaustausch nach DH wird zwar bis heute eingesetzt – aber fast nur deshalb, weil er häufig bevorzugt worden war, wenn es darum ging, ein patentschutzfreies Verfahren in kryptographische Anwendungen einzubinden. Unter technischen Gesichtspunkten bot der neue Ansatz von RSA jedoch nur Vorteile. Er ist universeller und zugleich einfacher als das Schlüsselaustauschverfahren DH. Während dieses das Problem der asymmetrischen Verschlüsselung auf die Lösung des Schlüsselaustauschproblems reduziert hatten, lässt sich mit RSA jede beliebige Zeichenkette direkt asymmetrisch verschlüsseln.[42] Die Universalität des RSA-Verfahrens hat unter anderem den Vorteil, dass ein- und derselbe Schlüssel sowohl zum Verschlüsseln als auch zum Signieren verwendet werden kann.
In der kryptologischen Fachliteratur wird darauf hingewiesen, wie bemerkenswert es ist, dass RSA bereits zwei Jahre nach der Veröffentlichung von Diffie und Hellman herauskam, jedoch bis heute der unangefochtene de-facto-Standard unter den asymmetrischen Verschlüsselungsalgorithmen geblieben ist. Trotz aller weiterer Erfindungen auf diesem Gebiet gilt: Weder ist in dem sehr gut untersuchten Verfahren RSA eine Sicherheitslücke entdeckt worden, noch konnte eine Methode des asymmetrischen Verschlüsselns von ähnlicher Einfachheit und Universalität vorgelegt

41 R. Rivest, A. Shamir und L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21 Februar 1978, Nr. 2 ⟨URL: `http://theory.lcs.mit.edu/~rivest/rsapaper.ps`⟩ – Zugriff am 1.5.2003.

42 Dieser Vorteil hat sich allerdings als nicht allzu relevant erwiesen, da in der kryptographischen Praxis fast ausschließlich sogenannte Hybridverfahren angewendet werden. Das heisst, asymmetrische Verschlüsselung kommt meistens beim Austausch eines Einmal-Schlüssel ins Spiel, der zuvor von einer der beiden Seiten erzeugt worden ist. Der auf diesem Wege ausgetauschte sogenannte Sitzungsschlüssel kann dann selbst symmetrisch sein. Das hat insbesondere ein paar ökonomische Vorteile – vor allem wenn man bedenkt, dass die Rechenoperationen, die von asymmetrischen Verfahren genutzt werden, weit aufwändiger sind als die der üblichen symmetrischen Verfahren.

werden – obwohl es spätestens seit dem E-Commerce-Boom der neunziger Jahre angesichts des amerikanischen RSA-Patents ein großes ökonomisches Interesse an guten Alternativen zu RSA gegeben hätte.

2.5 Du sollst keine Kryptologie haben neben mir

Die Reaktion der US-Behörden auf die vorstehend diskutierten Erfindungen war eindeutig: Wenn die Fachzeitschriften und Kongresse, auf denen die Algorithmen vorgestellt wurden, für Ausländer zugänglich waren, dann lag ein Verstoß gegen das Verbot über die Verbreitung von Kriegszubehör vor. Man hatte durch die Veröffentlichung der PKC gleichsam einen Nachholbedarf entdeckt – einen Nachholbedarf darin, die Verbreitung von in den USA hergestellten Waffen im Ausland zu kontrollieren. Aber warum ist in diesem Zusammenhang überhaupt von Waffen die Rede?

Eine staatliche Waffenexportkontrolle war in den USA bereits zu Beginn des 20. Jahrhunderts eingerichtet worden. Während sie anfangs nur verhindern musste, dass befeindeten Staaten in den USA hergestellte Waffen verkauft werden, war die Situation nach dem Zweiten Weltkrieg – eigentlich: Nach Hiroshima – eine andere. Das Aufgabenfeld der Kontrollen wurde erheblich erweitert, und die neuen Aufgaben forderten ganz neue Erzwingungsmittel. Gegenstand der Kontrolle durften angesichts der Realität der Atombombe nicht mehr ausschließlich materielle Güter sein. Unter Ausfuhrkontrolle wurden nun auch 'technologische Daten' gestellt. Für den gesamten Zeitraum des Kalten Kriegs lässt sich eine permanente Ausweitung der offiziell für schützenswert erachteten technologischen Daten konstatieren.[43]

So war es nur naheliegend, dass sich die 1977 in Kraft gesetzte ITAR-Munitions-List[44] und zugleich die multilateralen Exportkontrollmechanismen der westlichen Welt nun der Kryptographie annahmen. 1979 landeten alle relevanten kryptographischen Produkte auf der Liste. Diffie und Hellman gelang es nur durch einen Trick, am erklärten Willen von US-Regierungsbehörden vorbei ihre Erfindung öf-

43 Rainer Rilling: Rüstung und Wissenschaftsfreiheit in den USA (2). Informationsdienst Wissenschaft und Frieden 1984, Nr. 4 ⟨URL: `http://www.rainer-rilling.de/texte/8440600m.htm`⟩ – Zugriff am 1.5.2003.

44 ITAR ist die Abkürzung von International Traffic in Arms Regulations.

fentlich zu machen.[45] Als es zu spät war, die Veröffentlichung zu verhindern, konnte es eigentlich nur noch darum gehen, klarzustellen: Es soll sich in der freien Welt wenigstens kein Geschäft damit machen lassen, Anwendungen der kriegstauglich anwendbaren Mathematik im 'Reich des Bösen' zu vermarkten. Nicht mehr, aber auch nicht weniger wurde mit den Exportbeschränkungen erreicht – der Rede zum Trotz, es sei absurd, den Export von etwas zu verbieten, das sich auf fünf Codezeilen in der Programmiersprache PERL zusammenfassen lässt.[46]

Zunächst war es diese verwaltungstechnische Abwicklung der Beschränkungen, die eine ganz neue Binnendifferenzierung der Algorithmen hinsichtlich ihrer Anwendung aufkommen ließ. Es ging nun darum, ob es sich jeweils um 'strong crypto' handelte oder nicht. 'Strong' bedeutete in diesem Zusammenhang, dass selbst ein weiterhin exponentielles Wachstums der Rechnerkapazitäten vorausgesetzt, sich nicht davon ausgehen lässt, dass man die Algorithmen in absehbarer Zeit wird 'knacken' können. Anwendungen (seien es nun reine Computerprogramme, oder Geräte, deren Chips entsprechende Algorithmen beherrschten), sollten nur noch dann exportierbar sein, wenn sie keine 'strong crypto' beinhalteten.

Heute, vom bekannten historischen Ergebnis her, mag sich beinahe die Frage stellen, warum nicht restriktiv gegen das Internet vorgegangen wurde. Es sollte sich später sowohl als das Medium der Verbreitung als auch des Einsatzes der Kryptographie erweisen. Die Vorstellung war, dass die extreme Offenheit und Flexibilität, die im Internet durch die Struktur eines stark normierten, paketorientierten Datenverkehrs gewährleistet war, sich rein als Mittel des Datenaustauschs innerhalb der USA bewähren sollte. Heute sieht man darin den Geburtsfehler der mangelnden Internetsicherheit. Das Konzept war nie auf ein Netz ausgelegt, unter dessen Teilnehmern die bad guys sind, obendrein noch solche im Ausland, das heisst dem hoheitlichen Zugriff entzogen. Ein Vorläufer dieser nachdrücklichen Offenheit der Computernetze waren Mitte der siebziger Jahre die sogenannten Bulletin Board Systems. Sie sollten eine entscheidende Rolle für die Verbreitung von PGP, der erste populären Anwendung der PKC für den Heim-PC spielen, noch bevor das Internet selbst seinen kommerziellen Boom erlebte.

---

45 Ausführlich ist der Einfluss der US-Exportkontrollen auf die kryptologischen Entwicklungen in den siebziger Jahren dokumentiert worden in Levy: Crypto. beat, S. 109 ff.

46 Vgl. 5.3.

3 1981-1990: Die blockierte Anwendung der kryptographischen Innovationen

3.1 Man of the year des Time Magazines 1983: Der PC

Seitdem im Zweiten Weltkrieg die Kryptanalyse feindlichen Codes der Hauptantrieb der Computerwissenschaften war, waren die Computer als Universalrechenmaschinen für die Kryptologie unerlässlich geworden. Die jeweils erreichte Leistung der Maschinen war der Maßstab dafür, ob in vertretbarer Zeit die Ver- und Entschlüsselung möglich und vor allem das Brechen der aktuell eingesetzten Verschlüsselungstechnik unmöglich war. Allein schon diese technische Grenze war drei Nachkriegsjahrzehnte zugleich die ökonomische Grenze, die zuverlässig jeden vom erreichten Stand der Kryptographieanwendung ausschloss, der weder eigenes Kapital besaß noch im Dienste des Staates forschte, und die wohnzimmergroßen *mainframes* der fünfziger und sechziger Jahre waren nicht nur teuer, sondern bedurften auch eines spezialisierten Personals. Der Verschleiss der Maschinenteile war enorm; das Mensch-Maschine-Interface war ebenso wenig normiert wie die Betriebssysteme und Anwendungen der Rechner selbst, von komfortablen graphischen Benutzeroberflächen oder ähnlichem ganz zu schweigen. Nicht zuletzt handelte es sich um Computer, deren Rechenleistung und Speichergröße sich ungefähr auf dem Niveau der heutigen Taschenrechner bewegte.

Noch in den siebziger Jahren mussten die Bediensteten und Studenten der Hochschulen Zeiträume anmelden, in denen sie sich der Rechenleistung dieser Giganten bedienen durften. Folgt man der Darstellung Joseph Weizenbaums in *Die Macht der Computer und die Ohnmacht der Vernunft*, dürfte in dieser Zeit der 'Hacker' heutigen Typs entstanden sein. Die Zeiträume, in denen man zum Programmieren angemeldet war, wurde dann exzessiv und unterbrechungslos genutzt, um irgendwelcher Software so viele neue Programmeigenschaften wie eben möglich hinzuzufügen, einfach um des Kultes der Maschinenanwendung willen.[47] Eine andere Facette dieser Hackerkultur war eine blühende Szene von Hardware-Bastlern, die aus den marktgängigen elektronischen Bauteilen eigene Computer zusammenlötete. Zutreffenderweise wird häufig darauf hingewiesen, dass aus den jungen Män-

47 Joseph Weizenbaum: Die Macht der Computer und die Ohnmacht der Vernunft. Frankfurt/Main, 1978.

nern, die sich damals dem Großrechner-Terminal bzw. dem Lötkolben verschrieben hatten, zwanzig Jahre später die Firmenbosse und Einkommensmillionäre der new economy geworden waren. Unter diesen Bedingungen folgten 1980 und 1981 ein paar wichtige technische und ökonomische Schritte hin zu einem billigen, kleinen, quasi allgegenwärtigen Computer, den Personal Computer, kurz PC. In Serienfertigung umgesetzt wurde dieses Konzept 1981 mit dem gleichnamigen 'PC' der Firma IBM, dessen Betriebssystem von dem damals ebenso unbedeutenden wie unbekannten Kleinunternehmen Microsoft beigesteuert wurde. Ganz folgerichtig ernannte das Time Magazine im Jahre 1983 erstmals nicht einen Menschen zum „Man of the year" – sondern den PC.[48]

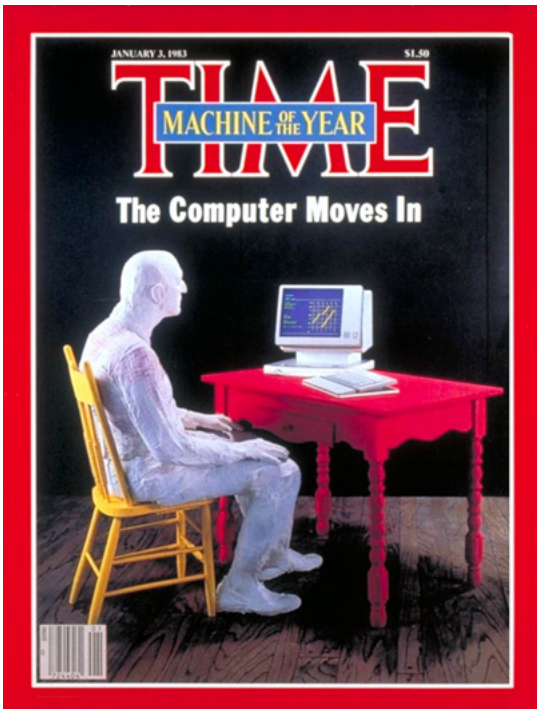

Abb. 1: *1983 – Der Personal Computer kommt in die Welt, oder: „Der Computer zieht (Zuhause) ein"*

Man brauchte seitdem weder ein Bastler noch ein amerikanischer Student der Informatik zu sein, um Zugang zum erreichten Stand der Computertechnik zu erhalten. Freilich hätte man mit dem IBM PC der ersten Stunde die zu jener Zeit verfügbaren kryptographischen Algorithmen nicht in akzeptablen Rechenzeiten anwenden können. Aber mit der kommerziell betriebenen Verbreitung 'persönlicher Rechner', die in Wahrheit zunächst die Büroarbeit revolutionierte, änderten sich die Bedingungen der individuellen Aneignung von Software grundlegend. Das Konzept des PCs sah vor, dass alle Daten auf einem lokalen Massenspeicher vorhanden waren, und damit prinzipiell im vollen Zugriff des Benutzers. Ob es sich dabei nun um eine Floppy Disk mit 160 Kilobyte oder zwanzig Jahre später um eine Festplatte mit 100.000 mal so viel Kapazität handelt, alle Programme werden lokal auf dem eigenen Rechner ausgeführt und sind dem Benutzer mindestens als Binärcode, das heisst in ausführbarer Form, verfügbar. Die Computertechnik hatte ihre Kathedralen verlassen und sich auf den Weg zu den Einzelnen gemacht.

48 Vgl. Abb. 1.

3.2 Der kryptographische Fortschritt erlebt eine bleierne Zeit

Mit Computern wie dem ersten IBM PC war die ökonomische Hürde zur massenhaften Verbreitung eines Kryptosystems wie der RSA-Verschlüsselung noch nicht genommen. In den achtziger Jahren waren zunächst spezielle Chips erforderlich, um mit Massenkommunikationsmitteln kryptographische Anwendungen in akzeptabler Rechenzeit zu ermöglichen. Ein prominentes frühes Anwendungsbeispiel war ein vom amerikanischen Geheimdienst NSA tausendfach produziertes ISDN-Telefon, das allerdings ausschließlich US-Militärs und ihren Zulieferern zugänglich war und ca. 3.000 US-Dollar pro Stück kostete.[49] Abgesehen von einer handvoll solcher Gerätetypen aus dem Dunstkreis des US-Militärs und seiner Geheimdienste entstand in den achtziger Jahren zunächst nichts Vergleichbares. 1986 stellte RSA Security Inc., die Firma, die den mittlerweile patentierten RSA-Algorithmus vermarktete, eine E-Mail-Verschlüsselungssoftware für den PC mit dem Namen MailSafe vor. Das Produkt schlug bei den anvisierten Konsumenten noch weniger ein als die ersten Büroprogramme, die mit dem RSA-Algorithmus arbeiteten. Zum Teil erklärt sich das daraus, dass die zunehmend schneller und besser werdenden IBM- und IBM-kompatiblen-PCs, Apples, Home Computer und andere, erst selten miteinander vernetzt waren. Die Szenerie war also einerseits bestimmt von geheimdienstlichem Behindern, kombiniert mit den zunächst noch relativ hohen Kosten für spezielle kryptographische Hardware, sowie andererseits einem Markt für PC-Anwendungen ohne Internet, der noch keinen massenhaften Absatz für Kryptographie-Anwendungen versprach.

Die amerikanische Innenpolitik und die Strafverfolgungsbehörden hatten die kryptopolitische Szenerie im engeren Sinne zwar noch nicht betreten. Dennoch führen sie bereits Kämpfe auf eng benachbartem Terrain. Nachdem bekannt geworden war, wie leicht es für Privatleute ist, den Mobiltelefonverkehr in ihrer näheren Umgebung abzuhören, wurde mit dem Electronic Communications Privacy Act (ECPA) 1986 erstmals umfassend das Abhören elektronischer Kommunikationsmittel geregelt.[50] Dieser Gesetzgebungsakt war angestoßen worden von der Ame-

---

49 Diffie, S. 570.

50 Jenny Shearer und Peter Gutmann: Government, Cryptography, and the Right To Privacy. Journal of Universal Computer Science 2 März 1996, Nr. 3 ⟨URL: `http://www.jucs.org/jucs_2_3/government_cryptography_and_the/paper.pdf`⟩ – Zugriff am 1.5.2003, S. 122.

rican Civil Liberties Union (ACLU). Die ACLU ist eine große, respektierte Bürgerrechtsorganisation, die keineswegs auf ein einzelnes Thema wie den Schutz der Privatsphäre spezialisiert ist; so hatte sie bereits in den sechziger Jahren gegen die rassistische Diskriminierung von US-Bürgern gekämpft. Es ist nicht ohne Ironie, dass die ACLU nach der Verabschiedung des ursprünglich von ihr initiierten Gesetzes zu dessen schärfstem Kritiker wurde. Der ECPA stellt zwar gegenseitiges Abhören der Bürger unter Strafe, erleichtert jedoch das legale Abhören durch die zuständigen Behörden. Eine weitere große Ausnahme macht das Gesetz hinsichtlich der elektronischen Kommunikation von Angestellten; diese soll unter locker gefassten Bedingungen vom Arbeitgeber mitgelesen und mitgehört werden dürfen.[51] Der ECPA ist nicht nur in den USA, sondern auch in den europäischen Nationalstaaten bis heute modellhaft für die einschlägige Gesetzgebung geblieben. Trotz des ambivalenten Verlaufs dieser ersten, folgenreichen Intervention der ACLU in die staatliche Regulation der elektronischen Individualkommunikation wurde sie in den neunziger Jahren zu einer der wichtigen liberalen Lobbies auch im Bereich der Kryptopolitik; weitere wichtige Bürgerrechtsorganisationen, allen voran die Electronic Frontier Foundation (EFF) entzündeten sich hingegen erst an dem neuen Thema. Von diesem neuartigen innenpolitischen Interesse war 1986 aber noch nichts zu merken; individuelle technische Vorkehrungen zum Schutz vor dem Abgehörtwerden wurden sowohl von der Gesetzgebung als auch von den bürgerrechtlichen Kritikern weitgehend ignoriert. Das sollte sich fünf Jahre später, um 1991, in den USA schlagartig ändern.

Währenddessen tobte um den erst potentiellen Markt der Kryptosysteme bereits ein erbitterter Kampf zwischen verschiedenen Abteilungen der US-Administration – wenngleich noch ohne Interesse seitens der breiten Öffentlichkeit.[52] Sollte starke und asymmetrische Kryptographie normiert werden, um staatlicherseits ihre kommerzielle Verbreitung voranzutreiben? Oder sollte, ganz im Gegenteil, die Verbreitung und der Einsatz der einschlägigen Algorithmen unterdrückt werden – oder, wo nötig, ihr Einsatz unter volle staatliche Kontrolle gestellt werden? Mit diesen unversöhnlich scheinenden Positionen standen sich auf der einen Seite das *National*

51 Zum ECPA und den diesbezüglichen Interventionen der ACLU vgl. Jones International and Jones Digital Century: Family Educational Rights and Privacy Act of 1974 (FERPA). 1999 ⟨URL: `http://pioneer.nactc.cc.ar.us/cup_additional.htm`⟩ – Zugriff am 1.5.2003.

52 Hauptquelle für diesen Abschnitt ist Levy: Crypto. beat, S. 155 ff.

Institute of Science and Technology (NIST)[53] zusammen mit dem Handelsministerium und auf der anderen Seite die NSA zusammen mit dem Verteidigungsministerium gegenüber. In diesem Zusammenhang sei an die relativ hohe Eigenständigkeit staatlicher Institutionen in den USA erinnert. Wäre es nach dem NIST gegangen, hätte man bereits 1982 RSA zum 'Standard' für den Bereich der asymmetrischen Kryptographie erklärt, analog zum DES als dem normierten Algorithmus für den Bereich des symmetrischen Verschlüsselns. Dies unterblieb auf Druck der NSA,[54] die ja bereits mit der ITAR-Munitions-List unter anderem die negative staatliche Sanktionierung diverser kryptographischer Algorithmen auf ihrer Seite hatte. Mitte der achtziger Jahre jedoch wandelte die NSA ihre Handlungsweise radikal und ging vom bloß negativen, repressiven Reagieren in die Offensive über. Zwischen 1985 und 1987 versuchte sie einen neuen symmetrischen Verschlüsselungsstandard zu etablieren, dessen Verschlüsselungsalgorithmus vollkommen geheim bleiben sollte – in expliziter Abgrenzung zu DES. Obwohl DES damals immer noch offiziell als sicher galt, versuchte die NSA nun durchzusetzen, dass er nur noch für die Kommunikation im Bankgeschäft eingesetzt werden dürfe. COMSEC Endorsement war nicht weniger als der Versuch, den Staat zum direkten Besitzer kryptographischer Zweitschlüssel aller US-Bürger zu machen. Auf diese Weise hätte man technisch bedingt Zugriff auf alle kommunizierten Daten gehabt – und hätte, noch bevor RSA seinen Markt gefunden hatte, diesen bereits absorbiert. Nachdem Ronald Reagan der NSA 1984 mit relativ großen Vollmachten beauftragt hatte, die Sicherheit aller Regierungsrechner zu gewährleisten, versuchte die NSA nun mit dem COMSEC Endorsement Program diese Vollmachten selbstständig auf die zivilen Computer auszudehnen.[55] Damit hatte man sich freilich einen Schritt zu weit hinaus gewagt. Der Republikanische Kongressführer Jack Brooks sorgte 1987 dafür, dass die alte Aufgabenverteilung wiederhergestellt wurde. Das NIST war nun wieder hauptverantwortlich für die zivilen Rechner, der NSA sollte nur noch eine assis-

53 Genau genommen zunächst das *National Bureau of Standards* (NBS); kurze Zeit später wurde dieser Aufgabenbereich ausgegliedert ins NIST.

54 General Accounting Office: Communications Privacy – Federal Policy and Actions – Report to the Honorable Jack Brooks, Chairman, Committee on the Judiciary, House of Representatives. 1993 ⟨URL: `http://www.epic.org/crypto/reports/gao_comm_privacy.html`⟩ – Zugriff am 1.5.2003, Appendix II:2.1.6

55 Shearer und Gutmann, S. 124.

tierende Funktion zukommen. In ihrer Domäne, der Kriegswaffenexportkontrolle, bleibt die NSA freilich die gesamte Zeit über Herr im Haus. Nachdem sich 1990 der Wegfall des Feindbildes aus dem Kalten Krieg kaum noch leugnen ließ, strich die US-Regierung zwar jene Produkte von der 'Munitions List' der Kriegswaffenexportbeschränkung, die gleichzeitig unter die Kontrolle des multilateralen *Coordinating Committee for East-West-Trade-Policy* (COCOM) fielen. Auf Druck der NSA wurde bei kryptographischen Produkten allerdings eine Ausnahme gemacht, weil die COCOM-Mechanismen, so der nun offizielle Standpunkt, nicht ausreichten, um ihre Verbreitung zu drosseln. Software-Herstellern, in deren Anwendungen 'strong crypto' vorkam, erschwerte es die NSA also weiterhin systematisch, solche Programme zu verbreiten – mit der Begründung, dass man die Verbreitung in den USA entwickelter kriegstauglicher Technologien ins Ausland unterbinden müsse.
Anfang der neunziger Jahre veränderte die Geheimdienst-Fraktion der US-Administration ihre Strategie erneut. Nachdem die – vom willfährigen Reagan damals noch geförderte – Machtausdehnung der NSA Mitte der achtziger Jahre gescheitert war, ging man nun auf einen propagandistisch gestützen Umarmungskurs gegenüber dem Handelsministerium. Erstmals war nun in der US-Öffentlichkeit mehr als nur gerüchteweise von der NSA die Rede. Vielleicht noch wichtiger ist jedoch, dass neben den Militärs und ihren Nachrichtendiensten einerseits und der liberalen, handelsfreundlichen Fraktion im US-Regierungsapparat andererseits nun eine dritte Partei den Ring betrat: Die Verfechter der inneren Ordnung, repräsentiert vor allem durch die Bundes-Strafverfolgungsbehörde FBI, interessierte sich nun auch für den öffentlichen Kryptographiegebrauch. Die offizielle Ideologie zum Thema wurde also nicht nur popularisiert, sondern vor allem auch um ein neues Element aktualisiert. Die staatliche Regulation des Kryptographiegebrauchs wurde offen zu einer Schlüsselfrage der zukünftigen inneren Sicherheit erklärt. In einem gemeinsamen Memorandum of Understanding (MOU) von NSA und NIST wurde die Zusammenarbeit der Kontrahenten von einst besiegelt. Eine Arbeitsgruppe, die aus dem MOU von 1989 hervorging, erarbeitete nun etwas Neues, den *Clipper Chip*, in dem der *Escrowed Encryption Standard* (EES) und der *Digital Signature Standard* (DSS) zum Einsatz kommen sollen. Diese technischen Entwicklungen sollten praktisch den Beweis liefern, dass Förderung des kommerziellen Kryptographie-Einsatzes und innere Sicherheit einander nicht ausschließen müssen. Clipper Chip und DSS sollten wenige Jahre später jedoch von einer amerikanischen Öffentlich-

keit wahrgenommen werden, die ganz anders auf derlei Vorstöße vorbereitet war. Dazwischen liegt eine Serie von Ereignissen in den Jahren 1990 und 1991, über die im nächsten Kapitel zu sprechen sein wird.

3.3 Zero-Knowledge, David Chaum und Co.

David Chaum und andere Kryptologen haben seit Anfang der achtziger Jahre immer wieder versucht, das Feld der Kryptographieanwendungen um eine weitere Dimension zu erweitern.[56] Um eine Vorstellung von diesen Anwendungen zu liefern seien zunächst drei klassische Modelle vorgestellt.

1. Bei der Vorstellung des Konzepts der digitalen Signatur hatte sich bereits gezeigt, dass es naheliegt, jeweils die Urheberschaft einer Person im juristischen Sinne digital zu belegen. Man ersetzt die Rechtswirkung der Unterschrift von Hand durch die einer digitalen Signatur. Wie aber kann ich durch die Unterschrift einem Dritten gegenüber etwas beurkunden, dabei jedoch selbst anonym bleiben? Anhand eines konkreten Beispiels: Wie kann ich den Nachweis der Mitgliedschaft in einer bestimmten Krankenkasse gegenüber dem behandelnden Arzt so erbringen, dass er bei seiner Abrechnung mit meiner Kasse zweifelsfrei nachweisen kann, dass ich ihr angehöre – ohne dass diese erfährt, wer ich bin? Und ein weiterer konkreter Anwendungsfall: Wie bekomme ich einen Geldbetrag von meiner Bank zuverlässig zu einem Händler – ohne, dass die Bank etwas über den Händler erfährt oder der Händler Name und Nummer meines Kontos? Mit Bargeld lässt sich ja selbstverständlich anonym bezahlen – aber geht das zum Beispiel auch in einem Onlineshop?

2. Wenn ich mit jemandem per verschlüsselter E-Mail kommuniziere, sollte idealerweise niemand erfahren, was wir uns schreiben. Nun aber einen Abhörer unterstellt, der alles mitlesen kann, was sich auf den von uns verwendeten Kommunikationskanälen abspielt. Im Internet ist das kein sehr unwahrschein-

56 Chaums erste Veröffentlichung enthielt bereits ausführliche, gute Erläuterungen zu seinen in diesem Abschnitt diskutierten Anwendungen: David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24 1981, Nr. 2 ⟨URL: `http://world.std.com/~franl/crypto/chaum-acm-1981.html`⟩ – Zugriff am 3.4.2003.

liches Szenario.[57] Er wüßte dann immerhin, *dass* wir uns schreiben, und auch wann, wer, wem, wieviel. Wie ließe sich verhindern, dass er dies erfährt?

3. Wie kann ich im Internet unter einem Pseudonym erscheinen? Genauer: Kann ich mit einer E-Mailadresse in Erscheinung treten, unter der ich stets zuverlässig erreichbar bin – ohne, dass selbst der mächtige Abhörer aus 2.) erfährt, wer die E-Mails von wo aus abruft und liest?

Alle hier geschilderten Probleme lassen sich durch informationstechnische und kryptographische Kniffe lösen. Bei diesen sogenannten Zero-Knowledge-Proofs (Beispiel 1.) und den von David Chaum entwickelten 'Mixen' (Beispiele 2. und 3.) handelt es sich um relativ komplexe Algorithmen, die explizit inspiriert waren von Diffies und Hellmans Veröffentlichungen; teilweise setzen sie den Einsatz von asymmetrischer Verschlüsselung sogar direkt voraus. Ob es zum Beispiel sinnvoll ist, wie in 2. die Route einer E-Mail zu verschleiern, hängt ganz davon ab, ob ihr Inhalt dem Abhörer nicht ohnhin Rückschlüsse auf Absender oder Adressat erlaubt. Erst bei E-Mails, deren Inhalt verschlüsselt wurde, ist die Verschleierung der Route mit zusätzlichen Mitteln auch auf jeden Fall wirksam.
Die Ideen Chaums bauten jedoch nicht nur systematisch und technisch auf der Erfindung Diffies und Hellmans auf; wie die oben genannten Modelle andeutungsweise zeigen, sollten auch sie qualitativ neuartige Anwendungsbereiche von Kryptographie zum Schutz der individuellen Privatsphäre erschließen. Chaums Versuch, die virtuelle 'Bargeldzahlung' mit seiner Firma Digicash zu vermarkten, scheiterte allerdings. Die Digitalisierung der Märkte geht zwar einher mit der – in dieser Arbeit noch zu untersuchenden – Wertschätzung eines geschäftlichen Zusatznutzens dieser Digitalisierung durch Kryptographie. Aber der kommerzielle Mißerfolg von Chaums digitalem Bargeld deutet bereits darauf hin, dass Dienstleistungen wie 'Schutz der Privatsphäre', oder, in letzter Konsequenz, die Dienstleistung 'Anonymität', kaum in typische Geschäftspläne passen. Auch die Krankenkassen scheinen dieser eher reservierten Haltung zu den Chaumschen Innovationen in nichts nachzustehen.[58]

---

57 Die Funktionsweise der umfassenden 'Traffic Analysis' des Internet-Datenverkehrs durch Geheimdienste wird zum Beispiel dargestellt bei Wobst, S. 387 ff.

58 Die Bewegung der Cypherpunks hat sich dieser neuen Anwendungsbereiche angenommen – wenngleich auch nur innerhalb ihrer eigenen mikroskopischen Subkultur. Vgl. 4.4.

4 1991-1993: It‘s all about Pretty Good Privacy

4.1 Um 1991: Voraussetzungen des Internet-Booms

1989 wurden die Weichen gestellt, um aus dem Internet ein Massenkommunikationsmittel zu machen. Die frühen kommerziellen Internet-Diensteanbieter MCI und CompuServe wurden in diesem Jahr an die offiziellen Internet-Strukturen des amerikanischen Hochschulnetzes angeschlossen, und mit ‘The World’ gab es den ersten kommerziellen Anbieter von Dial-Up-Internetzugängen per Modem von Zuhause aus. Aufgrund dieser strukturellen Veränderung der Nutzung und der Zugangsbedingungen des Internets ist die oft zitierte Zahl von erstmals mehr als einhunderttausend registrierten Internet-Hosts 1989 erklärlich als der Anfang der Explosion des kommerziellen Internet-Wachstums in den darauffolgenden zehn Jahren.
Zwei Jahre später, 1991, schafft Tim Berners-Lee am Genfer Kernforschungszentrum CERN mit der Erfindung der Seitenbeschreibungssprache HTML eine weitere entscheidende Grundlage für die Popularisierung der Computernetzwerke. Elektronischer Text konnte nun durch sogenannte Hypertext-Referenzierung – mittlerweile jedem geläufig als *link* – gleichzeitig ein Verweis sein auf andere Seiten im universellen Namensraum der HTTP-Adressen. Dieses Referenzsystem lässt sich ‘intuitiv’ benutzen, ein Mausklick auf die Referenz ist bereits der Befehl an das Anzeigegerät, eine Kopie der referenzierten Seite zu holen und lokal darzustellen. Die auf viele verschiedene Rechner in vielen Ländern verteilten elektronischen Dokumente würden ein einziges ‘World Wide Web’ bilden, das sich durch Maschinenhilfe als ein rein ‘semantisches Netzwerk’ erschließen lässt. Den Maschinen kommt dabei konsequent eine dienende Rolle zu. Durch die Standardisierung der Sprache HTML und des Datenübertragungsprokolls HTTP funktionieren die links auf jedem Rechner, und es ist gleichgültig, auf was für einem Rechner und wo auf der Welt das abzurufende Dokument liegt. Das WWW sollte ein universeller Raum allseitig zugänglicher Informationen sein, die untereinander sozusagen nur inhaltlich, als Texte, miteinander verknüpft sind – ohne dass diese Struktur jeweils Rücksicht nehmen müßte auf aktuelle technische Entwicklungen oder Unterschiede von

Computern oder Netzwerken.[59] Unverkennbar steht an der Wiege des WWWs ein Idealist des freien Informationsaustausches.

4.2 PGP, oder: PKC in der Regie privater PC-Benutzer

Phil Zimmermann, Friedensaktivist sowie Computerbastler und -programmierer, kam in den achtziger Jahren mit der Public-Key-Kryptographie in Berührung, als seine Arbeit durch ihre Nützlichkeit für die Hardware-Einbindung des bis heute wichtigsten PKC-Algorithmus RSA aufgefallen war.[60] Er kannte auch das Programm 'MailSafe' von den RSA-Machern, und versuchte zunächst, sie davon zu überzeugen, ihm für eine Neuentwicklung eines populären Verschlüsselungsprogramms eine kostenlose RSA-Lizenz zu erteilen. Die bekam er nicht, und aus verschiedenen Gründen brachte Zimmermann es nun zu einer recht ungewöhnlichen Konsequenz, die für die weitere Geschichte der angewandten PKC gleichwohl sehr bedeutsam werden sollte. Er entwickelt ein auf den ersten Blick eher unscheinbares Programm für den privaten PC. Ein kleines, kostenloses Kommandozeilenprogramm, das nicht verknüpft war mit einer umfangreichen Büro- oder Internetanwendung. Zimmermann mißachtete nun einfach das RSA-Patent, indem er dieses Programm kostenlos auf den Bulletin-Board-Systems zu Verfügung stellte. Pretty Good Privacy (PGP) war nach den Worten des RSA-Chefs Jeff Bidzos nicht anderes als „Pretty Good Piracy".[61] Mit den einfachsten Mitteln erledigte PGP

1. starke symmetrische Ver- und Entschlüsselung von sowohl Binärdateien als auch einfachen ASCII-Zeichenketten;[62]

2. digitale Signatur;

59 World Wide Web Consortium (W3C): Semantic Web. 2001 ⟨URL: `http://www.w3.org/2001/sw/`⟩ – Zugriff am 1.5.2003.

60 Zur Biographie Zimmermanns ausführlich Levy: Crypto. beat, S. 187 ff.

61 William M. Bulkeley: Cipher Probe: Popularity Overseas Of Encryption Code Has the U.S. Worried. The Wall Street Journal LXXV 28. April 1994, Nr. 138 ⟨URL: `http://www.interesting-people.org/archives/interesting-people/199405/msg00000.html`⟩ – Zugriff am 3.4.2003.

62 ASCII ist die Abkürzung für American Standard Code for Information Interchange. ASCII umfasst den Zeichensatz einer amerikanischen Schreibmaschinentastatur und ist bis heute ein Minimalstandard vieler Intertnetprotokolle, zum Beispiel bei der Übertragung von E-Mails. Um der historischen Genauigkeit willen: Der von Zimmermann selbst entwickelte symmetrische Verschlüsselungsalgorithmus für PGP 1 stellte sich rasch als fehlerhaft und damit leicht zu

3. Schlüsselaustausch der verwendeten Sitzungsschlüssel nach RSA;

4. Zertifizierung und Selbstzertifizierung von RSA-Schlüsseln[63] und

5. eine rudimentäre Verwaltung solcher öffentlicher Schlüssel sowie eigener, passwortgeschützter Schlüsselpaare.[64]

Hinsichtlich des Einsatzes von RSA unterschied sich die nicht-kommerzielle Anwendung PGP in doppelter Hinsicht stark von vergleichbaren Programmen, die damals verfügbar waren. RSA wurde in seiner starken, und nicht in einer zwecks legaler Exportierbarkeit abgeschwächten Variante implementiert. Vor allem jedoch legte das Programm es nahe, mittels weniger einfacher Befehle in völlig eigener Regie Schlüsselpaare zu erstellen und fremde Schlüssel zu zertifizieren.
Ein mit PGP[65] erzeugter Schlüssel sieht so aus:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.3.2 (GNU/Linux)

mQENAzxaitUCuwEIAMZZF7+pJmrNTjDyVQ6U8SwLnVz37ble1XUhIpvYLaRNanLl
IyGIuAOSgDrpYaaUzAcUcqCBqDLfkFsT2TaxJ0wiO/sm9aQPWZ0iw3pvx3wQirlG
Ev5gcuyJ8ISkZJ5VBvc+dcrs00/dm+BRbuNK8Xph541NTDYivZCG+ftCPUNlzj0g
w04VASS8q7QhrJoyqYz3Mrc23xkxwO5O0ByYt27dYwwm9kfh3udfyd8QkxUAh9xf
ywTi6rRe1wxEgWQG1UbnVyacBykPuc+4dxgici4Sv29BgP+23jmKJdwNp6bxkk6e
Zm3GsY1oAuFG9On+WUGkKH3AWmc/ixJSeA9Wr+sABRGOKExhbWJlcnQgSGVsbGVy
IDIgPGxhbWJlcnQuaGVsbGVyQGdteC5kZT6JARUDBRA8WorVixJSeA9Wr+sBAXYc
B/964CvFkTrx3TpEXm2B0g71gQQqb+v0/V0YIldm95Y93SXix3d0L+/dzj0LveVw
fVKt5iqj4P1/JGv7G8xA7XG7h89EbcVxN0e/0GBZVJkqYHUpNlWEnahfsIfgCAqW
b6ioXY1cyO9b07eYm/umLwMd3Y8aI9tHEZfM3pPYMVIMxJStVztXm9SfV54a4DpR
8dZqKYPx7E7x06RGklKlNONFHHAQ8ZgR7+mNjCezuk7wZhmTQk3eLFwPeMcTNr1r
ASsIBq7y8arbZv9vPVQ5agMFvxIjIom7kdCF60OllzDUxu1v7ILo4rSOjL06ev1L
Amjv1+nDhcivKVlINVvFJmVEiQEVAwUQPFqj4e5HTCBjwSFzAQHLagf/d+AdAhaA
94SXMd3NTZWI+yZJPsWVu9gt5oYv5DajBrB5/J78GwNrkn9xy1bAL6OlAKvUg5K9
au5FCGvMnEGvge7TVBt19GJMZbmUpKjM26VzXKnRyPJFC2nKeURdJ+aWYfm9OP/e
hfTKM2ykHhax/YWnoIn2SjoQMhSW3UgIVvTfu2Bu4Qhze0+NSc9kbBusGBytDEOH
```

knacken heraus. IDEA, der in den Versionen ab 1992 (PGP 2.0) verwendete Algorithmus, gilt bis heute als sicher.

63 Ebenfalls erst ab PGP 2.0.

64 Philip Zimmermann: PGP(tm) User‘s Guide. Boulder, Colorado, 1994.

65 Dieser Schlüssel wurde mit dem PGP-kompatiblen Programm GnuPG erzeugt, vgl. 6.2. Zur Demonstration dient hier ein Beispiel, das sich auf die Person des Autors bezieht.

```
mQP3otf4sHqcczKA2GPgeQm6YB1d3vNhV9PAep3fINgVpgxTj8jm5ypOFaY/V6ZD
f5xkroQJFlfZor2oV4dGWQYuE+a591+nlIWW0SlS+oBADddyf4U6FpCvZDAO3ya4
MVRIJVN0jueCGQ==
=L5ZY
-----END PGP PUBLIC KEY BLOCK-----
```

Wenn diese Arbeit hier als Datei vorliegt, kann der obenstehende Textblock herauskopiert und in den Schlüsselbund einer PGP-Installation eingefügt werden. Im Schlüsselbund wäre dann zu sehen, dass es sich um einen PGP-Public Key handelt, dem ein Eigentümer namens „Lambert Heller“ zugeordnet ist. Als Eigentümer des Schlüssels braucht keine natürliche Person aufzutreten; stattdessen könnte er auch einem Pseudonym zugeordnet sein. Im folgenden Anwendungsbeispiel wurde eine Nachricht mit dem Secret Key digital unterschrieben, der zum oben angegebenen Public Key gehört; die Korrektheit der digitalen Signatur lässt sich mit einem lokal installierten PGP prüfen, in dessen Schlüsselbund der Public Key eingebunden worden ist.

```
-----BEGIN PGP SIGNED MESSAGE-----

Dieser Satz ist digital unterschrieben mit dem oben angegebenen
Schlüssel.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.3.2 (GNU/Linux)

iQEVAwUBPs0AKosSUngPVq/rAQEHnggAtFai69n1frmesYrPa3ex7W6ARXROk89s
QIwGAJTc8lXk05+xK3cclVEFMumx8QbToRMlsVVl5JNzdUQwmVyK6XIUeoPFqsml
Wq7ggXtj+rjMD9ao3ZIB2LjTLEvFVbtZJ4UH+52pdy8U4OoTAs1gsBTrsllt kwB8
0ZTbN/BpLyzkLkHfcnzOS5X7XBQjrl0ZtGZ+CG4Its+jEWcAmFNHGHSHSk6Ckd3t
PrPUGzUAKGnOAOQjfzrAtilLIb0H0wNLTzai1CjCzSLk2FWulDkjn5OkaYDuF1U9
R8K3DWI1rgxvU0e0VciLv37SoUa2mWvwRi/nBtSR9GUbQ6O5Fahgxg== =Il1l
-----END PGP SIGNATURE-----
```

Die folgende Nachricht besteht aus demselben Satz, verschlüsselt an den Schlüssel des PGP-Erfinders Zimmermann. Zimmermanns Public Key hat der Autor von einem öffentlich zugänglichen PGP-Keyserver abgerufen.

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.3.2 (GNU/Linux)

qANQR1DBwU4Dou0bwSIJMtcQB/4jtNjoeCFk/z0y7l06OOwqh/FYS0FLgeNnu0hA
```

```
AT/hQztEzDzuLblmnA2+xtNfsHhvBChEfDGxzbRAPSCDDbDdw1oEzAEgz8IKRg/U
yCuh+KokpHKFtzb2feWKLMackbPHYRzbRuTkTrSYRzwEnxuSIiRQ2T/1TaQBfHHM
mEiaSnQX6+9uIEfsJBy91NZ399H16UIrCMCUrcP8IWkpY6XVxz4YAcw+cjvXNYdU
B99RggoiIaqabyqvR+uui6nnMdZErQi+XOE7tEq6kubHSk4ACFmRAbmcBQ9Mji29
aehqsUgr6s14V1yCcfHuAX2dR0vXrmmitCeRxPJfWtfEvtb3CAC2FGGDWIE5t7EC
xBdwpD+ocNprvPu3NhIUc2Wv50oEcYH2ceR8CPZraMKEBkuRM5wp+0D9Y0YI2tkz
KM5wZWRbVEJHeMfWz486hu69Sd6wqtoFLIZElbpvT5768TpnzmsfuukppO84Whxl
EV9zhiMKYxNuHU5itiUunRn3hjdAsRsEICbLAq+Rgol4vsrXYn3JiHW6YgomxFg5
FmBdqWo4nHoiUR/JPs7SQkPK9fEN4rNVk4djArXK3LlFEe6xkHlXO3XfkhH0yhPG
fe6zr+RO6lOvOrFGijFRTOP5jhPDyioCom4NGtTERE0AoEB1hji2hBZZTdob9qp1
ue6tv90eycDNyQm7G6xQgHcF8IbNm4cLBniKwSqF4jazRkYrUeaAyC1FRkelcp0j
n7pPPe/+sZ8vdCVosPWQMTA0cbcCxB2jdmM1jsAbnEMj4kJDI7ey4CZSff/2YIby
BZBp19BlNfM798Z2uBP3l6TU0OEHpWuBJg8viD5zDZxHaAb7QhxlLsdL9CU5a+4i
23oUy2C/EOrwcN4kQPpsxCKs72I15NBR3r/VL5ssyUVf3VIDUbu4qdsy+sC6Fm6E
PCCT6aj4U2088eFVkYYdAlC9UvhjEsfmyXBOVy6DI9aR9QNU1QuLdGdYGFZ67NRS
9HTm9x+O1YpmufY3QRj95OPhjSUcX5fcfjRKiwojkEJfM9bfJSgfkd7vKYCdGSFl
ci/gzayqJRvgRmEreFvnhHSG9JLtVxFZeiCT76xTHZAxzgG9NTVEn2BK1w5RKafd
PQIbqTXPkkbwHBhOiZLgw/b79fXXZqhyWXlzgtiCcasXBhmBkcJgzo5JYPkYrv0X
btcMOW8rSwk7sR+At+Mb4JloJc+l5Q== =/haG
-----END PGP MESSAGE-----
```

Die verschlüsselte Nachricht ist wiederum mit dem Public Key des Autors digital unterschrieben. Aber lediglich Philip Zimmermann als Adressat der Nachricht ist in der Lage, zu überprüfen, ob es sich tatsächlich um denselben Satz und dieselbe Signatur handelt. Für eine zuverlässige Überprüfung meiner Signatur bräuchte er sich nicht allein darauf zu verlassen, dass mein von öffentlichen PGP-Keyservern abrufbarer Schlüssel auch tatsächlich mir gehört.

Eine Manipulation von Schlüsseln während zum Beispiel einer Übertragung über Internetverbindungen kann mit den Mitteln von PGP ausgeschlossen werden, indem vor der Zertifizierung anhand des 'Finger Prints' die Echtheit eines Schlüssels überprüft wird. Der Finger Print, eine unverwechselbare Prüfsumme des Public Keys, wird dazu einmal auf demjenigen Rechner erzeugt, auf dem der Original-Key erstellt wurde, und ein weiteres mal auf einem beliebigen Rechner, der eine Kopie des Schlüssels hält. Die selbstgemachte Zertifizierung und der einfache Weg dorthin, der Austausch von Finger Prints, scheinen wie dafür gemacht zu sein, das Versprechen der PKC einzulösen, den Individuen alle Möglichkeiten zu eröffnen, die sich daraus ergeben, dass sie spontan und relativ voraussetzungsarm selbstgemachte Schlüssel untereinander austauschen können. Neal Stephenson hat in *Cryptonomicon* den Schlüsseltausch in den Alltag seiner Romanhelden eingehen

lassen. PGP heisst im Roman Ordo.
Randy, eine Hauptfigur des Romans, schlendert über den Flughafen von Tokio und telefoniert mit seinem Kollegen Avi.

> „'Ich habe einen Fingerabdruck für dich', sagt Randy.
> 'Schieß los.'
> Randy betrachtete seine Handfläche, auf die er mit Kugelschreiber eine Ziffern- und Buchstabenfolge geschrieben hat. 'AF 10 06 E9 99 BA 11 07 64 C1 89 E3 40 8C 72 55.'
> 'Registriert', sagt Avi. 'Kommt von Ordo, stimmt's?'
> 'Stimmt. Ich habe dir per E-Mail den Schlüssel von SFO geschickt.'"[66]

PGP-Benutzer sollten nach den Vorstellungen Zimmermanns vollständig auf ein *Web of Trust* gegenseitiger Zertifizierungen bauen können, in dem eine zentrale Zertifizierungsinstanz möglich, aber nicht zwingend erforderlich ist. Eine weitere Stärke des Web of Trust liegt im Verzicht auf eine verbindlich durchgesetzte Policy der Zertifizierung. Verschiedene, grob definierte Stufen des Vertrauens in die Echtheit eines Schlüssels sind vorgesehen; inwieweit eine Zertifizierung gegebener Stufe als hinreichend vertrauenswürdig anerkannt wird liegt somit im Ermessen der Einzelnen. Diese sind damit allerdings auch sehr nachdrücklich als aufgeklärte Teilnehmer des Web of Trust vorausgesetzt.
Es ist kein bloßer Zufall, dass Zimmermann das Web of Trust im selben Jahr erfand wie Tim Berners-Lee das *semantic web*. Die späteren expliziten Übergänge zwischen diesen beiden webs sind mittlerweile Legion.[67] Das Web of Trust bildet ein Netzwerk zwischen Einzelnen, das eine technische Grundlage für den selbstbestimmten und dabei zuverlässigen Gebrauch von Kryptographie in der Individualkommunikation abgeben soll. Das semantic web ist die selbstgewählte Unterwerfung des individuellen elektronischen Publizierens unter eine Metastruktur, die für die allseitige Zugänglichkeit und Auffindbarkeit der publizierten Informationen eine technische Grundlage abgeben soll. In beiden Fällen soll die selbstbestimmte Unterwerfung unter eine technisch ausdifferenzierte Infrastruktur im weitesten

66 Neal Stephenson: Cryptonomicon. München, 2001, S. 39.

67 So ließ es sich Berners-Lee nicht nehmen, Public-Key-Cryptography später als wichtiges ergänzendes Element in das Konzept des semantic web aufzunehmen. Eine spezielle Anwendung von PGP findet mittlerweile in der Community der Weblogs an Bedeutung, die *friend of a friend*-Dateien (FOAF). Hier sind Verweise auf freundschaftliche oder sachlich-inhaltliche Nähe zwischen Web-Publizisten Gegenstand einer PGP-Signatur.

Sinne dem freien Fluß von Informationen dienen. Auch in ihrer sozialen Funktion ähnelt sich die Geschichte dieser beiden webs. Beide stellen relativ hohe Anforderungen an das Wissen und Engagement der beteiligten Individuen; beide waren modellbildend für spätere, kommerziell motivierte Innovationen im Bereich des elektronischen Publizierens im Internet und der Public-Key-Cryptography.

4.3 PGP als Waffe zur Verteidigung der Privatsphäre

Zimmermann legte es zunächst nicht darauf an, mit seinem Programm Geld zu verdienen. Seine demonstrative Nachlässigkeit gegenüber dem RSA-Patent und vor allem gegenüber den Vorschriften der Kryptographie-Exportbeschränkungen brachte Zimmermann einigen Ärger ein. Als PGP bereits weit verbreitet war, wurde der PGP-Erfinder mit Prozessen überzogen; die Androhung hoher Geld-, gar Gefängnisstrafen stand im Raum.[68] Die Installationspakete der frühen PGP-Versionen waren stets mit einer Textdatei versehen, in der auf die rechtliche Verfolgung Zimmermanns eingegangen und um Spenden an einen Solidaritätsfonds gebeten wurde. Worin lag nun der politische Charakter der Herausgabe von PGP, die Zimmermann all diese 'Begleiterscheinungen' seiner Tätigkeit als Programmautor wie selbstverständlich ertragen ließ?

Zimmermann unterstellt, dass die Regierung der Masse der einfachen Computeranwender etwas vorenthält, worauf diese ein Recht haben.[69] Um die legitime Alltäglichkeit eines Schutzes der individuellen Privatsphäre darzustellen, greift Zimmermann auf eine Metapher zurück, die zur Beschreibung von PGP berühmt und immer wieder fälschlich Zimmermann zugeschrieben wurde. E-Mails, so Zimmermann, wären ohne (starke, asymmetrische) Verschlüsselung wie Postkarten; der Kryptographiegebrauch käme in seiner Funktion der Verwendung von Briefumschlägen gleich.[70]

---

68 Bulkeley.

69 Im Abschnitt „Why Do You Need PGP?“ von Zimmermann stellt Zimmermann seine diesbezüglichen Argumente sehr anschaulich und kompakt zusammen; in seinen späteren Veröffentlichungen wird vor allem dieser vielzitierte Text stets aufs Neue variiert.

70 Tatsächlich findet sich die Envelope-Metapher jedoch bereits zehn Jahre zuvor bei Gustavus J. Simmons: Introduction. In Gustavus J. Simmons (Hrsg.): Secure Communications and Asymmetric Cryptosystems. Boulder, 1982, AAAS Selected Symposia (new series), S. 3.

Das Beharren auf der Selbstverständlichkeit des Kryptogebrauchs kommt auch darin zum Ausdruck, dass bei Zimmermann[71] immer dann, wenn es darum geht, die Funktionsweise von PKC anhand von Beispielen zu illustrieren, aus dem Bereich der privaten Individualkommunikation geschöpft wird. Nie ist es eine Firma A, die mit ihrem Kunden B oder ihrem Angestellten C kommunizieren will, sondern stets sind es 'Alice' und 'Bob', die sich 'etwas Vertrauliches mitzuteilen haben'.[72]

Die spezielle Konstellation der Ideologie um PGP ergibt sich daraus, dass sich das Beharren auf der Selbstverständlichkeit des privaten Gebrauchs avancierter Verschlüsselungstechnologie im selben Augenblick kämpferisch und ohne Kompromissbereitschaft gegen die Regierung wendet. Die Regierung gerät bei Zimmermann auf eine charakteristische Weise ins Visier – und ebenso bei vielen weiteren, die von ihm bis heute inspiriert worden sind. Der erste und hauptsächliche Einwand gegen den Regierungsstandpunkt ist stets, dass diese auf ein Verbot der Kryptographieanwendungen hinauswolle. Dieses Interesse wird im zweiten Schritt damit erklärt, dass die Regierung ihre Potenz, alles abzuhören, nicht in Frage gestellt sehen möchte. Eigentümlicherweise erhält man so im zweiten Schritt dasjenige, was zu allererst den Anlass, den materiellen Grund dafür abgibt, als Einzelner auf die Idee zu kommen, etwas verschlüsseln zu wollen.

Abb. 2: *1991 – Die Technik als das Mittel einer anonymen, umfassenden Bedrohung der Privatsphäre.*

Zimmermann ist jedoch stets und von Anfang an klar, gegen welche bestimmte Bedrohung sich der Schutz der Privatsphäre richtet – anders als in Diffies und Hell-

71 und den Cypherpunks, vgl. 4.4.

72 Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2. Auflage. New York, 1996, S. 30.

mans Aufsatz *New Directions*,[73] in dem die Bedrohung der Privatsphäre der elektronischen Individualkommunikation noch rein technisch gefasst war, von einem abstrakt austauschbaren Dritten verkörpert wurde. Der Unterschied zwischen Diffies und Hellmans Aufsatz einerseits und Zimmermanns *PGP(tm) User's Guide*[74] andererseits zeugt von einer intensiven Auseinandersetzung mit der Entwicklung der PKC und den Bedingungen ihres Gebrauchs in den vergangenen 15 Jahren. Der Ausbau der Überwachung der Telekommunikationssysteme wird bei Zimmermann explizit und als Grund thematisiert: PGP war von vornherein politische Software, ein Programm zur Vereitelung bekannter Absichten der Regierung.
Der systematische Zusammenhang zwischen der Potenz, alles jederzeit abhören können zu wollen, und der Regulierungshoheit über den Einsatz von Verschlüsselungstechnik liegt im Hoheitsanspruch der Staatsgewalt über die gesamte elektronische Kommunikation ihrer Bürger. Dieser allgemeine Sachverhalt wird von Zimmermann jedoch nicht diskutiert. Die Betonung eines 'Recht auf den Kryptographiegebrauch' ist mehr als ein notorischer Tick Zimmermanns, sondern korrespondiert mit der Aneignung staatlicher Zwecke. Wenn Zimmermann im *PGP(tm) User's Guide*[75] feststellt, dass dem offiziellen und richtigen Auftrag der staatlichen Verbrechensbekämpfung und Wirtschaftsaufsicht nicht gedient sei, da sich die Repression gegen den Kryptographiegebrauch dieser speziellen Teilbevölkerung ohnehin nicht durchsetze, führt er eine Diskussion über die richtigen Mittel einer staatlichen Politik, deren Zwecke bereits als im Großen und Ganzen richtig vorausgesetzt sind. Somit ist in Zimmermanns Fassung der Kampf um die allseitige, private Zugänglichkeit 'starker' kryptographischer Produkte, in dem PGP als Waffe dienen soll, von vornherein der Kampf einer Bürgerrechtsbewegung, die in erster Linie an die Recht setzende Gewalt appelliert, den Gesetzesbruch hingegen nur als ultima ratio in Kauf nimmt. Man wird sehen, dass die Cypherpunks im Gegensatz dazu zwar auch für Bürgerrechte kämpften, diese Rechte in ihrem Verständnis aber nur Teil des Verhältnisses der Bürger untereinander waren, ganz jenseits einer Unterwerfung der Bürger unter eine Zentralgewalt.

---

73 Diffie und Hellman.

74 Zimmermann.

75 A. a. O.

4.4 Technik-Angst als Ausgangspunkt von libertärer Krypto-Euphorie

Am Niedergang der Geheimen Kabinettskanzleien im 19. Jahrhundert[76] wird deutlich, dass der Gedanke des Datenschutzes nicht erst seit dem Beginn des Computerzeitalters seinen Ort in der bürgerlichen Gesellschaft hat. Kennzeichnend ist jedoch, dass sich Begriffe wie 'Datenschutz' erst in den siebziger, in Europa vielleicht sogar erst den achtziger Jahren durchsetzten. Während 'Artificial Intelligence' der fruchtbare Leitbegriff der zeitgenössischen Informatik war und in der Science Fiction die Angst vor einem Maschinenaufstand gegen die Menschheit kultiviert wurde, hatte der 'Einzug des Computers nach Zuhause'[77] noch kaum stattgefunden. Je weniger man über die Wirklichkeit 'des Computers' wusste, desto besser taugte er offenbar als Projektionsfläche für eine Zukunft, in der die Macht beinahe mehr von den Computern selbst als durch sie ausgeübt wird. Die Generation der in den achtziger Jahren erst Aufwachsenden konnte sich schnell und handfest davon überzeugen, dass der Computer wirklich ein so dummes elektronisches Etwas war, wie es in populären Erklärungen der Computertechnik in der damaligen Zeit so gern behauptet wurde. Die Apple-II-Rechner im Informatikraum der Schule konnten, bevor man ihnen in PASCAL die Anweisung dazu gegeben hatte, nicht mal „Hallo Welt!“ ausgeben. Dabei war die Technikeuphorie, die nahezu unterbrechungslos auf die Technikangst zu folgen schien, nicht weniger ideologisch. Die Tatsache, dass es tatsächlich einen Zusammenhang gibt zwischen dem Übergriff auf die Privatsphäre der Einzelnen und dem Computer als *Mittel* dieses Übergriffs, hatte der große Kryptologe der Nachkriegsära, Horst Feistel, in weiser Voraussicht bereits 1973 beschrieben:

> „Computers now constitute, or will soon constitute, a dangerous threat to individual privacy. Since many computers contain personal data and are accessible from distant terminals, they are viewed as an unexcelled means of assembling large amounts of information about an individual or group.“[78]

---

76 Vgl. 1.3.

77 Vgl. Abb. 1.

78 Horst Feistel: Cryptography and Computer Privacy. Scientific American 228 Mai 1973, Nr. 5.

Was der ehemalige Kollege Martin Hellmans hier als Hypothese ausmalt, war bereits die klare Fassung eines Problems, dessen Diskussion heute längst Bücherregale füllt. Selbst die Rolle der Vernetzung von Informationssystemen ist zutreffend hervorgehoben.[79]

Aus Sicht der Skeptiker bot Kryptologie die Möglichkeit dessen, was später oft als 'subversive Technikaneignung' bezeichnet worden ist. Diese Computeranwendungen waren für sie, die einfachen Normalbürger, nicht vorgesehen; sie dennoch voranzutreiben hieß zum einen ein veraltetes Technik-Entwicklungsmodell hinter sich zu lassen und sich auf diese Weise selbst an die Spitze eines technischen Fortschritts zu stellen. Zum andern ließ sich so der Widerspruch bewältigen, sich selbst an neue technische Realitäten anzupassen, einer Veränderung etwas abgewinnen zu können, die ohnehin passiert, unabhängig von der eigenen Zustimmung – und dabei dennoch eigenständig zu bleiben, der Regierung sogar ein Monopol streitig zu machen. Es gab also gute Voraussetzungen dafür, um anhand ein- und desselben Themas, Privacy,[80] vom radikalen Skeptiker zum flammenden Apologeten der neuen Technik zu werden. Apologet ist in diesem Zusammenhang keine allzu polemische Übertreibung, denn bereits von Anfang an war das Vertrauen ins rebellische Potential einer individuellen Techniknutzung, die notfalls auch gegen den Strom durchgehalten werden müßte, mindestens ebenso ausgeprägt wie der historische Optimismus, auf der Seite der Eigendynamik der technischen Entwicklung selbst zu stehen.

Eine Rede, die auf der *Future of Freedom Conference* 1987 gehalten wurde, zeigt exemplarisch, wie zu diesem Zeitpunkt liberale Programmierer den Zusammenhang von Technikentwicklung und der Gefahr für die persönlichen Informationen neu

---

79 Es versteht sich beinahe von selbst, dass in dem Artikel eine sehr technische, kryptographische Lösung dieses Problems unterbreitet wird. Feistel stellt einen revolutionären neuen Cipher namens Lucifer vor, der unter seiner Leitung – und der damals obligatorischen Beaufsichtigung seitens der NSA – bei IBM entwickelt worden war, und der bereits wesentliche Merkmale seines berühmten Nachfolgemodells DES enthielt. (Vgl. 2.2.)

80 Dieser Begriff wäre mit Privatsphäre unzureichend übersetzt. Der Merriam-Webster Dictionary verzeichnet als die beiden Hauptbedeutungen von „privacy" „a: the quality or state of being apart from company or observation :SECLUSION b: freedom from unauthorized intrusion (one's right to privacy)". „Privatsphäre" hingegen bedeutet laut Duden, Deutsches Universalwörterbuch, vor allem „die: private (1 a) Sphäre, ganz persönlicher Bereich". Das ist jedoch lediglich eine Nebenbedeutung von „Privacy", der Nachdruck liegt hier vielmehr auf der Negation: Privacy meint vor allem das Nichtgeschehen der Teilnahme Anderer.

herstellten. Der PKC-Gebrauch wurde glatt als das in wenigen Jahren anstehende Ende jeglicher staatlicher Überwachung interpretiert:

> „Within a few years, [...] Technology will not only have made wiretapping obsolete, it will have totally demolished government's control over information transfer.“[81]

Um 1991 inspirierte die Krypto-Euphorie eine neue soziale Bewegung, die Cypherpunks. Diesen Namen hatte Jude 'St Jude' Milhon erdacht. Es handelt sich um eine Zusammenziehung des kryptographischen Fachbegriffs 'Cipher' und der fiktiven, hochtechnisierten Lifestyle-Figur des 'Cyberpunks' in den Romanen des Science-Fiction-Autors William Gibson. St. Jude ist nicht nur die Namensgeberin der Cypherpunks, sondern auch eine der wenigen Frauen in dieser Bewegung. Ganz wie in der Generation der großen kryptologischen Erfinder in den siebziger Jahren überwogen auch hier weiße männliche US-Amerikaner, die gerade Informatik studierten oder studiert hatten.

Die Cypherpunks waren von vornherein über den falschen Gegensatz von Technik-Angst und Krypto-Euphorie hinaus.[82] Anhand des Schicksals der kryptologischen Erfindungen neuer Richtung und der zunehmenden gesetzlichen Regulation des Datenverkehrs wussten sie bereits Anfang der neunziger Jahre, dass das bloße Vorhandensein und individuelle Benutzen einer Technik wie der asymmetrischen Verschlüsselung auf nichts eine Antwort war. Zur Aktivität der Cypherpunks gehörte daher stets Technikentwicklung (also zum Beispiel Weiterentwicklung des Quellcodes von PGP) und zugleich die öffentliche Reflexion darauf, wie die Regierungen – später auch die Entwickler proprietärer Software – mit dem technischen Fortschritt umgehen wollten.

Die 'physischen' Meetings der Cypherpunks, die hauptsächlich über eine Mailingliste mit mehreren hundert Teilnehmern kommunizierten, waren nicht nur Schauplatz politischer Diskussion, sondern wurden rasch auch zu 'Key Signing Parties'. Bei einer solchen 'Party' identifiziert man sich gegenseitig als Besitzer des PGP-Schlüssels mit einem bestimmten Finger Print, und webt so am 'Web of Trust', der

---

81 Chuck Hammill: From Crossbows to Cryptography: Thwarting the State via Technology. Culver City, 1987 ⟨URL: `http://www.t0.or.at/crypto/crossbow.htm`⟩ – Zugriff am 1.5.2003.

82 Hauptquelle für die folgende Schilderung der Cypherpunk-Aktivitäten ist Levy: Crypto. beat, S. 187 ff.

Zertifizierung nach dem Modell von PGP. Die aktive, aber keineswegs selbstlose Beteiligung an einer Gebrauchsweise von Kryptographie, die politische und soziale Implikationen hat, wurde so zum kulturellen Habitus erhoben – ein markantes Beispiel für die hochgradige Verschränkung von Lifestyle, Politik und Technik, dank derer die Cypherpunks sofort eine große Ausstrahlung hatten. Cypherpunk zu sein, war gleichzeitig sowohl zeitgemäß als auch exzentrisch, technisch-pragmatisch und politisch radikal.

Neben ihrer kulturellen Aura und der Bedeutung für die technische Fortentwicklung der PKC-Anwendung hatten die Aktivitäten der Cypherpunks einen direkten Einfluß auf den Verlauf der kryptopolitisch bewegten neunziger Jahre. Bruce Schneiers Buch *Applied Cryptography*[83] war 1994 der markante, öffentlich scharf beobachtete Testfall für das Funktionieren der Waffenexportkontrollen in der Zeit nach dem Mauerfall und Zimmermanns PGP-Alleingang. Immerhin enthielt das Buch quasi die gebündelten, anwendungsfertigen Resultate der Kryptographientwicklung der bis dahin vergangenen zwanzig Jahre – als Code in der Programmiersprache C sowohl im Buch abgedruckt als auch digital auf einer beiliegenden CD. Das salomonische Urteil über *Applied Cryptography* lautete schließlich, dass zwar sein gedruckter Text durch das Recht auf freie Rede gedeckt sei und somit sein Export ins Ausland nicht verboten werden könne, dass dieser grundrechtliche Schutz sich jedoch nicht auf den Inhalt der CD erstrecke.

Diese rechtliche Situation wurde von den Cypherpunks Lucky Green und Stale Schumacher als eine einzige Herausforderung an ihre Auslegungskunst und technische Raffinesse aufgefasst. Die gestellte Aufgabe lautete in ihren Augen etwa so: Finden Sie eine Weg, den in den USA geschriebenen jeweils aktuellen PGP-Programmcode legal im Ausland zu verbreiten! – Der Lösungsweg bestand darin, den Programmcode in C so auf die Seiten eines Buches zu drucken, dass die Bögen optimal für einen einzigen Zweck präpariert waren: Von Scannern eingelesen und mit Hilfe von Zeichenerkennungsprogrammen wieder zurückverwandelt zu werden in eine digitale Zeichenkette. Das resultierende Druckwerk umfasste jeweils mehrere Bände mit insgesamt mehr als Zwölftausend Seiten. Es war aber kein Problem, auf ‘Hacking In Progress’-Konferenzen viele Freiwillige zum Einscannen der Buch-

83 Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York, 1994.

seiten zu rekrutieren. Kaum war in den USA eine neue PGP-Version erschienen, konnten Menschen auf der ganzen Welt völlig legal Stale Schumachers Website www.pgpi.org („PGP International“) ansurfen und sich ihre Kopie der gleichnamigen PGP-Variante, PGPi, besorgen.

Die Guerilla-Taktik gegen das US-amerikanische Exportkontroll-Regime entsprach vollkommen dem individualistischen Anarchismus der Cypherpunks,[84] nicht nur wegen der Verächtlichmachung des Regierungshandelns, sondern auch wegen dem konstruktiven Beharren auf dem positiven Sinn wahrhaft freien Handels. Die spezifische Zusammensetzung der Cypherpunk-Ideologie als einer Spielart des individualistischen Anarchismus soll im folgenden aufgezeigt werden.

> „Now I'm not talking about lack of accountability here, at all. We must be accountable to the people we communicate with. We must be accountable to the people we trade with. And the technology must be built to enforce that. But we must not be accountable to THE PUBLIC for who we talk to, or who we buy and sell from.“[85]

Mit der Pseudonymität soll die Verpflichtung auf accountability (Verantwortlichkeit, Haftbarkeit) des individuellen Handelns also nicht in Frage gestellt werden. Der Staat wird zwar rhetorisch fundamental in Frage gestellt, zugleich bleibt er jedoch unterbestimmt. Er kommt nur ins Blickfeld als der Apparat, die Gewalt, die äußerlich steht zu den privaten Beziehungen der Bürger. Diese Vorstellung drückt sich auch sprachlich aus, wenn selten vom Staat und seiner Gewalt, und fast immer stattdessen von der Regierung die Rede ist.[86] Dass die Form dieser Beziehungen nicht spontan variieren kann, sondern wesentlich überindividuell vorgegeben ist, und dass diese Form zugleich Folge und Voraussetzung ökonomischen Zwangs in diesen Beziehungen ist, wird nicht problematisiert. Stattdessen wird die Verfassung der USA zur Berufungsinstanz gegen die konkret ausgeübte Staatsgewalt. Und der Markt ist nicht nur kein Problem, sondern im Gegenteil der Wind im Rücken der eigenen Bewegung:

---

84 Eine kompakte Beschreibung dieser Anschauung anhand des Cypherpunk-Vordenkers Hughes liefert Levy: Crypto. beat, S. 206 f.

85 John Gilmore: Privacy, Technology, and the Open Society. 1991 ⟨URL: `http://www.cpsr.org/conferences/cfp91/gilmore.html`⟩ – Zugriff am 1.5.2003.

86 Dieser Wortwahl wird hier bei der Wiedergabe der Vorstellungen von Zimmermann, den Cypherpunks und der von ihnen inspirierten öffentlichen Meinung stets gefolgt, auch bei Benutzung indirekter Rede.

> „Combined with emerging information markets, crypto anarchy will create a liquid market for any and all material which can be put into words and pictures. And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.“[87]

Dieses Zitat aus einer vielzitierten Schrift der Cypherpunks verdeutlicht den zentralen Impuls der Bewegung: Die Vorstellung von der „crypto anarchy“ als dem ungehinderten Zugang aller zu geistigen Produkten – und insbesondere natürlich zu starken Kryptographieanwendungen wie PGP, die nicht zuletzt diesen ungehinderten Zugriff auf geistiges Eigentum verbürgen sollen. Damit erweist sich die Idee der „crypto anarchy“ als mehr als eine rhetorische Geste. Sie ist vielmehr eine Variante des originären Individual-Anarchismus. Im Eigentum, so diese Spielart des Anarchismus, bewähre sich die Freiheit des Einzelnen. Da sie das bedingungslos tun muss, kann und soll, wird die staatliche Gewalt nicht als notwendige Bedingung des Eigentums identifiziert, sondern, ganz im Gegenteil, als eine Instanz, die zu den Eigentumsverhältnissen der Einzelnen immer erst nachträglich und äußerlich hinzutritt. Der Staat gefährdet das Eigentum demnach eher, als dass er ihm dient, oder es gar setzt.
Die Utopie der unmittelbaren Beziehung unter Privateigentümern, inhaltlich bestimmt dadurch, dass keine Dritter, keine staatliche Gewalt dazwischentrete, ist auch der Tenor von Mays Definition von „crypto anarchy“ im *Cyphernomicon*, dem später nicht weiterverfolgten Versuch einer FAQ[88] der Cypherpunk-Bewegung:

> „Strong crypto is here. It is widely available. [...] What emerges from this is unclear, but I think it will be a form of anarcho-capitalist market

87 Anonymus, The Crypto Anarchist Manifesto, 1988; zit. n. Timothy C. May: The Crypto Anarchist Manifesto. 1992 ⟨URL: `http://www.activism.net/cypherpunk/crypto-anarchy.html`⟩ – Zugriff am 1.5.2003.

88 Frequently Asked Questions, Akronym für die im Internet verbreitete Zusammenstellung ‘häufig gestellter Fragen’.

> system I call 'crypto anarchy.' (Voluntary communications only, with no third parties butting in.)"[89]

Mays Frontier-Metapher beweist zum einen den US-Patriotismus der Cypherpunks.[90]

Zum anderen wird hier in einer Metapher ausgedrückt, dass man „den Stacheldraht" nicht nur zerschneiden möchte, sondern die Kryptographie selbst ein dem Stacheldraht ebenbürtiges Mittel sein soll, Ordnung zu stiften. Die Cypherpunks wollen mit ihr eine neue, andere Ordnung schaffen. Die spielerisch-militante Entgegensetzung zur Staatsgewalt, die dennoch nicht richtungslos ist, sondern sich mit – wenngleich selbstironischen – Insignien einer alternativen Macht ausstattet, ist auch ein Merkmal der „Heimlichen Bewunderer" Ordos, einer Anspielung auf die Cypherpunks in Stephensons Cryptonomicon.

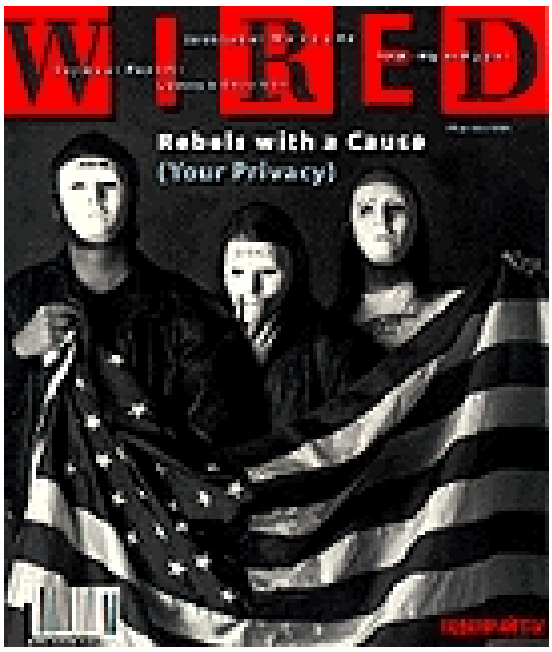

Abb. 3: *„Rebels with a cause (Your Privacy)"*

> „Mike oder Mark steigt aus seinem Auto und gibt dabei in einem langen scharzen Westernmantel eine dramatische Figur ab, ein Eindruck, der allerdings durch das T-Shirt, das er darunter anhat, eher verdorben wird: schwarz mit einem dicken roten Fragezeichen in der Mitte. Er hängt sich den Riemen seiner Schrotflinte über die Schulter, beugt sich in den Kofferraum und holt einen breitkrempigen schwarzen Cowboyhut heraus, den er aufs Autodach legt. Er wirft die Ellbogen hoch, steckt sein langes Haar hinter die Ohren, schaut zum Himmel und klemmt sich dann den Cowboyhut auf den Kopf. Lose um den Hals gebunden trägt er ein schwarzes Tuch mit einem Fragezeichenmuster,

89 Timothy C. May: The Cyphernomicon: Cypherpunks FAQ and More, Version 0.666. 1994 ⟨URL: `http://www.swiss.ai.mit.edu/6805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ`⟩ – Zugriff am 1.5.2003.

90 Die leider etwas undeutliche Abb. 3 sei hier kurz beschrieben. Sie zeigt das Titelblatt der zweiten Ausgabe des US-Magazins *Wired*, Sommer 1993. Unter dem Titelschriftzug sind drei Cypherpunks zu sehen. Sie halten den star-spangled banner und tragen Masken, auf denen PGP-Finger Prints stehen. Vgl. auch den Leitartikel zu diesem Titelblatt: Steven Levy: Crypto Rebels. Wired Mai/Juni 1993, Nr. 1.02 ⟨URL: `http://www.wired.com/wired/archive/1.02/crypto.rebels.html`⟩ – Zugriff am 1.5.2003.

> das er sich jetzt bis über den Nasenrücken hochzieht, sodass zwischen ihm und dem Cowboyhut nur noch ein Sehschlitz frei bleibt.“[91]

Der militante Gestus der Verweigerung gegen die Regierung und das Beharren darauf, einen eigenen, besseren Weg zu kennen, der vor allem das Individuum nicht gängelt – dies alles mag vordergründig im Widerspruch zum Patriotismus von May und dem Wired-Titelbild stehen. Die Einheit dieser beiden Seiten heisst jedoch Amerika. Auch ohne dass jeder US-Bürger deshalb bekennender Anarchist sein müßte, war das Verhältnis der Bürger zu ihrer Staatsgewalt hier doch stets ein anderes als in den alten europäischen Nationen. Die Hinfälligkeit der tradierten Hierarchien, denen mehrere Generationen nach Amerika Ausgewanderter den Rücken gekehrt hatten; von vornherein den Verhältnissen kapitalistischen Eigentums, aber auch der ebenso kapitalistischen persönlichen Freiheit ausgesetzt zu sein; der Protestantismus als nach Innen gekehrte Religiösität und nicht zuletzt vielleicht auch die Weite eines Siedlungsgebiets, die es zulässt, ‘für sich zu bleiben’ (Privacy!),[92] auf eigene Faust hinauszugehen und die Neuaneignung besitzlosen Landes zu riskieren: Dies alles waren historische Bedingungen, die zur Ausprägung einer sehr spezifischen Vaterlandsliebe geführt hatten. David DeLeon rekapituliert diese historischen Bedingungen und setzt sie ins Verhältnis zum individualistischen Anarchismus, der in den USA schon lange vor den Cypherpunks eine starke Anhängerschaft besaß.

> „Anarcho-libertarian impulses have also been generated by capitalism, which has broken down many traditional frameworks of authority in this culture, generally replacing them with self-interest. [...] The radicalism that grows out of this is most often individualist, but, when communal, it also has been remarkably preoccupied with issues of decentralization and fears of the tyranny of organization.“[93]

DeLeon geht so weit, zu behaupten, dass der ‘rechte Anarchist’, der am individuellen kapitalistischen Erfolgsstreben alles andere relativiert, der ultimative Amerikaner sei:

---

91 Stephenson, S. 887.

92 Vgl. Fußnote zu diesem Begriff in diesem Abschnitt.

93 David DeLeon: The American as Anarchist. Baltimore, 1978, S. 24.

> „A few who have trusted completely in the natural order of the marketplace have become explicit right anarchists. ‘Mind your own business’ became the literal basis for an American anarchism. [...] Such an anarchist is, in one sense, the ultimate American.“[94]

Zusammen mit Zimmermann haben die Cypherpunks den Staat identifiziert als den Angreifer auf die autonome Verfügung der Einzelnen über ihre Informationen; und ebenfalls mit Zimmermann wird der Kampf mit diesem Angreifer gefasst als eine kollektive Verteidigung des Rechts darauf, sich individuell mit technischen Mitteln gegen den staatlichen Übergriff des Überwachens zu verteidigen. Von den technischen Mitteln selbst ist bereits bei Diffie und Hellman die Rede, dort allerdings nur implizit von der konkreten Gestalt der Überwachung. Doch wie sollte mit den kryptographischen Innovationen neuer Richtung weiter umgegangen werden, nun, nachdem sie von Zimmermann und den Cypherpunks zur Waffe in einem doppelten Verteidungskampf gegen die staatliche Überwachungsmacht politisiert worden waren? Als entscheidend für das Funktionieren dieser neuen Waffe wird weiterhin die Entwicklung und Verbreitung von Computerprogrammen betrachtet. Diffie und Hellman waren implizit davon ausgegangen, dass mit dem Veröffentlichen eines Algorithums und Protokolls unmittelbar eine technische Revolutionierung der Individualkommunikation einherginge, die diese jeder Überwachung ‘durch Dritte’ entzöge. Die Cypherpunks wollten nun Anwendungen schaffen, mittels derer solche Algorithmen und Protokolle auf den (inzwischen ‘zu Hause’ angelangten) Computern individuell nutzbar wären. Das reflektiert auf die Erfahrung, dass solche Anwendungen, auch wenn mit dem PC eine notwendige technische Voraussetzung gegeben ist, keineswegs wie von selbst entstehen – auch nicht motiviert durch das bereits von Diffie und Hellman anvisierte Interesse an einem E-Commerce. Und auch eine weitere Hürde beim Gebrauch von Kryptographie als politischer Waffe wurde identifiziert, die den ersten Quasi-Cypherpunks der achtziger Jahre offenbar noch nicht geläufig gewesen war:[95] Selbst eingebettet in ein gebrauchsfertig öffentlich zur Verfügung gestelltes Computerprogramm kann die angestrebte Variante massenhafter Kryptographienutzung vom Staat durch Verbots- und Regulie-

94 DeLeon, S. 65.

95 Vgl. die oben zitierte Rede auf der Future of Freedom Conference.

rungsversuche bekämpft werden. Deshalb musste nun neben der Entwicklung auch die Verbreitung von Software kultiviert und politisiert werden. Natürlich bleibt Krypto-Euphorie der Impuls dieses Engagements, aber das Engagement ist variantenreicher und um einige Erfahrungen klüger geworden.

Die Krypto-Euphorie der bürgerrechtsbewegten Cypherpunks korrespondierte, wie gesagt, mit dem Bild der breiten bürgerlichen Öffentlichkeit vom sich entwickelnden Internet. Dabei war diese Korrespondenz keineswegs eine Einbahnstraße. Spätestens seit Schneiers *Applied Cryptography* würdigten Medien und Fachöffentlichkeiten die kritische Stellung der Cypherpunks zum Internet und seiner Regulierung als die ernstzunehmende Position einer technisch hochqualifizierten Avantgarde.

> „We know that software can't be destroyed and that a widely dispersed system can't be shut down."[96]

Die Öffnung des Internets für kommerzielle Dienste 1988 hatte wichtige Fakten geschaffen, die in der Tat für diese 'kritisch-euphorische' Avantgardeposition zu sprechen schienen. Die Prämissen, unter denen Internet- und Verschlüsselungstechnologien in den nach aussen geschlossenen Intranets staatlicher und kommerzieller Einrichtungen eingesetzt wurden, schienen seitdem unwiederbringlich auf einen verhältnismäßig kleinen, jedenfalls geschlossenen Geltungsbereich beschränkt, die absolute Definitionsmacht dieser Einrichtungen über die Technikanwendung schien plötzlich relativiert zu sein. Der neue, 'öffentliche' Raum der Techniknutzung schien weitgehend definiert durch das Belieben zahlloser individueller 'Endanwender'. Wie wenig unverrückbar unter den Prämissen moderner staatlicher Herrschaft solche Entwicklungen jedoch bis heute geblieben sind, zeigen neueste Gesetzesentwürfe in den USA. Sie können so interpretiert werden, dass der Einsatz von Techniken wie End-to-End-Verschlüsselung mit PGP nur unter Bedingungen erlaubt ist, die der 'zuständige' Serviceprovider setzt. Anonymisierende Techniken scheint das Gesetz gleich prinzipiell für illegal erklären zu wollen: „The bills include a ban on devices that 'conceal ... the existence or place of origin or destination of any communication.'"[97] Das Inkrafttreten eines solchen Gesetzes wäre die Grundlage

96 Eric Hughes: A Cypherpunk's Manifesto. 1993 ⟨URL: `http://www.activism.net/cypherpunk/manifesto.html`⟩ – Zugriff am 1.5.2003.

97 Mike Godwin: A Brief Analysis of the 'Super DMCA' (the Draft Model Communications Security Act). 2003 ⟨URL: `http://www.politechbot.com/docs/godwin.state.dmca.041603.pdf`⟩ – Zugriff am 1.5.2003, S. 3.

dafür, den Raum der 'öffentlichen' Internetnutzung radikal zu verändern – nicht als ein direktes Verbot der Nutzung einer Technik, sondern als massive, mit Strafandrohung versehene Delegitimierung der autonomen Nutzung von Verschlüsselungs- und Anonymisierungstechnik, die sich nicht gegen die Telekommunikationsdienste-Anbieter richtet, sondern ihnen im Gegenteil eine gestaltende, mitwirkende Rolle in der Repression einräumt. Dass auch die Anbieter der notwendigen öffentlichen Internetdienstleistungen lieber gläserne Kunden haben, scheint hier vom Gesetzgeber bereits reflektiert und als Gestaltungsmoment in den Repressionsvorbehalt mitaufgenommen worden zu sein.

Neben PGP und dem Web of Trust waren es vor allem die Konzepte David Chaums, an die sich die Hoffnung knüpfte, Ordnung ließe sich, zumindest 'im Cyberspace', gerechter und individualistischer herstellen. Exemplarisch für die Anknüpfung an Chaums Konzepte stehen die Remailer. Es handelt sich dabei um Internet-Server, die auf die anonymisierende Weiterleitung von E-Mails spezialisiert sind. Remailer empfangen E-Mails, entfernen alle Informationen aus dem E-Mail-Header, die Auskunft über die wahre Herkunft der E-Mail geben könnten (vor allem die eindeutige Internet-Protocol-Adresse des Ursprungsrechners), und senden sie dann an den endgültigen Empfänger der E-Mail weiter. 1993 gründete Julf Helsingius den Remailer „Penet".[98] Helsingius hatte bald alle Hände voll zu tun, diesen rasch sehr populären Remailer am Laufen zu halten. Zur Einstellung des öffentlichen Remailerbetriebs sah sich Helsingius jedoch erst genötigt, als ihn die Staatsanwaltschaft dazu zwang, Logdateien herauszugeben, mithilfe derer ein Benutzer des Servers identifiziert werden sollte. Das wiederum war gerichtlich erzwungen worden von Scientology, die ihren Ruf durch eine anonyme Internetpublikation verletzt gesehen hatten.

Doch solche Rückschläge hielten die Cypherpunk-Community nicht davon ab, weitere Remailer aufzubauen. Wenig später vereinbarte man ein einheitliches Protokoll zur Verwendung komplexerer Remailer, Mixmaster. Mixmaster-Remailer bilden untereinander ein Netzwerk Chaumscher Mixe.[99] Als potentielle Angreifer auf die Anonymität der E-Mails werden bei Mixmaster explizit staatliche Geheimdienste unterstellt – Mixmaster soll nicht weniger leisten als die Anonymität von E-Mails

98 Levy: Crypto. beat, S. 222, 291 ff.

99 Vgl. 3.3.

zu gewährleisten angesichts einer Überwachung, die den gesamten ein- und ausgehenden Nachrichtenverkehr der Remailer lesen kann. Klar war ohnehin, dass, ohne auf 'starke Verschlüsselung' mit PGP aufzusetzen, keine angemessene Anonymisierung zu erreichen wäre. Das hätte aber immer noch nicht das Problem gelöst, dass die gleiche PGP-verschlüsselte Nachricht im Nachrichten-Eingang und -Ausgang der Remailer beobachtet werden konnte. Das Mixmaster-Protokoll sieht daher eine Verschlüsselung der E-Mails in der Art einer russischen Puppe vor: Die Nachricht wird zunächst mit dem Public Key des endgültigen Adressaten verschlüsselt, und die so verschlüsselte Nachricht wird dann, einschließlich aller Header, nochmals verschlüsselt – diesmal an den Public Key des Remailers. Der Remailer wiederum entschlüsselt die eingegangene Nachricht automatisch und leitet sie dann weiter. Selbstverständlich lässt sich dieses Verfahren auch in Kette schalten. Bei der Verwendung mehrer Remailer, die möglicherweise in verschiedenen Ländern von verschiedenen Personen betrieben werden, lässt sich selbst die Möglichkeit, dass mancher Remailer direkt von einem Geheimdienst selbst betrieben wird, miteinkalkulieren. Zugleich jedoch entlastet das Mixmaster-Protokoll die ehrlichen Betreiber eines Remailers. Wäre Helsingius' Remailer Teil eines Mixmaster-Netzwerks gewesen (das es damals freilich noch nicht gegeben hatte), hätte weder ihn die Herausgabe der Logfiles an den Staatsanwalt angefochten, noch den betroffenen Scientology-Kritiker.

Die Erfinder des Mixmaster-Protokolls und die Betreiber der Mixmaster-Remailer rückten ihre Erfindungen nicht zu unrecht in die Tradition von PGP selbst. Was nützt schließlich PGP alleine als Waffe zur Verteidigung meiner Privacy, wenn ich unterstellen muss, dass die potentiellen Angreifer weiterhin ohne nennenswerten Aufwand feststellen können, mit wem ich kommuniziere, wann wie viel?

4.5 Clipper oder PGP – Welche wird die 'Encryption for the Masses'?

Wir befinden uns am Anfang der neunziger Jahre. Noch deutet sich der spätere E-Commmerce-Boom erst an. Die vorangegangenen Teile dieses Kapitels behandelten eine subversive Variante der massenhaften Verbreitung von Kryptographie-Anwendungen – subversiv sowohl was den bezweckten Bruch mit der zeitgenössischen Realität der Kryptographieanwendung anbelangt („crypto anarchy"), als

auch in der Wahl ihrer Mittel (Bruch gesetzlich geschützter Patente und Ausfuhrbestimmungen). Die Verbreitung der Kryptoanwendungen als solche war programmatischer Teil dieser Subversion, Zimmermann hatte PGP quasi den Untertitel „Public Key Encryption for the Masses“.[100] gegeben. Parallel wurde das Ziel der massenhaften Verbreitung eines Kryptosystems jedoch auch von der Gegenseite, dem FBI und der MOU-Gruppe von NSA und NIST, verfolgt. Diese ‘Neuaufstellung’, sowohl die plötzliche Hinwendung der für die innere Sicherheit zuständigen Behörden zum Thema Kryptographie als auch die konstruktive Wendung des Streits zwischen NSA und NIST nach dem Ende der Reagan-Ära hatten ihren gemeinsamen Nenner in einer gänzlich neuen Haltung zur Kryptographieanwendung. Unter den Präsidenten George Bush sr. und Clinton galt auf einmal das Wie des Kryptographieeinsatzes als fundamentale gestalterische Frage. Und die Antwort darauf war jener der Cypherpunks zwar entgegengesetzt, aber dennoch nicht ganz andersartig. Das Ziel war fortan nicht mehr Verhinderung um jeden Preis, sondern ebenfalls die massenhafte Durchsetzung einer Krypto-Anwendung – die wie PGP politisch bewusst gestaltet war, wenngleich mit ganz anderen Vorzeichen. Dieser Abschnitt soll erhellen, warum beide Projekte der ‘Encryption for the Masses’ scheiterten.

Mit dem Clipper Chip und dem Digital Signature Standard (DSS) sollte bewiesen werden, dass die Förderung des kommerziellen Kryptographie-Einsatzes und die staatliche Sicherheit nach innen und außen einander nicht ausschließen müssen.[101] Die gemeinsame Arbeitsgruppe von NSA und NIST legte einen Entwurf für ein neues kryptographisches Protokoll, den Escrowed Encryption Standard (EES), vor. Kernstück war der von der NSA entwickelte symmetrische Verschlüsselungsalgorithmus Skipjack. Dieser sollte fortan in alle US-amerikanischen Telefone und Computer eingebaut werden müssen; der Chip im Computer sollte Capstone, der im Telefon Clipper heissen. Unter dem Schlagwort Clipper wurde dieses Vorhaben für die Cypherpunks und die Internet-Bürgerrechtslobby, die sich in den Jahren zuvor etabliert hatten, die letzte, aber auch am schärfsten zugespitzte staatliche Provokation. Mit Clipper war auch der obligatorische Gebrauch starker asymmetri-

100 Zimmermann.

101 Eine kompakte Darstellung des Clipper-Plans findet sich bei Wobst, S. 253 ff.; wie immer ausführlich hingegen Levy: Crypto. beat, S. 226 f.

scher Verschlüssselung und Signatur am Telefon und im Datenaustausch zwischen PCs beabsichtigt – ein Aspekt, den die Bürgerrechtler als reinen Vorwand für die eigentlichen Absichten der NSA von der Hand wiesen. Wahr ist an dieser Kritik, dass die mit Clipper verfolgte Hauptabsicht offensichtlich woanders lag. Denn in jedem Chip sollte ein zusätzlicher öffentlicher Schlüssel hinterlegt sein, mit dem es auf staatsanwaltliche Weisung hin jederzeit möglich sein sollte, den gesamten verschlüsselten Datenverkehr abzuhören. Anders als durch den obligatorischen Einbau kryptographischer Chips in sämtliche national verfügbare Hardware, so das Kalkül, wäre eine zentrale Hinterlegung aller verwendeten kryptographischen Schlüssel nicht durchsetzbar; anders als durch eine solche zentrale Hinterlegung jedoch, so die Befürchtung, würde der Datenverkehr endgültig der Überwachung durch die geheimdienstlichen und strafverfolgenden Behörden entzogen.

Matt Blaze wird für die Cypherpunk-orientierte Fachöffentlichkeit zum Hauptzeugen der Anklage gegen Clipper, als ihm der Nachweis gelingt, dass sowohl der Skipjack-Algorithmus selbst als auch seine geplante Implementation kryptographisch unzulänglich sind. Die Diskussion scheint verschoben wie in Diffies und Hellmans *New Directions*.[102] Die fachliche Kritik an den Mitteln des Abhörplans ersetzt die Kritik des politischen Zwecks, oder soll dieser Kritik zumindest Legitimität verschaffen. Dabei hätte sich aus Blazes Analyse ebenso gut die Konsequenz ziehen lassen, dass man den Abhörplan dann eben noch technisch perfektionieren muss. Anzumerken ist natürlich dennoch, dass das Urteil des kryptologischen Einzelkämpfers Blaze die Kryptographieanwendung Clipper schlecht aussehen lässt, gerade in Anbetracht der Tatsache, dass hinter dem Skipjack-Algorithmus und seiner Implementation vermutlich die NSA gestanden hat. Das ist kennzeichnend für den Gesamteindruck, den die Planung des Escrowed Encryption Standards nachträglich macht.

So sollten zunächst staatliche Stellen die Schlüssel haben; 1996 gab es den neuen Plan, Schlüssel privat hinterlegen zu lassen; und danach gab es dann gar keine Spezifikation mehr, bei wem die Schlüssel hinterlegt werden sollten.

> „The Administration's original key escrow proposals required that government agencies hold the key copies. More recent proposals suggest

102 Diffie und Hellman.

> that keys could be held by private industry. The latest proposal leaves identity of the key holder unspecified.“[103]

Blaze räumte im selben Text ein, dass ‘Key Recovery’ im kommerziellen Bereich eine berechtigte Funktion haben könne, beim staatliche Einsatz hingegen ein unabsehbarer Qualitätsverlust der jeweiligen Kryptosysteme zu befürchten sei. Blaze argumentiert, wie er es selbst formuliert, mit ‘dem direkten Interesse’ der Industrie am Einsatz guter und billiger Kryptographie:

> „It is in the direct interest of any industry that hopes to benefit from electronic commerce to encourage wide availably of high-quality, inexpensive cryptographic products that enable secure communications and commerce.“[104]

Der Druck des herannahenden Geschäfts mit dem Internet, das die Nagelprobe auf jedes massenhaft implementierte Kryptosystem wäre, schlägt sich nieder im Bild der Widersprüchlichkeit und Konzeptionslosigkeit der US-Kryptopolitik dieser Jahre.

> „Key recovery has been given so many names (key escrow, law enforcement access, key recovery, data recovery, trusted third parties, etc etc) that it’s now known by the general term GAK (Government Access to Keys)“[105]

Es wäre jedoch verkürzt, einen völligen Bruch zwischen der Clipper-Episode und der Kryptopolitik während des E-Commerce-Booms der späten neunziger Jahre zu postulieren. Vielmehr begann mit dem Clipper-Plan erst die bis heute anhaltende Kontinuität einer aktiven, eingreifenden Kryptopolitik. Der Anspruch auf die Diskretion von Kommunikationsdaten sowohl gegenüber dem Ausland als auch gegenüber der inländischen Geschäftskonkurrenz wird mit und nach Clipper aufgenommen und bestätigt, und zugleich wird jeder absolute Anspruch auf die Privatheit der Kommunikation, die sich dann konsequenterweise auch gegen die ‘eigene’,

---

103 Matt Blaze: Cryptography Policy and the Information Economy. 1996 ⟨URL: `http://secinf.net/uplarticle/4/policy.txt`⟩ – Zugriff am 1.5.2003.

104 A. a. O.

105 Peter Gutmann: Encryption and Security Tutorial, Part 1. Auckland, 2001 ⟨URL: `http://www.cryptoapps.com/~peter/part1.pdf`⟩ – Zugriff am 3.4.2003.

zuständige Staatsgewalt richten würde, verneint. Die Staatsgewalt wird damit zur Verwalterin des privaten Anspruchs auf Diskretion in einer Doppelrolle. Sie anerkennt und gewährt diesen Anspruch, und macht sich zugleich zu seiner absoluten Grenze und Bedingung.

Das Interesse daran, 'jeden Dritten' von der privaten Individualkommunikation auszuschließen, schien sich bei Diffie und Hellman problemlos gleichsetzen zu lassen mit dem Geschäftsinteresse an einem künftigen E-Commerce. Dem direkt entgegengesetzt, in einer bestenfalls obsoleten, jedenfalls rein repressiven Rolle erscheint der staatliche Monopolanspruch auf die Kryptographienutzung. Auf die Relation der Unternehmer zu Kunden und Angestellten einerseits, sowie auf die Relation zwischen Staat und Bürgern andererseits wirft die neuartige Haltung der Staatsgewalt zur Verschlüsselungstechnik ein neues Licht. Die impliziten Prämissen, die sich in Diffies und Hellmans Aufsatz *New Directions*[106] von 1976 ausdrückten, erscheinen zwei Jahrzehnte später als überaus problematisch. Die praktisch durchgeführte Trennung zwischen einerseits dem – offiziell anerkannten – Interesse nach Diskretion gegenüber dem Ausland und der Konkurrenz im Inland und andererseits dem – nur bedingt und begrenzt anerkannten – Interesse an Privacy gegenüber jedem Dritten, also auch dem Staat, widerlegt Diffies und Hellmans stillschweigende Annahme. Außerdem war nun jeder Zweifel daran widerlegt worden, dass der Staat jenseits bloßer Verbote überhaupt eine Rolle spielen könnte in der Welt der Kryptographie neuer Richtung, die doch ausschließlich eine Sache sein sollte, die sich zwischen den jeweiligen Kommunikationspartnern abspielt.

Dass die PKC nicht in Gestalt des Clipper-Chips die Massen erreicht hat, galt spätestens 1998 allgemein als erwiesen. Dass sie es, bis auf den heutigen Tag, auch in Gestalt ihres 'de-facto-Standards' PGP nicht geschafft hat, ist weniger bekannt und soll hier mit einer kleinen empirischen Untersuchung gezeigt werden.

Laut eines Werbematerials des damaligen PGP-Herstellers Network Associates Inc. (NAI) von 2001 gab es zu diesem Zeitpunkt „over 7 million people worldwide“,[107] die PGP benutzten. NAI gibt keine Quelle für diese Zahl an; dennoch sei sie der nachfolgenden Überlegung der Einfachheit halber zugrunde gelegt. Die wohl am

106 Diffie und Hellman.

107 Inc. Network Associates: PGP Corporate Desktop Privacy Products. 2001 ⟨URL: `http://www.omicron.ch/new/produkte/DataSheets/PGPsecurity/pgp-corporatedesktop.pdf`⟩ – Zugriff am 1.5.2003.

häufigsten zitierte Quelle zur Schätzung der Internet-Benutzerzahlen weltweit, das US-Marktforschungsunternehmen Nielsen//NetRatings, gab für den April 2001 ca. 205 Millionen aktive[108] Internetbenutzer an.[109] Zugrunde liegt dieser Zahl eine Untersuchung repräsentativer Stichproben mit Internet-Benutzern aus 21 Industriestaaten. Nielsen//NetRatings gibt an, mit Untersuchungen in normalerweise 23 Ländern mehr als 84 Prozent der Internetbenutzer auf der ganzen Welt erfassen zu können. Wenn man unterstellt, dass bis auf eine verschwindend geringe Anzahl die PGP-Nutzer eine Teilgruppe der aktiven Internetnutzer in diesen Industriestaaten sind, ergibt sich mit den NAI-Zahlen im Jahre 2001 ein Verbreitungsgrad von PGP unter diesen Internet-Nutzern von „mehr als“ 3 Prozent. Es ist jedoch anzunehmen, dass von diesen sieben Millionen nur ein Bruchteil einigermaßen konsequent PGP einsetzen wird. Ein Merkmal, das sich hierzu statistisch erheben ließe, wäre, ob ein gültiger Public Key einschließlich mindestens eines fremden Zertifikats auf einem öffentlichen Server zur Verfügung gestellt wird.[110] Ein Public-Key-Server, der regelmäßig statistisches Material veröffentlicht, ist M. Drew Streibs www.dtype.org. Nach den frühesten Angaben Streibs, aus dem Juni 2001, gab es zum damaligen Zeitpunkt ca. 152 Tausend veröffentlichte Schlüssel, die den oben genannten Anforderungen genügen.[111] Diese Zahl ergäbe einen Anteil von ca. 0,07 Prozent ernsthaft PGP einsetzenden Nutzern unter den insgesamt 205 Millionen aktiven Internet-Nutzern von April 2001 nach Nielsen//NetRatings. Man muss also von einem immer noch sehr geringen Verbreitungsgrad einer solchen PGP-Verwendungsweise sprechen. Dabei ist für den E-Mail-Verkehr mit PGP immerhin eine populäre Verschlüsselungsanwendung zugänglich – anders als beim Telefonieren, worauf an anderer Stelle näher einzugehen sein wird. Der Einsatz von PGP in Unternehmen

---

108 Mindestens eine Nutzung des Internets pro Monat. Bei einer selteneren Nutzung kann man kaum von einem aktiven Gebrauch des Mediums E-Mail ausgehen.

109 Nielsen//NetRatings: Nielsen//NetRatings finds Strong Global Internet Growth in Monthly Internet Sessions and Time spent Online between April 2001 and April 2002. 2002 ⟨URL: `http://www.nielsen-netratings.com/pr/pr_020610_global.pdf`⟩ – Zugriff am 1.5.2003.

110 Auch dies kann nicht mehr als ein grobes Indiz sein. Es ist davon auszugehen, dass gültige, fremdzertifizierte Schlüssel ungenutzt auf dem Server liegengelassen werden, manche Personen gleichzeitig mehrere Schlüssel veröffentlicht haben etc. – was die Zahl jeweils künstlich erhöhen würde.

111 M. Drew Streib: Key Analysis begun 12 Jun 2001. 2001 ⟨URL: `http://dtype.org/keyanalyze/200106.php`⟩ – Zugriff am 1.5.2003.

und Behörden muss in immerhin so nennenswerter Größenordnung stattfinden, dass NAI und nun die PGP Corp. darauf kalkuliert haben, mit der Vermarktung von PGP allein in diesem Bereich Gewinne erzielen zu können, denn für den privaten und nichtkommerziellen Gebrauch boten sie stets eine kostenlose PGP-Version an. Das ist immerhin ein Indikator dafür, dass PGP über das Informatik-Millieu hinausgewachsen sein muss, aber dennoch muss resümiert werden, dass sich starke Verschlüsselung im Bereich der individuellen digitalen Kommunikation per E-Mail bis heute kaum durchgesetzt hat. Zehn Jahre nach Veröffentlichung der einschlägigen Kryptographie-Anwendung PGP hat diese lediglich einen Verbreitungsgrad im Promille-Bereich zu verzeichnen.

5 1994-1999: Starke Kryptographie für starke Standorte

5.1 E-Commerce-Boom, Ideologie und Politik

Seit 1994 hat die Integration von Krypto-Software in kommerzielle Produkte eine regelrechte Explosion erlebt. Die erste Illustration, mit der man als Internet-Surfer heute nahezu zwangsläufig mit den kryptographischen Innovationen neuer Richtung vertraut gemacht wird, ist das kleine Schloß- oder Schlüsselsymbol unten im Browser-Rahmen beim Aufbau einer Verbindung zu einem Onlineshop oder dergleichen. Das Symbol erscheint, wenn eine Verbindung nach dem Secure-Socket-Layer-Protokoll (SSL) aufgebaut wird, bei der unter anderem der RSA-Algorithmus zum Einsatz kommt. Die Firma RSA Data Security, Inc. hatte ad hoc eine Reihe solcher kryptographischer Prokolle entwickelt, die es erlauben, per RSA-Algorithmus die Authentizität von Internetservern abzusichern, mit denen man kommuniziert, sowie alle kommunizierten Daten zu verschlüsseln. Das Stammzertifikat soll dem Kunden eines Online-Shops die Arbeit abnehmen, sich vor dem Aufbau einer verschlüsselten Verbindung selbst von der Echtheit des Onlineshop-Schlüssels zu überzeugen. Dass ihm das Stammzertifikat auf einer bedruckten CD überreicht wird, oder gar beim Kauf eines neuen PCs zusammen mit dem Betriebssystem vorinstalliert auf der Festplatte liegt, soll ein hinreichend starkes Indiz für die Echtheit des Stammzertifikats sein – und mit diesem lassen sich dann beliebig viele wei-

tere Schlüssel zertifizieren. Es müssen keine eigenen Schlüsselpaare erzeugt und somit auch nicht der geheime Teil eines solchen Paars geschützt werden, und es müssen und können keine eigenen oder fremden Schlüssel zertifiziert werden. Freilich wäre es unsachgemäß, die Weglassung dieser technischen Komponenten als ein Defizit SSL-verschlüsselter Netzverbindungen und mitgelieferter Stammzertifikate zu beurteilen. Denn SSL tritt von vornherein nicht mit den Zwecken an, die mit der Zertifikation in eigener Regie nach der Art von PGP verfolgt werden. Das von den Software- und Dienstebetreibern kalkulierte Risiko des Abhörens von Verbindungen soll lediglich um eine Sicherheitskomponente erweitert und damit relativ erschwert werden. Wie bei allen Kryptographieanwendungen im Zeitraum bis 1999 wurden die Extrakosten, zwei oder noch mehr Versionen jedes Programms zu verbreiten, eine mit starker Verschlüsselung, eine mit für den Export zulässiger Verschlüsselung, von den US-amerikanischen Softwareherstellern billigend in Kauf genommen. Diese zeitweilige Inkaufnahme schwacher Verschlüsselung verdeutlicht zugleich, dass Sicherheit im Sinne eines technisch ausgereiften Schutzes der privaten Individualkommunikation vor staatlichem Abhören hier von vornherein nicht das wesentliche Ziel war.

Da nun das Wort vom kommenden E-Commerce-Boom umging, glaubten es sich weder Netscape noch Microsoft (damals die beiden großen Hersteller von Internet-Browsern) leisten zu können, auf die Lizenz zum Einsatz dieser Protokolle zu verzichten. Durch die mit der vorinstallierten Software gebündelten Stammzertifikate ist auch festgelegt, wer das Geschäft mit der Zertifizierung der Softwarehersteller und Internet-Dienstleister machen kann. Als Lizenzgeber ist weiterhin RSA Data Security, Inc. beteiligt, deren Boom an einer ungeheuren Expansion im Bereich der Internet-Dienstleistungen abzulesen ist. Mit Verisign geht 1995 aus RSA Data Security, Inc. ein Offspin hervor, der seit den Jahren des Internet-Booms sowohl Marktführer im Bereich der RSA-Zertifizierung als auch bei der Registrierung von Internet-Domänennamen ist.[112] Aus einem Kleinunternehmen, das jahrelang gegen eine Serie von ökonomischen, technischen und kryptopolitischen Hindernissen kämpfen musste, um seine Ware anbieten zu können, war ein Monopolist in zwei strategisch wichtigen Segmenten der boomenden Branche dieses Jahrzehnts geworden.

Der Einbau kryptographischer Algorithmen, Protokolle und Stammzertifikate in Software seit 1994 war jedoch keine bloße Luftnummer zugunsten des Aktien-

112 Schmeh, S. 492.

kurses der beteiligten Unternehmen. Es handelte sich um den ersten Schritt im Aufbau einer kryptographischen Infrastruktur, die in absehbarer Zeit vollwertig rechtskräftige Handlungen per digitaler Datenübertragung ermöglichen sollte.[113] Seit ungefähr 1996 machte das Schlagwort die Runde, Kryptographie sei – neben anderen Neuen Technologien – ein *Fundament der Informationsgesellschaft*.[114] Sobald die ökonomische Potenz des neuen Massenkommunikationsmittels Internet offensichtlich geworden war, schritt die Rehabilitierung der Kryptographie neuer Richtung, die seit ihrer Erfindung als Element eines solchen Massenkommunikationsmittels konzipiert war, rasch voran. Die offizielle Beförderung der asymmetrischen Verschlüsselung vom Störenfried zum Standortfaktor stand nun auf der Tagesordnung. Die politische Unterstützung für die Schaffung einer kryptographietechnischen Grundlage für den E-Commerce war weitaus mehr als der weitgehende Rückzug von der Repression gegen die angewandte Kryptographie. Die Entstehung einer Norm für eine rechtlich verbindliche digitale Signatur muss von der Recht setzenden Macht Staat nicht nur geduldet werden – letztlich muss der Staat sie selbst aktiv setzen.

Wenn nämlich Geld und Ware, ob diese nun die Gestalt von Daten haben oder nicht, ihren Eigentümer wechseln, muss diese Transaktion rechtssicher und verbindlich gemacht werden. Je voraussetzungsloser, billiger, schneller jede solche Transaktion mit jedem beliebigen Einzelnen vonstatten gehen kann, desto besser für das jeweilige Geschäft. Der E-Commerce, letztlich aber auch der Einsatz kryptographischer Technologie im E-Commerce, ist ein Hebel dieser Verbilligung. Das abstrakte Gesamtinteresse am Zurverfügungstehen solcher Technologie, möglichst schon in anwendungsreifer Gestalt, kann letztlich nur gesondert von den einzelnen Privatpersonen und Unternehmen wahrgenommen werden, also von der Staatsgewalt. Das staatliche Engagement ergibt sich zum einen unmittelbar aus der Notwendigkeit zur Veränderung rechtlicher Normen im Zusammenhang mit dem E-Commerce – qua definitione ein staatliche Aufgabe. Zum anderen rechtfertigt die zu erwartende Verbilligung durch Technologien, die mit zunächst ungewissem Resultat entwickelt sein wollen, nur bedingt den erforderlichen Aufwand. So hat also zwar niemand die Entwicklung der Kryptographie zu einem Hebel des E-Commerce von Anfang an geplant, aber rückblickend ist es dennoch nicht zufällig, dass ausgerechnet staatliche Förderung von Lehrstühlen und Stipendien notwendige materielle Ausgangsbedingungen der kryptographischen Innovationen Neuer

113 Vgl. 6.3.

114 Exemplarisch dafür der Titel einer umfangreichen gemäßigt-liberalen Studie über Kryptographie, Ökonomie und Politik in den USA: Kenneth W. Dam und Herbert S. Lin (Hrsg.): Cryptography's Role in Securing the Information Society. Washington, D.C., 1996 ⟨URL: `http://www.nap.edu/books/0309054753/html/`⟩ – Zugriff am 1.5.2003.

Richtung in den siebziger Jahren waren. Das Neue an der politischen Würdigung des E-Commerce und der Kryptographie als seines Mittels Mitte der neunziger Jahre ist, dass in ihr die Reflexion auf die notwendige fördernde und bedingende Rolle des Staates explizit und programmatisch wird.

Die Regeln von Eigentum und Person, einmal gründlich durchgesetzt, verstetigen die Konkurrenz, das schlechte Abschneiden vieler in dieser Konkurrenz, und letztlich auch die Kalkulation vieler auf besseres Abschneiden in der Konkurrenz, notfalls auch durch das Brechen der Regeln. Die Verwaltung von Warenverkehr unter den Verhältnissen des kapitalistischen Eigentums umschließt daher auch immer die Verwaltung seines Misslingens; die digitale Signatur zum Beispiel ist Mittel zum Abschließen legaler Verträge und zugleich, untrennbar von dieser positiven Funktion, auch Mittel der 'technischen Kriminalprävention'[115], negative Vorwegnahme des Betrugs also, der stets zu erwarten ist, solange das legale Vertragswesen besteht.[116] Die kryptopolitische Würdigung des privaten Geschäfts mit dem E-Commerce stand insofern stets nur bedingt im Widerspruch zum staatlichen Aufsichtsinteresse. Die Fassung der 'digitalen Signatur' als 'Technischer Kriminalprävention' und das explizite Lob der 'Unwiderrufbarkeit' als Qualität dieser Signaturen lassen bereits erahnen, dass es sich hier um eine Kryptographieanwendung handelt, in der beide genannten staatlichen Interessen mit ein und demselben Mit-

Abb. 4: *1994 – Das Internet als Neue Welt, bestimmungslos und daher vielversprechend und bedrohlich zugleich.*

115 Ein aktuelles Beispiel für die Subsumtion kryptographischer Verfahren unter die technische Kriminalprävention ist Ansgar Heuser: Prävention durch Informationssicherheit. Internetdokumentation Deutscher Präventionstag 2003 ⟨URL: `http://www.praeventionstag.de/content/5_praev/doku/heuser/praevention1.pdf`⟩ – Zugriff am 1.5.2003.

116 Vgl. zu den weiteren Implikationen der Einführung einer digitalen Signatur 6.3.

tel verfolgt werden können: Einerseits die aktive Förderung der marktwirtschaftlichen Interaktion der Bürger mit allen passenden kryptographischen Mitteln und andererseits ihre Beaufsichtigung zur Bekämpfung von Regelbrüchen aller Art.
Aber die staatlichen Anforderungen der USA und der EU-Staaten an Anwendungen wie die digitale Signatur gehen jeweils auch über ihre eigenen Landesgrenzen hinaus. Das Internet eignet sich auch zur weltweiten Senkung von Zirkulationskosten. Die dazu erforderliche Soft- und Hardware stellt eine eigenständige Gewinnquelle dar; unter dem Gesichtspunkt der Standortpolitik müssen aber vor allem möglichst früh die Bedingungen geschaffen werden, unter denen die inländische Industrie mit den neuen technischen Mitteln ihre Zirkulationskosten senkt. Der Abschnitt zur Kryptographie als Standortfaktor[117] behandelt exemplarisch die Strategie der hiesigen Kryptopolitik als einer Waffe, wohlgemerkt einer Waffe zum Ausfechten der internationalen Standortkonkurrenz.
Ferner übertragen Staaten das Modell der Zirkulationskostensenkung auf ihre eigenen Verwaltungsstrukturen, insbesondere auf den Informationsaustausch zwischen Staat und Bürger. Der Reibungsverlust an dieser Stelle wird durch eine nicht mehr nur papierförmige, sondern digitale Repräsentation aller Daten, die zur Verwaltung der eigenen Bevölkerung verwendet werden, minimiert. Maßnahmen wie die Einführung digitaler Personalausweise, Steuererklärungen und Grundbücher, das sogenannte E-Government, versprechen die erhöhte Mobilität und Einsetzbarkeit aller ohnehin erhobenen Daten, nebst einer Kostensenkung in der Verwaltung. Selbstverständlich ist das alles nur durch den massiven Einsatz starker asymmetrischer und symmetrischer Kryptographie angemessen sicher realisierbar.

5.2 The Open Code And Its Enemies: PGP nach 1996

1996 wurden die Verfahren gegen den PGP-Erfinder Zimmermann eingestellt; mittlerweile war auch ein Arrangement mit RSA Data Security, Inc. über eine bedingt lizenzfreie Verwendung des RSA-Algorithmus gefunden worden.[118] PGP war längst zum Symbol geworden; wenn es einen hauptsächlichen Kristallisationspunkt der öffentlichen Debatte um Kryptopolitik gab, dann war es das Schicksal der Anwen-

117 Vgl. 5.3.

118 Inc. RSA Data Security: RSAREF License. Redwood, 5. Januar 1993 ⟨URL: `http://bs.mit.edu/pgp/rsalicen.html`⟩ – Zugriff am 1.5.2003.

dung PGP und ihres Erfinders Zimmermann. So mangelte es nicht an Versuchen, PGP als Marke zu etablieren, nachdem der Patentrechtsstreit mit RSA Data Security, Inc. halbwegs beigelegt worden war. Dabei war die Vermarktung von PGP bis heute immer nur teilweise erfolgreich. Das ambivalente Schicksal der kommerziellen Verwertung der Marke PGP ist zugleich die Geschichte des Übergangs von einem inkriminierten, originär bürgerrechtlich- und cypherpunk-inspirierten Stücks Software hin zu einem Werkzeug des E-Commerce und Spielball der Standortkonkurrenz um die nationale Subsumtion der PKC.[119]

Der – sowohl historisch als auch der Sache nach – erste Grund für den komerziell überraschend geringen Erfolg von PGP war die Tatsache, dass PGP als ein Produkt auf die Schiene gesetzt wurde, mit dem in dieser Hinsicht überhaupt kein Erfolg erzielt werden sollte. Technisch schlug sich die Geringschätzung dieses Ziels vor allem darin nieder, dass von Anfang an die Offenlegung des Quellcodes zum symbolischen Kapital des Programms gehört. PGP lag immer als Binärdatei vor, so das das Programm ohne komplizierte Vorbereitung direkt einsetzbar war. Zusätzlich jedoch lag es auch als Quellcode in der Programmiersprache C vor und war somit für jedermann frei verwend- und veränderbar. Die Wahl von C hatte ihre besondere Bedeutung darin, dass ausgehend vom einmal veröffentlichten Quellcode, eine Portierung zu verschiedenen Computersystemen hin möglich ist. Je nachdem, wie der Programmcode compiliert worden ist, läuft dieselbe Software zum Beispiel sowohl auf einem Windows- als auch auf einem Unix- oder Linux-Rechner. Auch darin unterschied sich PGP grundsätzlich vom geschlossenen geschlossenen Programmcode des E-Mail-Verschlüsselungsprogramms MailSafe der Firma RSA Data Security, Inc.

Die Quelloffenheit diente der selbstständigen Weiterverbreitung von PGP durch seine Benutzer und war insofern Teil des politischen Programms der Weiterverbreitung dieser Software. Zum Teil was das Interesse an einer hohen 'Teilbarkeit' von PGP aber auch der Eile geschuldet, mit der das Programm verbreitet worden war. Zimmermann und seine Kollegen hatten allen Grund für die Eile und für die geradezu konspirative Verbreitung des Codes über die Bulletin Board Systems. Schließlich sah sich Zimmermann schon bald mit Vorwürfen konfrontiert, sich mit

119 Zur Versionsgeschichte von PGP vgl. Kai Raven: Deutsche Anleitung zu GnuPG & PGP. ⟨URL: `http://kai.iks-jena.de/pgp/`⟩ – Zugriff am 1.5.2003.

der Veröffentlichung einer ganzen Reihe zivil- und strafrechtlicher Vergehen schuldig gemacht zu haben,[120] und bevor die Verbreitung noch ernstlich hätte behindert werden können wollten Zimmermann und die Cypherpunks Fakten geschaffen haben.
Aber die Offenlegung des Quellcodes hat noch weitere Implikationen.

> „[...] I'm pretty sure that PGP does not contain any glaring weaknesses (although it may contain bugs). The crypto algorithms [...] have been individually subject to extensive peer review. Source code is available to facilitate peer review of PGP and to help dispel the fears of some users.“[121]

Der 'Peer Review' des offengelegten Programmcodes spricht die Programmbenutzer als diejenigen an, die sich selbstständig mit der Sicherheit der kryptographischen Algorithmen und ihrer Einbettung in die PC-Anwendung PGP auseinander setzen sollen. Bei aller strukturellen Ähnlichkeit zu den RFCs der Internet-Community geht dieses Konzept in einer Hinsicht noch weiter. Die RFCs diskutieren lediglich Standards, die der Interoperabilität von Anwendungen dienen sollen, erklären jedoch die Einbettung dieser Standards in die Anwendungen und Geräte selbst zur Angelegenheit der jeweiligen Programmierer. Darüber hinaus entspricht die Quelloffenheit kryptographischer Programme auch der Maxime Kerckhoffs', den Kryptographiegebrauch so zu gestalten, dass möglichst wenige Elemente und Prozesse geheim gehalten zu werden brauchen. Diffie und Hellman hatten sogar die Public-Key-Cryptography als ganze explizit in die Tradition dieses Gebots gestellt.[122]
Das rationale Moment der nachrücklichen Quelloffenheit von PGP ist der tatsächliche Nutzen des Peer Reviews einer offenen Scientific Community für die Sicherheit und die kontinuierliche Fortentwicklung des Programms. Zugleich war die Offenlegung des PGP-Quellcodes aber nie zu trennen von beliebten verschwörungstheoretischen Hypothesen, denen zufolge die Vermarkter von PGP nicht vielleicht doch auf Druck der Regierung eine 'Hintertür' zur Entschlüsselung PGP-verschlüsselter Nachrichten eingebaut haben könnten.

---

120 Vgl. 4.3.

121 Zimmermann.

122 Vgl. 2.4.

Diese Verschwörungstheorie machte sich bald vom Kriterium der Offenheit des Quellcodes unabhängig. Als PGP die asymmetrische Verschlüsselung mit RSA aufgab, schien der Ersatz, Schlüsselaustausch mit DH (der Algorithmus von Diffie und Hellman) und digitale Signaturen nach dem DSS (Digital Signature Standard), die neuen PGP-Versionen zum klassischen PGP 2.x absichtlich inkompatibel zu machen. Welcher Schritt wäre besser geeignet gewesen, die Anwender von PGP zum Umstieg von den alten, quelloffenen und daher nicht-kompromittierten Versionen auf neue, teilweise nicht mehr quelloffene und somit höchst verdächtige Versionen zu nötigen?
Doch alle einschlägigen Verdächtigungen kulminierten schließlich, als es 1998 zur Einführung des ADK (Additional Decryption Key) kam. Dabei handelte es sich zwar um ein Ereignis, dass überaus geeignet war, ohnehin schon vorhandene Verschwörungstheorien zu bestätigen. Tatsächlich handelte es sich um eine rationale Umgestaltung von PGP zugunsten einer neuen Anwendung des Programms, die auf spezifische Bedürfnisse von Behörden und Privatunternehmen einging.
Beim ADK handelt es sich um ein System zur zentralen Hinterlegung privater Zweitschlüssel. Allgemein gesprochen dient diese Anwendung dazu, den Kreis derer, die eine Nachricht entschlüsseln oder eine Unterschrift leisten können, zu vergrößern. Im Normalfall soll diese 'Schlüsselmacht' an eine bestimmte Person gebunden bleiben – aber eine Kontrolle des Nachrichtenverkehrs der jeweiligen Person soll während der Kommunikation oder hinterher möglich sein. Darin liegt kein Skandal, sondern eine Anpassung der Verschlüsselungsanwendung an das Verhältnis eines gewöhnlichen Arbeitgebers zu den vertraulichen Informationen, mit denen er seine Angestellten umgehen lässt. Den Angestellten selbst überlässt er diesen Zugriff lediglich in der Rolle auswechselbarer Funktionsträger; ihr Zugriff auf die Information muss dementsprechend stets rekapitulierbar und revidierbar bleiben. Die Kritiker des ADK-Protokolls wiesen darauf hin, dass der ADK im kleinen Maßstab das Konzept des GAK (Government Access to Keys) umsetzt, wie es in den Clipper-Plänen vorgesehen war. Eine rationale, ohne Unterstellung 'geheimgehaltener Tatsachen' mögliche Erklärung des ADK hätte diesen Zusammenhang zwar auch erschließen und kritisieren können, aber stattdessen war das

gewichtigste Argument für diesen Zusammenhang stets NAIs Zugehörigkeit zur sogenannten 'Key Recovery Alliance',[123] die das Unternehmen 1997 widerrief.

Der verschwörungstheoretische Ansatz vermag auch nicht zu erklären, warum die Programmeigenschaft ADK keineswegs geheim gehalten wurde, sondern im Gegenteil offen angepriesen wurde, mit der – zunächst erfolgreichen – Kalkulation, so ganz neue Anwenderkreise für PGP zu erschließen.

Die vielleicht wichtigste Bedingung für eine weitere Popularisierung des Programms war jedoch schon vor dem ADK gesetzt worden. Bereits 1996 – kurz vor dem Wechsel von RSA zu DH/DSS, der von der Cypherpunk-orientierten Nutzergemeinde zurückhaltend bis skeptisch zur Kenntnis genommen worden war – erhält PGP erstmals eine grafische Benutzeroberfläche, mit denen die gewöhnungsbedürftigen Kommandozeilenbefehle der Vergangenheit angehörten.[124] Zwischen 1997 und 2002 baute Network Associates als Besitzer der Marke PGP die Interoperabilität des Programms systematisch aus. Vorkompilierte Versionen für verschiedene Betriebssysteme sowie Plugins für verbreitete E-Mail-, Groupware und Chatprogramme wurden in das Installationspaket integriert. Ende 1999, direkt nach der Veröffentlichung von GnuPG (siehe weiter unten), gewährte die US-Regierung PGP offiziell eine Exporterlaubnis ohne jede Beschränkung der Schlüssellänge – einzig die 'Schurkenstaaten' blieben und bleiben weiterhin von dieser Erlaubnis ausgenommen.[125] Ein halbes Jahr später machte PGP Negativschlagzeilen, als ein kritischen Fehler bei der Implementation des ADK entdeckt wird.[126] Network Associates, Inc. beeilte sich mit der Lösung des Problems. NAI und auch der neue Besitzer von PGP (PGP Corp.) ließen den Quellcode der kryptographischen Kernkomponenten von PGP stets geöffnet, und die Inkompatibilität zu den alten PGP-Versionen

123 Ein Kreis von IT-Unternehmen, den die Regierungsbehörden in einem institutionalisierten, aber offenbar eher unverbindlichen Rahmen von den Vorzügen zu überzeugen versuchte, die es für sie hätte, sich aktiv an den Regierungsplänen zur obligatorischen Hinterlegung von Zweitschlüsseln zu beteiligen.

124 GUI ab PGP 4.5, Umstieg auf DH/DSS ab PGP 5.0 – beide Versionen wurden herausgegeben von der Firma Viacrypt, die nach Phil Zimmermann und vor Network Associates Besitzer der Marke PGP war.

125 Nancy Weil: United States grants PGP encryption export license. InfoWorld.com Dezember 1999 ⟨URL: `http://archive.infoworld.com/articles/en/xml/99/12/13/991213enpgp.xml`⟩ – Zugriff am 1.5.2003.

126 Bernd Schöne: Schlüssel für den dritten Mann. Die Verschlüsselungs-Software PGP hat ein Sicherheits-Leck. Süddeutsche Zeitung September 2000, Nr. 204.

mit RSA wurde längst wieder aufgehoben. Dennoch, von den 'klassischen' PGP 2.x-Versionen einmal abgesehen, die heute noch zum Lieferumfang allen wichtigen Linux-Distributionen gehören, ist das Markenimage von PGP inzwischen angeschlagen. Aber auch sachlich hat das Produkt PGP Schäden von der wechselvollen Geschichte seiner Kommerzialisierung davongetragen. So hatte sich unter der Ägide von NAI herausgestellt, dass die Kommandozeile PGPs Cash Cow ist. Sie erleichtert automatisierte Kryptographieanwendungen auf Servern, und dieses Feature wird von E-Commerce-Betreibern und -Dienstleistern gut bezahlt. Auf einem klassischen Feld wie der verschlüsselten Übertragung von Kreditkartennummern an Onlineshops vermag PGP mit Produkten wie SSL zu konkurrieren. Beim Verkauf von PGP an die PGP Corporation behielt NAI dieses Filetstück, mit der merkwürdigen Konsequenz, dass PGP Corp. das Programm nun mit rein graphischer Oberfläche verkauft.

1999 brachte der deutsche Programmierer Werner Koch GnuPG heraus, einen Klon von PGP – ein Nachbau also, der genau so funktionieren soll wie das Original. Koch verwendet dazu ausschließlich Code, auf den keinerlei Patentansprüche erhoben werden. Daher war GnuPG im Lieferzustand zunächst inkompatibel zu den alten PGP-Versionen, denn der bis damals noch patentgeschützte RSA-Algorithmus konnte ja nach Kochs Maxime nicht ins Programm übernommen werden. Anders als beim Erscheinen von PGP 5.0 Mitte der neunziger Jahre nahm dies jedoch niemand Koch übel, denn GnuPG steht unter der 'General Public License' (GPL), und diese Lizenzform versprach den PGP-Nachfolger vor den Übeln der Kommerzialisierung von PGP gefeit zu machen.

Der GPL zufolge muss das Programm jedem Benutzer komplett als Quellcode nicht nur zur Einsicht, sondern auch zur individuellen Veränderung zur Verfügung stehen, und zwar explizit für jeden denkbaren Zweck. Dafür gilt eine einzige Einschränkung: Was immer mit dem Code gemacht wird, darf lediglich unter genau denselben Bedingungen wie das Original wiederveröffentlicht werden. Unbeschränktheit in Hinsicht auf die Benutzung des Programms und die legitime Veränderbarkeit des Codes verbreiten sich somit auf alle Erweiterungen und Bearbeitungen des Codes von Koch und seinem Team. Die GPL wurde von Richard Stallmann erfunden und erlangte im Laufe der neunziger Jahre Berühmtheit durch die Verbreitung des unter der GPL stehenden Betriebssystems GNU/Linux, dessen Komponenten von tausenden Entwicklern weiterentwickelt wird, die via

Internet zusammenarbeiten. In den siebziger Jahren gab es zur Unterscheidung zwischen freier, proprietärer oder noch anders lizensierter Software keine Begriffe, denn es gab diese Unterschiede noch nicht – selbstverständlich war alles Public Domain, stand jedem bedingslos zur Verfügung. Die unternehmerische Großtat von Bill Gates bestand darin, frei verfügbare Software privat anzueignen, in der Gegenbewegung hierzu entstand die freie-Software-Bewegung.[127] Programmcode, so argumentiert Stallmann, lässt sich von allen benutzen, ohne dass dabei ein Mangel entsteht. Erst durch den Ausschluss Dritter von der völligen Verfügung über den Programmcode (das Geheimhalten des Quellcodes ist ein technisches Mittel dieses Ausschlusses, Lizenzverträge über den Gebrauch gekaufter Software ein juristisches) wird ein solcher Mangel künstlich erzeugt. Die GPL soll Software davor schützen, zum Material dieser profitablen Verknappung zu werden; damit soll sie zugleich den Interessen der Anwender und Entwickler von Software dienen.
Am Aufstieg und Fall von PGP ist abzulesen, inwieweit die Kommerzialisierung dieses Computerprogramms zugleich

1. wesentlich zur Durchsetzung kryptographischer Innovationen neuer Richtung beigetragen hat – PGP war Kristallisationspunkt der Entstehung kommerziell bedeutsamer kryptographischer Protokolle und Anwendungsbereiche und bewirkte sogar eine im Ansatz massenhafte[128] Verbreitung einer 'starken' Krypographieanwendung auf privaten PCs;

2. das Spektrum der Nutzungsmöglichkeiten dafür allerdings auch um Zwecke erweiterte, die im Widerspruch stehen zum Konzept eines solchen Programms als einer Waffe zur Verteidigung der individuellen Privatsphäre – wie es von seinem Erfinder Phil Zimmermann zunächst, in Fortschreibung der Intentionen der Erfinder der asymmetrischen Verschlüsselung, gefasst worden war;

3. dem Produkt selbst im Laufe seiner Entwicklung schadete – mittelbar, indem nicht zuletzt die Geringschätzung des Peer Review durch Network Associates, Inc. den ADK-GAU ermöglichte; unmittelbar, indem die Filetierung von

127 Tilman Baumgärtel: Am Anfang war alle Software frei. Microsoft, Linux und die Rache der Hacker. In Alexander Roesler und Bernd Stiegler (Hrsg.): Microsoft. Medien, Macht, Monopol. Frankfurt/Main, 2002, S. 105 f.

128 Vgl. 4.5.

PGP nach dem Verkauf durch Network Associates, Inc. das Programm ohne seine alte Kernkomponente, die Kommandozeile, zurück ließ;

4. durch all dies schließlich Anlass gab zur Schaffung eines Klons von PGP, GnuPG.

GnuPG nimmt die Kernfunktion seines Vorbilds PGP auf, soll jedoch nicht die negativen Folgen von dessen Kommerzialisierung erleiden müssen. Dass Programmeigenschaften wie der ADK in GnuPG fehlen, ist Ausdruck einer auch politischen Definition der Mängel von PGP. Zwischen den Intentionen der Autoren und Benutzer von GnuPG und der politischen Rolle, in der es von Deutschland und der EU aufgegriffen wurde, bestand von Anfang an objektiv eine Kluft. Die Förderung von GnuPG durch die Bundesregierung[129] zeigt, was es bedeutet, dass Quelloffenheit auch Offenheit gegenüber beliebigen Zwecken bedeutet – was von der GPL ja explizit verlangt wird. Rein formal stellt diese Forderung bereits klar, dass beim Programmieren oder Benutzen von Software unter der GPL die individuelle Privatsphäre keineswegs besonders berücksichtigt werden muss. Mittlerweile wird Quelloffenheit vielmehr als besonders zweckmäßiges Feature staatlich kontrollierter Informationstechnik diskutiert:

> „Zwar reicht allein die Offenlegung des Codes für Sicherheit nicht aus, jedoch ist sie eine essentielle Voraussetzung für effektive Sicherheitsuntersuchungen: Im herkömmlichen Closed-Source-Modell können trojanische Pferde nicht ausgeschlossen werden. Solche Systeme sollten gerade in sicherheitskritischen Bereichen nicht eingesetzt werden. Es besteht ein nationales Interesse daran, dass vertrauenswürdige Hard- und Software bereitgestellt [...] wird.“[130]

Im folgenden Abschnitt soll unter anderem erläutert werden, wie und mit welchen Zielen die Bundesregierung ein Programm wie GnuPG zu einem zentralen Mittel ihrer nationalen Kryptopolitik machen konnte.

---

129 Näheres dazu im folgenden Abschnitt.

130 Kristian Köhntopp, Marit Köhntopp und Andreas Pfitzmann: Sicherheit durch Open Source? Chancen und Grenzen. DuD – Datenschutz und Datensicherheit 2000, Nr. 24, S. 513.

5.3 Standortfaktor Kryptographie: Modell Deutschland und EU

Die Widersprüche der unverhofften staatlichen Beförderung der starken Kryptographie haben sich bis auf den heutigen Tag nicht gänzlich aufgelöst. Um den Standortwettbewerb um die Kryptographie und mit der Kryptographie in der zweiten Hälfte der neunziger Jahre zu verstehen, muss man zunächst ein paar Jahre zurück gehen.
Die USA waren viele Jahre erfolgreich darin, durch ihre internationale Dominanz viele Länder von den Potentialen der modernen Kryptographie abzuschneiden. Die von Cypherpunks und US-Bürgerrechtsbewegung aufgestellte Behauptung, es sei absurd, ein kompaktes geistiges Erzeugnis wie einen kryptographischen Algorithmus vor Ausländern fernzuhalten, klingt zwar charmant, ist aber kurzsichtig. Denn auch wenn sie unter Beweis stellten, dass sich einer der Hauptgegenstände des Exportverbots in fünf Codezeilen PERL ausdrücken lässt, nämlich wie folgt:[131]

```
#!/usr/local/bin/perl -- export-a-crypto-system sig, RSA in 5 lines of PERL:
($s,$k,$n)=@ARGV;$w=length$n;$k="0$k"if length($k)&1;$n="0$n",$w++if$w&1;die
"$0 -d|-e key mod out\n"if$s!~/^-[de]$/||$#ARGV<2;$v=$w;$s=~/d/?$v-=2:
$w-=2;$_=unpack('B*',pack('H*',$k));s/^0*//g;s/0/d*ln%/g;s/1/d*ln%lm*ln%/g;
$c="1${_}p";while(read(STDIN,$m,$w/2)){$m=unpack("H$w",$m);chop($a=
`echo 16o16i\U$m\Esm\U$n\Esn$c|dc`);print pack('H*','0'x($v-length$a).$a);}
```

hätten die Cypherpunks selbst am besten wissen müssen, wie es sich tatsächlich verhielt. Sie selbst waren es, die früh auf die fälschliche Überhöhung des bloßen Algorithmus aufmerksam gemacht hatten, und zeigten, welche große Bedeutung demgegenüber die sachgemäße Implementierung der kryptographischen Algorithmen hat, wie sie nur in Gestalt ökonomisch extensiver und inhaltlich ausgefeilter Computerprogrammierung und sonstiger Dienstleistungen zu bewältigen ist.[132]
Dem Ausland maßgeschneiderte Programme und Dienste, allgemeiner: Computerwissenschaftliche Expertise in Gestalt hochqualfizierter menschlicher Arbeitskraft

131 Um auf die Sinnlosigkeit des Krypto-Exportverbots aufmerksam zu machen, trugen Cypherpunks ab 1995 diese Kurzfassung von RSA demonstrativ als T-Shirt-Aufdruck, kopierten sie ans Ende ihrer E-Mails – und einige ließen sie sich sogar tätowieren. Der Erfinder der *export-a-crypto-system sig*-Kampagne war Adam Back, vgl. Adam Back: Adam Back's home page. 2003 ⟨URL: `http://cypherspace.org/~adam/`⟩ – Zugriff am 3.4.2003.

132 Bruce Schneier: Software Complexity and Security. Crypto-Gram Newsletter März 2000 ⟨URL: `http://www.counterpane.com/crypto-gram-0003.html#SoftwareComplexityandSecurity`⟩ – Zugriff am 1.5.2003.

vorzuenthalten, das war der wahre Nutzen der Kryptographie-Exportbeschränkungen für die nationalen Interessen der USA.

Am Modell Deutschlands lässt sich recht gut verfolgen, wie sich die kryptopolitische Standortkonkurrenz auf Seiten der EU geltend macht. Bereits 1994 forderte der Firmenverbund TeleTrust die Einführung der digitalen Signatur in Deutschland, und das Trustcenter[133] der Telekom nahm bereits seine Arbeit auf, noch bevor eine gesetzliche Grundlage dafür bestand. Da das ehemalige Telekommunikationsdienste-Staatsunternehmen Deutsche Telekom AG für den internationalen Markt der Telekommunikations-Dienstleistungen fit gemacht werden sollte, musste es ein Trustcenter anbieten – soweit, so klar. In Deutschland fiel zu diesem Zeitpunkt noch niemand als Cypherpunk auf, und selbst für Bürgerrechtler, die sich wegen der zunehmenden Vernetzung Sorgen machten, war Kryptographie schlicht kein Thema.[134] Für die breite deutsche Öffentlichkeit wird das Thema erstmals 1997 interessant. Auch die Rekapitulation der Geschichte der deutschen Kryptopolitik beginnt meist hier – eine unverständliche, ja geradezu selektive Erinnerung, war Deutschland doch bereits 1995 aktiv beteiligt an der Planung einer gesamteuropäischen Variante des GAK, dem europäischen Key Escrow System (Euro-KES).

> „Inzwischen machen sich auch europäische Regierungen Sorgen über ihre schwindenden Abhörmöglichkeiten. Für Europa sei allerdings, so ist aus der Europäischen Kommission zu hören, eine einfache Übernahme des Clipper-Konzepts nicht geplant. Da eine EU-weite Vereinheitlichung in Sachen Kryptoregulierung und Abhörgesetze auf absehbare Zeit nicht zu erwarten ist, suchen die nationalen europäischen Sicherheitsbehörden nach technischen Lösungen, die ein einheitliches Key-Escrow-Verfahren bei gleichzeitiger Erhaltung der nationalen 'Schlüsselsouveränität' ermöglichen. Verschlüsselte innerstaatliche Kommunikation soll fremden Sicherheitsbehörden nicht zugänglich sein.
> Inzwischen findet ein auf einem Vorschlag der britischen Information Security Group basierendes Konzept breite Unterstützung.“[135]

133 Trustcenter stellen Zertifikate für Public Keys aus und folgen dabei einer Certification Policy, mit der zum Beispiel die Rechtswirksamkeit der digitalen Signaturen garantiert wird, die mit dem zertifizierten Public Key gegengeprüft werden können.

134 Vgl. das gänzliche Fehlen des Themas Kryptographie in einem Buch wie Beat Leuthardt: Leben online. Von der Chipkarte bis zum Europol-Netz: Der Mensch unter ständigem Verdacht. Reinbek bei Hamburg, 1996.

135 Dirk Fox: Taube Ohren? Europa ahmt US-Lauschinitiative nach. c't Magazin für Computertechnik 1995, Nr. 12.

Der damalige Innenminister Kanther (CDU) schlug 1997 ein GAK-Modell für Deutschland vor.[136] Dieser Vorschlag passte gut in die Einstimmung der Bevölkerung auf den 'Großen Lauschangriff', der qua Änderung des Grundgesetzes wenig später die 'Bekämpfung der Organisierten Kriminalität' durch Abhörmaßnahmen im Privatbereich legitimierte. Aus Euro-KES und dergleichen wurde aber dennoch nichts, denn Von Justizminister Schmidt-Jortzig (ebenfalls CDU) bis zu Bürgerrechtsbewegten, die nun auf das Thema aufmerksam werden, war man sich in der Ablehnung einig. Parallel zu der ganzen Debatte wurde Deutschland im selben Jahr Vorreiter mit einem Gesetz zur digitalen Signatur; die EU folgt kurz darauf mit einer Maßgabe an alle Mitgliedsstaaten, Entsprechendes in ihrer nationalen Gesetzgebung zu verankern.

Danach passiert erst einmal nicht viel Neues auf der kryptopolitischen Bühne BRD. 1998 übernimmt eine rot-grüne Koalition die Regierungsmacht. 1999 kommt es dann zum deutschen Krypto-Herbst.

Voraussetzung war zu diesem Zeitpunkt nach wie vor, dass es die US-Regierung nicht ohne weiteres zuließ, Produkte mit 'starker Kryptographie' wie PGP ins Ausland zu exportieren, ein Verbot, das selbst von NATO-Bündnispartnern wie Deutschland keine Ausnahme machte. Rot-Grün begann nun geradezu eine Offensive gegen das Defizit, das Deutschland in der internationalen Standortkonkurrenz hatte. Nicht, prinzipiell anders handeln zu wollen als die USA, sondern, im Gegenteil, im Vergleich mit ihr aufzuholen – und dies unter den widrigen Umständen der amerikanischen Exportbeschränkung – war das Motiv dafür, nun in eine eigenständige, ja geradezu autarke Kryptographieentwicklung einzusteigen. Mit Trustcentern und Digitale-Signatur-Gesetzgebung auf der einen Seite, und – den massenhaften Kryptographiegebrauch vorwegnehmend kompensierende – Verschärfung der Wohnraum- und Telekommunikationsüberwachung auf der anderen war bereits ein Anfang gemacht worden, der nun rasch ausgebaut wurde. Nicht Politiker, sondern eine angesehene deutsche NGO im Computerbereich, der Förderverein Informationstechnik und Gesellschaft e.V. (FITUG) formulierte die konfrontative Ausrichtung der neuen deutschen Kryptopolitik bereits in einer Pressemitteilung nach

136 Bernd Graff: Der Krypto-Komplex. Warum das Internet und E-mail den Minister Kanther ärgern. Süddeutsche Zeitung 9. Mai 1997, Nr. 105.

der Bundestagswahl.[137] Die Mitteilung trägt bereits einen programmatischen Titel. Der neuen deutschen Regierung wird empfohlen, die „US-amerikanische Krypto-Kontrollpolitik“ nicht zum „Vorbild für Europa“ zu machen. Die folgenden drei Gründe werden dafür am Ende der Mitteilung aufgezählt: Erstens habe die Diskussion über Echelon im Europäischen Parlament gezeigt, wie weit in Richtung „einer Totalüberwachung des Bürgers [...] gerade auch die Interessen der Vereinigten Staaten gehen“. Zweitens benötige „die deutsche und europäische [...] gleiche oder bessere Möglichkeiten“ als die amerikanische Industrie „zum Schutz ihrer vertraulichen Kommunikation“, solle sie „keinen gravierenden Wettbewerbsnachteil erleiden“. Drittens und letztens würden Krypto-Restriktionen „[innovative] und aufstrebende Technologieunternehmen“ schwächen oder gar „zum Auswandern“ treiben, was sich Europa „in der heutigen Situation nicht leisten“ könne.

Von Deutschlands Engagement für den Euro-KES und öffentlichen Debatten in Deutschland, die den GAK noch als zumindest diskutabel erschienen ließen, weiß die Pressemitteilung des FITUG zu abstrahieren. Der deutsche Kursschwenk zur Kryptoliberalität geschah zu einem Zeitpunkt, als von den Clipper-Protagonisten in den USA bereits monatelang nichts mehr zu hören gewesen war; dieses Programm wurde zwar nie offiziell für aufgegeben erklärt, war zu diesem Zeitpunkt jedoch erkennbar eingeschlafen.[138] Aber auch als die Clinton-Regierung die Abschottungslinie in der Kryptopolitik 1999 aufgab[139] hatte man in Europa bereits eine weitere Gelegenheit gefunden, sich im kryptopolitischen Wettbewerb mit den USA in die Pose moralischer Überlegenheit zu werfen: Das US-amerikanische Abhörsystem Echelon als unkalkulierbares Risiko für die Privatsphäre europäischer Bürger. Im Jahr 2000 erfolgt mit der Einsetzung einer Kommission des Europäischen Parlaments zum Thema der bisherige Höhepunkt in der Kampagne gegen Echelon. In ihrem Bericht vom Jahr 2001 holt diese Kommission erstens weit aus zu einem Vorwurf an die USA; ausführlich wird beschrieben, was sich die Aus-

137 Förderverein Informationstechnik und Gesellschaft (FITUG e.V.): FITUG: US-amerikanische Krypto-Kontrollpolitk kein Vorbild für Europa. München, 1998 ⟨URL: `http://www.fitug.de/news/aaron.html`⟩ – Zugriff am 1.5.2003.

138 Nur noch die Bundes-Strafverfolgungsbehörde FBI hielt die Forderung nach weit gehender Beschränkung des Gebrauchs abhörsicherer kryptographischer Systeme im US-Inland aufrecht – und tut das bis heute.

139 Vgl. weiter unten.

landsüberwachung von USA und einigen weiteren Verbündeten gegen den Datenverkehr in Europa herausnimmt.[140] Hervorgehoben wird der Vorwurf gegen die US-Regierung, amerikanischen Flugzeugbauern Echelon-Daten zur Wirtschaftsspionage gegen das europäische Airbus-Konsortium zur Verfügung gestellt zu haben. Zweitens kommt das Papier zu dem Schluss, dass angesichts all dessen auch Europa eine 'gemeinsame Aufklärung' benötige. Die Verteidigung gegen Echelon war nach 1999 ein besonders öffentlichkeitswirksamer Titel der EU dafür, einerseits die Entwicklung eigener Verschlüsselungssoftware wie GnuPG zu fördern und andererseits den Ausbau eigener weltweit abhörender Geheimdienste voranzutreiben.

Die Kampagne der EU zur Einstimmung auf den Ausbau ihrer eigenen Geheimdienste stößt bei den Bürgern der EU auf eine eigentümlich hohe Zustimmung, nicht nur beim FITUG. Die bürgerrechtliche oder gar libertäre Kritik staatlicher Politik scheint in Westeuropa keineswegs so stark verankert zu sein wie in den USA. Ansätze zu einer Bewegung wie den Cypherpunks werden regelmäßig überlagert von einer populären Abwehrhaltung gegen amerikanische Softwarefirmen, Geheimdienst- oder andere Staatstätigkeiten. Diese Abwehr sucht den Gegenstand ihrer Kritik in etwas, das sie für eine typische Ausprägung der US-amerikanischen Gesellschaft hält. Anders ist kaum erklärbar, warum der FITUG glaubte, die Bundesregierung öffentlich unter Druck zu setzen, indem er mahnend an das Negativbeispiel der angeblich US-typischen Tendenz zur 'Totalüberwachung des Bürgers' erinnert. Kurz zuvor hatte die neue Regierung in ihrem Wahlkampf damit geworben, dass sie in Punkto 'innere Sicherheit' nahtlos an die harte Linie ihrer Vorgängerregierung anknüpfen wolle. Ein jüngeres Beispiel aus einem europäischen Nachbarland, der Schweiz, ist der Eidgenössische Datenschutzbeauftragte Hanspeter Thür, der das europäische Engagement in der internationalen Standortkonkurrenz als ein verzweifeltes Ringen um die Aufrechterhaltung der eigenen Souveränität gegen deren Anfechtung durch die USA zu betrachten scheint. Die US-Administration suche „nach Hegemonie auf allen Ebenen". „Zunehmend werden nationale Gesetzgebungen ausgehebelt, indem die Vereinigten Staaten versuchen, die übrige Welt

140 Europäisches Parlament, Nichtständiger Ausschuss über das Abhörsystem Echelon: Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON). 2001 ⟨URL: `http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_de.pdf`⟩ – Zugriff am 1.5.2003.

ihrem Rechtssystem zu unterwerfen.“ Thür warnte vor der „sehr akuten Gefährdung unserer liberalen Ordnung“ durch ein Land, das „sich mit Bezug auf Daten- und Persönlichkeitsschutz auf dem Niveau eines Entwicklungslandes“ befinde – gemeint waren wieder die USA.[141]

Der FITUG beschrieb mit seinen Empfehlungen, was die neue Bundesregierung tatsächlich vorhatte. Sie unterstützt nun die Entwicklung einer starken Verschlüsselungssoftware, die zwar kompatibel zu PGP ist, aber eben eine eigene Entwicklung darstellt: GnuPG. Da das Programm unter der GNU General Public License entwickelt wird, wird dabei passenderweise systematisch die Verwendung von Patenten vermieden, die im Bereich der Kryptographie fast immer US-Patente wären. 1999 erschien GnuPG in der Version 1.0, unterstützt durch staatliche Finanzierung der Entwicklung und Verbreitung des Programms – ein durchaus historisch zu nennender Vorgang, denn „(d)amit beteiligt sich weltweit erstmalig eine Regierung offiziell und aktiv an der Entwicklung von freier Open Source Software.“[142] Die Bundesregierung verstand es besser als FITUG, die Abnabelung von der amerikanischen Kryptopolitik nicht nur als einen Dienst am Standort darzustellen, sondern diesen Schritt zugleich und scheinbar bruchlos aus der Kritik an der Kommerzialisierungsgeschichte von PGP hervorgehen zu lassen, wie sie von Cypherpunks und GnuPG-Entwicklern – teils in nachvollziehbarer, teils in verschwörungstheoretischer Weise – geübt worden war.

> „[...] zur Zeit können wir kein E-Mail-Verschlüsselungsprogramm empfehlen. [...] Die Bewertung [großes Vertrauen in PGP aufgrund der Quelloffenheit seines Programmcodes; L.H.] muss heute aber neu vorgenommen werden, seitdem der PGP-Erfinder Phil Zimmermann sein Produkt verkauft hat und PGP nun im Grunde ein kommerzielles Produkt der US-Firma Network Associates darstellt. Dieses Unternehmen soll seinerseits eng mit der National Security Agency (NSA) kooperieren. Welchen Wert die heute über das Internet vertriebenen Versionen im Hinblick auf die Sicherheit haben, kann nicht mehr beurteilt werden. Auch das Bundesamt für Sicherheit in der Informationstechnik

141 Angela Meyer: Schweizer Datenschutzbeauftragter übt harte Kritik an den USA. Heise News-Ticker Juli 2003 ⟨URL: `http://www.heise.de/newsticker/data/anm-01.07.03-000/`⟩ – Zugriff am 1.7.2003.

142 Rainer W. Gerling und Stefan Kelm: PGP, quo vadis? Die Zukunft von PGP, GnuPG und OpenPGP. DuD – Datenschutz und Datensicherheit 2001, Nr. 25 ⟨URL: `http://www.lrz-muenchen.de/~rgerling/pdf/dud2001_336.pdf`⟩ – Zugriff am 1.5.2003, S. 3.

> (BSI) weist auf mögliche erhebliche Schwachstellen hin und empfiehlt das Produkt wegen möglicher 'Falltüren' jedenfalls nicht für den Einsatz in der öffentlichen Verwaltung. [...] Fazit: es gibt im Moment keine einfache und sichere Lösung der E-Mail-Kryptographiefrage für den Privatanwender."[143]

Die Krypto-Liberalisierung hatte in den USA im Jahre 1999 ihren vorläufigen Höhepunkt gefunden, am symbolträchtigsten vielleicht in Gestalt der kurz nach der Veröffentlichung von GnuPG erteilten Exportlizenz an NAI für PGP mit starker Verschlüsselung. Die USA haben ihre nationale Exportkontrollpolitik in diesem Jahr zwar nicht aufgegeben, aber deutlich gelockert – ausgenommen sind nach wie vor die Maßnahmen gegen 'Schurkenstaaten'. Ebenfalls 1999 bekräftigte und generalisierte der US-Bundesgerichtshof den Schutz der Kryptographie durch den Free Speech-Verfassungszusatz. Ferner schrieb die Normierungsbehörde NIST den *Advanced Encryption Standard* (AES) aus.[144] Damit war das Urteil der Untauglichkeit, das die Kryptowirtschaft schon lange zuvor wegen der zu geringen Schlüsselgröße des alten Standards DES über diesen gefällt hatte, zur handlungsleitenden Maxime der US-Regierung geworden. Nun ließ das Commerce Department durch das NIST in aller Öffentlichkeit einen Nachfolger suchen, und Bewerbungen dafür wurden auch aus dem Ausland entgegengenommen. Ausgerechnet ein Kandidat aus Belgien, mitten in Europa, machte das Rennen: Rijndael.

Die Parallelentwicklung zwischen USA und EU beim Beaufsichtigen der elektronischen Kommunikation ging übrigens auch nach den Terroranschlägen gegen Ziele in den USA am 11. September 2001 weiter. Seitdem bauen die USA vor allem mit dem PATRIOT Act die Kompetenzen sowohl von Strafverfolgungsbehörden als auch Geheimdiensten weiter aus. Parallel dazu feilt der Europäische Rat weiter an einer schon seit längerem geplanten Richtlinie der nationalen Gesetzgebungen mit vergleichbarem Inhalt, der 'Convention on Cybercrime'.[145] Der Convention zufolge

---

143 'Sicherheit im Internet' (BMWi, BMI und BSI): Gute und schlechte Nachrichten zur eMail-Verschlüsselung. 1999 ⟨URL: `http://www.sicherheit-im-internet.de/themes/print.phtml?tdid=38`⟩ – Zugriff am 3.4.2003.

144 NIST: Advanced Encryption Standard (AES) Home Page. ⟨URL: `http://www.nist.gov/aes`⟩ – Zugriff am 1.5.2003.

145 Council of Europe, Treaty Office: Convention on Cybercrime. ETS No. 185. 2001 ⟨URL: `http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185`⟩ – Zugriff am 1.5.2003.

sollen zum Beispiel Telekommunikationsdienste-Anbieter darauf verpflichtet werden, auf ihre eigenen Kosten den Behörden jederzeit das Abhören aller Datenkanäle zu ermöglichen. Auch die übergesetzliche Norm, derzufolge ein Angeklagter nicht dazu gezwungen werden darf, sich selbst zu belasten, wird im Entwurf der Convention relativiert. Zwar soll jeder seine Daten verschlüsseln dürfen, aber wer eines Vergehens verdächtigt wird, soll dazu genötigt werden dürfen, die dazugehörigen Secret Keys oder Passwörter herauszurücken.

6 Die Zukunft der Kryptologie in der Standort-Nation

Im vorangegangenen Kapitel war beschrieben worden, wie zwischen 1996 und 1999 die Debatte um Regulierungen des inländischen Kryptographiegebrauchs kulminierte. Die faktische Kraft des E-Commerce-Booms, der politische Priorität erheischte, bestimmte den Verlauf der Debatte. Verhandelt wurde um nicht weniger als die letzte Chance, das Flussbett des reissenden Stroms Internet zu begradigen. Entweder würde diese Chance jetzt ergriffen, oder die „crypto anarchy“ hätte gesiegt. Ferner sah man, wie sich vollzog, was sowohl ordnungspolitische Hardliner als auch der cypherpunk-orientierte Großteil der Fachöffentlichkeit als den Sieg einer Seite in der Kryptodebatte interpretiert. Im Kern handelte es sich dabei um die Liberalisierung der US-amerikanischen Krypto-Exportpolitik. Es bleibt nun die Frage, inwiefern ein nationales Interesse bleibende Grundlage für eine widerspruchsfreie gesellschaftliche Gebrauchsweise der Kryptographie neuer Richtung sein kann. Im folgenden Abschnitt soll daher der Versuch unternommen werden, den gesellschaftlichen Kryptographiegebrauch zu umreissen, wie er unter den aktuellen politischen und ökonomischen Bedingungen der Industrieländer aussieht oder demnächst aussehen könnte.

6.1 Digitaltelefonie und kryptographische Technik

In Deutschland und den anderen EU-Ländern hatte bereits zu Beginn der neunziger Jahre die technische und legitimatorische Vorbereitung auf ein umfassenderes, systematischeres Abhören der inländischen Telekommunikation begonnen.

Hintergrund dieses Prozesses, der auf EU-Ebene offiziell vor allem der Terrorismusbekämpfung dienen sollte, war der Plan zu umfassenden Privatisierung der Telekommunikationsdienste-Infrastrukturen. Da Dienstleister und Abhörer nicht mehr identisch waren, musste das Abhören anders organisiert werden. Die Besonderheiten der Digitaltechnik und die kryptopolitische Diskussion diesseits und jenseits des Atlantiks spielten im Prozess der technischen und politischen Organisation des Abhörens stets eine entscheidende Rolle. In Deutschland reagierte der Gesetzgeber früh und entschlossen auf die Diskussion über die 'letzte Chance zur Flußbett Begradigung', die Mitte der neunziger Jahre stattfand. Man versah das Telekommunikationsgesetz (TKG) von 1996 mit den §§88-90, die besagen, dass die öffentlichen Telekommunikationsdienste-Anbieter sich technisch darauf einrichten müssen, alle Daten, die bei der Individualkommunikation ihrer Kunden anfallen, bei Bedarf den staatlichen Organen zur Verfügung zu stellen.[146] Interessanterweise provozierte dieser gesetzgeberische Akt wenig öffentliche Reaktion, anders als der 'Große Lauschangriff' zwei Jahre später,[147] oder die zu erwartenden Ausführungsvorschriften zu den §§98-90 TKG. Bei diesen Abhörvorschriften handelte es sich um die 2001 kontrovers diskutierte Telekommunikations-Überwachungsverordnung (TKÜV), die 2002 ihre veraltete Vorgängerin, die Fernmeldeanlagen-Überwachungsverordnung (FÜV) von 1995 ablöste.[148]

Die später konkretisierte und verschärfte Abhörvorschrift im TKG wirkt indirekt gestaltend auf ganze IT-Infrastrukturen wie vor allem die digitale Telefonie. Das Fehlen wirksamer Verschlüsselung in der Telefonie ist ein Exempel des Zusammenspiels von Abhörvorschriften, öffentlicher Wahrnehmung und Ökonomie. Im Falle der gesamten Digitaltelefonie liegt diesem Spiel stets derselbe Sachverhalt zugrunde: Es ist kein Geschäft mit einer End-to-end-Verschlüsselung beim Telefonieren möglich, wenn die Telekommunikationsdienste-Anbieter wie in Deutschland den Behörden jederzeit den Zugang zur Kommunikation erlauben müssen.

---

146 Telekommunikationsgesetz. BGBl I 25. Juli 1996 ⟨URL: `http://bundesrecht.juris.de/bundesrecht/tkg/`⟩ – Zugriff am 3.4.2003, S. 1120 ff.

147 Während der erhitzten öffentlichen Debatte um den 'Großen Lauschangriff' im Sommer 1997 war der deutsche Innenminister mit dem Vorstoß gescheitert, alle kryptographischen Schlüssel für den staatlichen Zugriff hinterlegen zu lassen; vgl. 5.3.

148 Telekommunikations-Überwachungsverordnung. BGBl I 28. Januar 2002 ⟨URL: `http://www.bmwi.de/Redaktion/Inhalte/Downloads/TKUEV1,property=pdf.pdf`⟩ – Zugriff am 3.4.2003, S. 458 ff.

Bereits Mitte der achtziger Jahre wäre der Einbau starker asymmetrischer Verschlüsselung in ISDN-Endgeräte möglich gewesen.[149] Sogar pseudonymisiertes Telefonieren über ein Netz Chaum'scher Mixe hätte man unter Einbeziehung der Vermittlungsstellen realisieren können, ohne dass die Diensteanbieter auf die Erhebung von Daten hätten verzichten müssen, die sie zur individuellen Abrechnung benötigen.[150]

Gleiches gilt für das in Europa und vielen anderen Ländern seit 1991 kommerziell verfügbare Mobiltelefonsystem GSM (groupe-speciale-mobile). Es erlebte im Laufe der neunziger Jahre einen Boom, der zur heute längst massenhaften Nutzung von Mobiltelefonen führte. GSM war von vornherein auf größtmögliche technische Kompatibilität zu ISDN angelegt. Die Weglassung kryptographischer Technik neuer Richtung ist dem GSM-Netzsystem gleichwohl noch deutlicher anzumerken als ISDN, nicht nur, weil es später als ISDN eingeführt wurde, sondern vor allem weil GSM ohnehin durch den Einsatz von kryptographischer Technik sicher gemacht werden sollte.

Das allzu leichte Abhören analoger Mobiltelefonie wenigstens mit Strafe zu bedrohen, war eines der Hauptziele, mit dem in den USA der Electronic Communications Privacy Act (ECPA) erlassen worden war.[151] Eine vergleichbare Regelung war in Deutschland erst mit dem angesprochenen TKG zehn Jahre später eingeführt worden. Das lag nicht nur daran, dass schon zuvor der grundgesetzliche Schutz des Fernmeldegeheimnisses bestanden hatte. Vielmehr glaubte man in Westeuropa[152] auf eine sichere Karte zu setzen, indem man eine digitale Übermittlungstechnik für sein Mobiltelefonsystem wählte. Dieses konnte und sollte eine zuverlässige (symmetrische) Verschlüsselung der Daten auf dem Weg zwischen mobilem Endgerät und Basisstation beinhalten: Kryptographie als technische Kriminalprävention, die im nationalen Maßstab alle Probleme der älteren amerikanischen Analog-

149 vgl. 3.2 zu der Realisierung von ISDN-Endgeräten mit integrierter PKC durch das US-Militär in den achtziger Jahren.

150 A. Pfitzmann, B. Pfitzmann und M. Waidner: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2*64 + 16)-kbit/s -Teilnehmeranschluß. Datenschutz und Datensicherung DuD 12 1989 ⟨URL: `http://www.semper.org/sirene/publ/PfPW1_89TelMixeDuD.ps.gz`⟩, S. 30 f.

151 Vgl. 3.2.

152 Die technische Planung von GSM fand in den achtziger Jahren statt, also noch unter Ausschluss der osteuropäischen Länder.

Mobiltelefonie von vornherein vermeiden sollte. Bei Einführung von GSM hätten mit Algorithmen wie RSA längst erprobte Technologien zur Verfügung gestanden, die das Problem der Abhörbarkeit zwischen Basisstation und Mobilgerät zuverlässig gelöst hätten. Aus der Sicht der Endanwender hätten sie auch den Zusatznutzen einer End-to-End-Verschlüsselung ermöglicht, also eine Verschleierung der Inhaltsdaten gegenüber allen Basisstationen und Vermittlungsstellen. Je nach Implementierung des Algorithmus in die Geräte wäre sowohl eine asymmetrische End-to-End-Verschlüsselung möglich gewesen als auch – unter Rücksichtnahme auf das Staatsinteresse am Abhören – eine Verschlüsselung lediglich der Strecke zwischen Basisstation und Mobilteil. Die an der Entwicklung des neuen Standards beteiligten Staaten und Unternehmen in Westeuropa zogen es jedoch vor, von der gesamten Entwicklung der Kryptologie neuer Richtung keinen Gebrauch zu machen. Am markantesten kommt dies darin zum Ausdruck, dass man das symmetrische Verschlüsselungsverfahren von GSM geheim hielt, statt auf Algorithmen oder gleich komplette Anwendungen zurückzugreifen, die bereits der jahrzehntelangen Prüfung einer breiten, engagierten Fachöffentlichkeit standgehalten hatten.[153] Allein die Gefahr der Nähe zum Anwendungspektrum der kryptologischen Innovationen neuer Richtung schien man bei der Wahl des Verschlüsselungssystems vermeiden zu wollen. So kann es denn auch kaum überraschen, dass das in GSM bis heute verwendete symmetrische Verschlüsselungsverfahren der vernichtenden Kritik seitens der internationalen kryptologischen Fachöffentlichkeit verfiel.[154] Große Aufmerksamkeit erregte die deutsche Hacker-Organisation Chaos Computer Club (CCC), als sie 1998 eine SIM-Karte eines großen deutschen GSM-Diensteanbieters klonte.[155] Seitdem ist auf öffentlichen Websites zu erfahren, wie sich mit modernen PCs SIM-Karten für GSM-Handys innerhalb weniger Sekunden 'klonen' lassen, wie sich also eine voll funktionstüchtige Kopie nachbauen lässt. Wäre es nicht so, dass das hierfür zusätzlich erforderliche technische Equiqment heute, 2003, immerhin noch ca. 40.000 US-Dollar kosten würde, hätten sich die Anbieter von GSM-Diensten inzwischen sicherlich zu einer technischen Änderung genötigt gesehen. So hinge-

153 Ian Goldberg und Marc Briceno: GSM Cloning. 1998 ⟨URL: `http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html`⟩ – Zugriff am 1.5.2003.

154 A. a. O.

155 Chaos Computer Club: CCC klont D2 Kundenkarte. 1998 ⟨URL: `http://www.ccc.de:8080/thema/gsm/`⟩ – Zugriff am 1.5.2003.

gen spekuliert man weiter auf die Alltagstauglichkeit des schwer angeschlagenen Kryptosystems im auslaufenden Mobiltelefonnetzsystem GSM.

Bei dem Mobilfunkstandard UMTS, dessen Einführung heute, 2003, unmittelbar bevorsteht, sieht sowohl der kryptopolitische als auch der computertechnische Kontext der Weglassung starker Verschlüsselung ganz anders aus. Die Kryptoliberalisierung galt während der Planung von UMTS bereits als Faktum. Die Endgeräte des neuen Netzsystems verfügen über eine gegenüber allen älteren Telefonen deutlich erhöhte Prozessorleistung. Das Pfund des neuen Standards UMTS ist die Übertragung multimedialer Inhalte bis hin zur Übertragung kleinformatiger Videofilme. Unter diesen Randbedingungen kontrastiert der Verzicht auf den Einsatz von Kryptographie neuer Richtung deutlicher mit den vorhandenen technischen Möglichkeiten als bei allen Digitaltelefonnetzen zuvor. Tatsächlich wurde für UMTS lediglich ein neuer Standard der Authentifizierung zwischen Basisstation und Mobilteil eingeführt. Zentrale Register der Secret Keys aller Geräte bleiben somit weiterhin fester Systembestandteil. Die eingesetzte symmetrische Verschlüsselung soll lediglich besser funktionieren als jene im GSM-Netzsystem.

Abb. 5: *1999 – Das Internet bringt Menschen zusammen und macht sie alle reich und glücklich.*

Der Unterschied der kryptographischen Verfahren, wie sie selbst in den jüngsten UMTS-Plänen vorgesehen sind, zu Clipper[156] liegt vor allem darin, dass kein technisch riskantes und ideologisch schwer verkäufliches Defizit in ein Kryptosystem eingebaut werden muss. Die prinzipielle Rücksichtnahme auf das staatliche Aufsichtsinteresse drückt sich hier rein negativ aus. Es wird auf einen möglichen technischen Fortschritt verzichtet. Dieser Verzicht braucht nicht direkt angeordnet

156 Vgl. 4.5.

zu werden, sondern ergibt sich als sachliche Notwendigkeit aus den Anforderungen der Überwachungsvorschrift. Da die Abhörvorschriften in allen Industriestaaten ungefähr gleich aussehen, entsteht auch kein Effekt eines Zurückfallens im Wettbewerb zwischen unterschiedlich gestalteten nationalen Märkten. Auch besondere nationale Exportbeschränkungen, die ja ebenfalls als Hindernisse in der Standortkonkurrenz aufgefallen waren, müssen nicht mehr erwogen werden, da es keine potentiellen Exportmärkte gibt. Die Gestalt des Kryptographiegebrauchs in der gesamten Digitaltelefonie ist bestimmt durch einen international still und wirksam vermittelten Zwang nationalstaatlicher Gewalt.

6.2 Technikgestaltung durch den Exportvorbehalt: Wassenaar

Das Coordinating Committee for Multilateral Export Controls (COCOM), die multilaterale Exportbeschränkung von 'strategisch wichtigen' Gütern seitens der führenden NATO-Staaten, wurde 1994 aufgelöst. 1998 fand COCOM seinen Nachfolgevertrag im Wassenaar Arrangement.[157] Der übriggebliebene Gegner nach dem Kalten Krieg, eine Hand voll durch die USA definierter 'Schurkenstaaten',[158] blieben de facto das Hauptziel der Exportbeschränkungen. Außerdem hatten die USA und andere Länder bereits zu COCOM-Zeiten eine schärfere nationale Sonderregelung ihrer Exporte im Bereich der Kryptographie beschlossen. Das Abkommen von Wassenaar ermöglichte es den USA weiterhin, einerseits allseitige Anerkennung für die eigenen Restriktionspolitik zu suchen, andererseits aber die eigene Souveränität durch zusätzliche nationale Regelungen zu unterstreichen. Wassenaar hat weit mehr Teilnehmerstaaten als COCOM, insbesondere traten auch Staaten des ehemals real existierenden Sozialismus dem Vertrag bei. Beobachtet und unter Vorbehalt gestellt wurden nun der Export von sogenannten Dual-Use-Gütern an die Staaten außerhalb des Vertrags, unter anderem, nach weitgehend denselben Definitionen wie bisher, starke Kryptographie-Anwendungen. Eine Ausnahme wurde nun jedoch bei den 'Mass Market'- und 'Public Domain'-Programmen gemacht. Eine restriktivere nationale Sonderpolitik behielten die USA bei, und Industrie- und Militärgroßmächte wie Russland und Frankreich schufen sich ähnliche Sonderre-

157 The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies. ⟨URL: `http://www.wassenaar.org/`⟩ – Zugriff am 1.5.2003.

158 Iran, Lybien, Syrien, Nordkorea, Kuba und damals auch noch der Irak.

geln.[159] In diesen Ländern blieb zunächst weiterhin, dem Internet-Boom und dem darauffolgenden neuen internationalen Pragmatismus zum Trotz, offiziell auch der Export von Programmen wie PGP unter Vorbehalt gestellt. In den darauffolgenden Jahren erfuhren allerdings sowohl das Wassenaar Arrangement als auch die diversen nationalen krypto-exportpolitischen Sonderwege erhebliche Lockerungen. Es wäre nur die halbe Wahrheit, würde man behaupten, dass der Wegfall der Blockkonfrontation in Verbindung mit dem weltweiten Boom des Internets die USA zur allmählichen Liberalisierung getrieben hätten. Darüber, ob diese Entwicklung die US-Kryptopolitik irgendwann obsolet gemacht hätten, kann nur spekuliert werden. Der konkrete Anlass lag woanders. Spätestens seit Wassenaar lieferten sich die erfolgreichen Industrieländer, allen voran jedoch die EU und die USA, einen Wettlauf um den richtigen Einsatz und die richtige Dosierung nationaler Restriktionen gegen den Einsatz starker Verschlüsselung. Von der Sonderpolitik Frankreichs abgesehen, zeigte sich am Umgang mit dem Vertrag von Wassenaar, wie die EU in ihrer Kryptoexportpolitik ihre Lage in der Standortkonkurrenz mit den USA reflektierte und selbst zum Mittel dieser Konkurrenz machte. Aus der Not sucht die EU eine Tugend zu machen; weil sie selbst nicht das Stammland der Kryptoentwicklung ist, musste sie erst einen eigenen Kryptowirtschaftszweig etablieren und suchte deshalb ihr Heil in der Entgegensetzung zu den USA mittels einer relativ frühzeitigen und relativ großen Liberalität. Am deutlichsten kristallisierte sich der Wettlauf um die Verfügbarkeit von im Inland entwickelten, auf die Bedürfnisse des E-Commerce zugeschnittenen Kryptographieanwendungen im deutschen Krypto-Herbst von 1999, der am Schluss des vorangegangenen Kapitels geschildert worden war.

Die Ausnahmen in der ersten Fassung des Wassenaar-Vertrags verdeutlichen, wie stark die Zwecke des Kryptographiegebrauchs in den Kryptoanwendungen verankert sind, und wie die Art der Kryptoanwendungen dadurch zum Kriterium ökonomischer Sanktionierung wird.

---

159 In Frankreich war bis 1998 die Anwendung bestimmter kryptographischer Systeme für private Zwecke untersagt worden. Diesen interessanten kryptopolitischen Sonderweg zu diskutieren würde den Rahmen dieser Arbeit sprengen. Vgl. die auch bezüglich anderer Nationen beispiellose Zusammenfassung bei Bert-Jaap Koops: Crypto Law Survey. ⟨URL: `http://rechten.kub.nl/koops/cryptolaw/`⟩ – Zugriff am 1.5.2003, sowie speziell zu den Besonderheiten der französischen Entwicklung auch Shearer und Gutmann, S. 118.

> „Ausgenommen von der Exportkontrolle wurden 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.“[160]

Die im vorangegangenen Abschnitt erörterte Nicht-Implementation eines technischen Schutzes vor staatlichem Abhören in der Telefonie ist nicht zuletzt das Resultat indirekter Technikgestaltung durch multilaterale Vereinbarungen wie das Wassenaar Arrangement.

6.3 Verbindlichkeit schaffen und verantwortlich machen

> „Identitäten sind vielseitig, konstruiert und in Bewegung, ja manchmal sogar ganz und gar fliessend, und weisen nur noch wenig innere Kohärenz auf. Im Internet kann man sein, wer man will, und sich jeden Pass und jede Überzeugung und jede sexuelle Orientierung zulegen, gerade wie es einem beliebt.“[161]

Mit dem Internet lassen sich Daten auf neuartige Weise von A nach B bewegen, und das macht es auf macherlei Weise nützlich. Aber für seine Benutzer ist das Internet auch etwas anderes als dieses technische Mittel. Es ist eine Metapher geworden für die persönliche Verfassung und Potenz seiner Benutzer: Mit dem Internet und durch das Internet alles Mögliche sein zu können, aber nichts Bestimmtes sein zu müssen, mit allen verbunden zu sein ohne Verbindlichkeit.
Dieses Bild vom Internet hat durchaus einen Bezug auf die sachliche Verfasstheit seines Gegenstands. Im Abschnitt über die Entwicklung des Internet in den siebziger Jahren[162] war auf die strukturelle und technische Offenheit der neuen Computer-Netzwerke hingewiesen worden. Die Ausdehnung dieses strukturell und technisch offenen Netzwerks auf die breite, nichtakademische Bevölkerung in den

---

160 Christiane Schulzki-Haddouti: Umrüstung. Kryptographie gilt weiterhin als Waffe. c't Magazin für Computertechnik 1998, Nr. 26 ⟨URL: `http://www.heise.de/ct/98/26/052/`⟩ – Zugriff am 1.5.2003.

161 Nigel Barley: Du sollst keine anderen Firmen neben mir haben. NZZ Folio. Die Zeitschrift der Neuen Zürcher Zeitung November 2000 ⟨URL: `http://www-x.nzz.ch/folio/archiv/2000/11/articles/barley.html`⟩ – Zugriff am 1.5.2003.

162 Vgl. 2.1.

Industriestaaten geschah Ende der achtziger Jahre in Gestalt der Kommerzialisierung der Netze und Netzdienste. Der Internet-Boom der neunziger Jahre ergriff die Offenheit des Mediums in höchst ambivalenter Weise. Einerseits waren offene und durchgesetzte Standards Bedingung für die Eignung dieses spezifischen Netzes zum elektronischen Handel zwischen Unternehmen und bis in die Wohnzimmer der Konsumenten. Andererseits jedoch war die Offenheit von vornherein etwas zu Überwindendes. Die praktische Synthese dieses widersprüchlichen Bezugs auf die Vorgefundene Einheit 'Internet' sind strukturierende Akte, die das Internet als ganzes nicht austauschen müssen, um seine Gesichtszüge entscheidend zu prägen. Als Modell dieser Verbindlichkeit schaffenden strukturierenden Akte kann die digitale Signatur betrachtet werden.

Wie man gesehen hat, standen die diversen infrage kommende kryptographischen Algorithmen und Protokolle für die Signatur bereits lange vor dem Internet-Boom bereit. Was aber ist die Voraussetzung dafür, dass die digitale Signatur auch tatsächlich zum Verbindlichkeit herstellenden Element einer umfassenden informationstechnischen Infrastruktur wird? Der Schlüssel zu dieser Rolle liegt in der Hardware. Die private Verbreitung von PCs hat durch das Internet in den neunziger Jahren einen gewaltigen Schub erhalten. Inzwischen ist man sich in der Branche allerdings einig, dass der typische private PC keine hinreichend sichere Umgebung zur Realisierung rechtsverbindlicher Akte darstellt. Der Kryptologe Peter Gutmann fasst das Problem in einem anderen Kontext prägnant zusammen:

> „Current crypto implementations rely on software running under general-purpose operating systems alongside a horde of untrusted applications, ActiveX controls, web browser plugins, mailers handling messages with embedded active content, and numerous other threats to security, with only the OS's [Operating Systems; L.H.] (often almost nonexistant) security to keep the two apart."[163]

Sollen PCs dennoch als Brückenkopf des E-Commerce bis ins Wohnzimmer hinein dienen können, dann nur, indem der algorithmische Kern der Kryptographieanwendung in ein gesondertes Stück Hardware ausgelagert wird. Und es gibt weitere Ansprüche in der Fachöffentlichkeit an das Gerät für die digitale Signatur.

163 Peter Gutmann: An Open-source Cryptographic Coprocessor. In Proceedings of the 9th USENIX Security Symposium. Denver, Colorado, 2000 ⟨URL: `http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/gutmann/gutmann_html/`⟩ – Zugriff am 3.4.2003.

Auch wenn der PC mittlerweile im Wohnzimmer steht: Er ist immer noch nicht persönlich genug, er kann noch nicht jede einzelne Person jederzeit überall hinbegleiten, er ist nicht das permanent anwesende Interface zur netzwerkvermittelten Erwartung rechtsverbindlicher Akte. Die Lösung ist die Chipkarte. Bereits 1976 konstatierte Whitfield Diffie den Ruf der Industrie nach einer – damals noch nicht existierenden – Karte.[164] Nicht zu verwechseln mit der Magnetstreifenkarte, einem passiven, relativ leicht manipulierbaren Speichermedium, das dank seiner viel geringeren Herstellungskosten bereits weiter verbreitet ist, stellt die Chipkarte einen eigenständigen Computer dar. Alle kryptographischen Verschlüsselungs- und Signiervorgänge finden auf dem Kartenprozessor statt; er selbst enthält die dazu erforderlichen Schlüsselpaare und Zertifikate in einer von außen möglichst unzugänglichen Gestalt.

Mit der gesteigerten Sicherheit solcher Kartenanwendungen korrespondiert immer auch eine gesteigerte Determination durch den Aussteller der Karte über die Zwecke, zu denen sich die Karte verwenden lässt. Es braucht keineswegs verheimlicht zu werden, was die Karte macht; möglicherweise wird sogar der Quellcode der Kartenanwendung offen gelegt. Es ist auch möglich, den Kartenbeitzer sein Schlüsselpaar initial selbst auf der Karte erzeugen zu lassen.[165] Fest steht hingegen, welche Anwendungen mit der Karte möglich sind; eine Neuprogrammierung der Karte durch ihren Besitzer ist keinesfalls vorgesehen. Fest steht ferner, was zertifiziert wird, denn das Trustcenter, das die Karte ausgibt, verleiht ihr zugleich durch sein digitales Zertifikat Gültigkeit.

Bis heute gilt der Preis für die Massenproduktion einer solchen Karte und – da die Karte selbst kein eigenes Benutzer-Interface und erst recht keine Netzwerkanbindung hat – der Schnittstellen-Geräte als der kritische Punkt für die Einführung einer digitalen Signatur. Es scheint festzustehen, dass, wenn diese ökonomische Barriere erst einmal durchbrochen ist,[166] die Allgegenwart der Möglichkeit, eine

164 Diffie, S. 574.

165 Wenn die Generierung des Schlüsselpaars durch die Ausgabestelle geschieht, ist die digitale Signatur-Karte technisch ein Einfallstor zur zentralen Hinterlegung der Secret Keys. Unabhängig davon, was die beteiligten Akteure gerade beabsichtigen, hat die digitale Signatur-Chipkarte daher das technische Potential, einen Politikwechsel hin zum Government Access to Keys zu erleichtern.

166 In Deutschland steht dieser Durchbruch möglichweise kurz bevor: Der Zentrale Kreditausschuss der Spitzenverbände der deutschen Kreditwirtschaft (ZKA) will demnächst RSA-Chipkarten

elektronische Unterschrift zu leisten, gewollt werden wird. Doch worin besteht die Qualität der digitalen Signatur?

Im Fokus der digitalen Signatur steht der einzelne Anwender als Träger von Rechten und Pflichten. Möglichst jederzeit und unabhängig von seiner Umgebung soll er dem Anspruch genügen können, Verträge abzuschließen, rechtsverbindliche Erklärungen abzugeben, letztlich als Person für juristisch vorab definierte Handlungen haftbar gemacht werden zu können. Charakteristisch dafür ist, dass die digitale Signatur nur unter der Voraussetzung ihrer 'Non-Repudability' als tauglicher Ersatz der Unterschrift von Hand gilt, dass der Signierende also nicht abstreiten können soll, eine Unterschrift geleistet zu haben. Es handelt sich um eine unhintergehbare Prämisse des kapitalistischen Systems, dass die Handlungen aller daran Beteiligten rechtsverbindlich sind. Unsichtbarer Dritter noch des kleinsten und alltäglichsten Einkaufs ist die Rechte, Pflichten und Eigentum setzende staatliche Gewalt. Der Allgegenwart des Verbindlichmachens, der für jede Handlung schon vorab definierten rechtlichen Verantwortung ihres Akteurs fügen weder die handschriftliche noch die digitale Signatur etwas grundsätzlich neues hinzu – sie machen diese Allgegenwart nur empirisch deutlich, dienen als Anhaltspunkte der Einklagbarkeit und somit letztlich der gewaltsamen Durchsetzbarkeit rechtlich legitimer Ansprüche. Theodor W. Adorno betont die Gewaltsamkeit der ihrem Anspruch nach allumfassenden juridischen Sphäre im Kontext seiner Kritik der hegelschen Rechtsphilosophie.

> „Das juristische Gesamtbereich ist eines von Definitionen. Seine Systematik gebietet, daß nichts in es eingehe, was deren geschlossenem Umkreis sich entziehe, quod non est in actis. Dies Gehege, ideologisch an sich selbst, übt durch die Sanktionen des Rechts als gesellschaftlicher Kontrollinstanz, vollends in der verwalteten Welt, reale Gewalt aus."[167]

Das 'zu offene' Internet wird durch die digitale Signatur gesellschaftlich-nützlich 'semipermeabel' gemacht, um ausnahmsweise auf eine biologische Analogie zurückzugreifen. Nach wie vor wird es technisch möglich sein, dass Informationen frei von

---

ausgeben, die zum Gesetz über digitale Signaturen konform sind, zunächst vor allem für das Home Banking am privaten PC.

167 Theodor W. Adorno: Negative Dialektik. Frankfurt/Main, 1970, S. 304.

A nach B fließen – frei allerdings nur im Sinne einer technischen Ungebundenheit, hinter der jederzeit die reale Gewalt des Rechts als gesellschaftlicher Kontrollinstanz steht.

In Anbetracht des Gesagten ist die Identifizierbarkeit des Unterschreibenden kein Fehler von Politik oder Rechtsprechung, sondern, im Gegenteil, sie ist selbst wesentliches Merkmal der Signatur. Persönliche Identifizierbarkeit ist durch den ökonomischen Gehalt der Signatur erzwungen, sie ist dasjenige, was sie fürs kapitalistische Geschäft so interessant macht – und was ihr dann auch die entsprechende Würdigung in Gestalt von Gesetzen und anderen Weg ebnenden Staatsmaßnahmen einbringt. Und ist eine technische Infrastruktur wie die der digitalen Signatur einmal eingerichtet worden, wird damit eine neue ökonomische Dynamik ausgelöst. Nun 'lohnt' es sich auch bei vergleichsweise geringen Anläßen, Angestellte oder Kunden sich identifizieren zu lassen. In diesem Zusammenhang spricht der Kryptologe Roger Clarke von den „[increased] expectations of identification".[168]

Clarke pocht darauf, dass eine Public-Key-Infrastructure (PKI), die beispielsweise keine Pseudonyme vorsieht, technisch nicht nötig, moralisch falsch und ökonomisch unsachgemäß sei. In seiner eingehenden technologie-immanenten Kritik bezieht er den Maßstab der technische Utopie von Diffie/Hellman und den Cypherpunks auf 'konventionelle' PKIs, wie sie beispielsweise in Deutschland seit den neunziger Jahren geplant und vorbereitet werden. Ein Stratege der digitale-Signatur-gerechten PKI hierzulande äußert sich zur Frage nach der Zulässigkeit von Pseudonymen so:

> „'Das mit den Pseudonymen haben wir nicht so gerne', erklärt Arno Fiedler, Consultant von d-trust, hinter der die Bundesdruckerei steht. Die Kosten für den Einbau und die Pflege mehrerer 'Identitäten' seien enorm. Ein Markt sei dafür bislang auch nicht vorhanden, da der Sinn und Zweck der Signatur ja gerade die 'Nicht-Abstreitbarkeit' eines Rechtsvorgangs wie etwa eines Einkaufs sei."[169]

Noch deutlicher ist in diesem Punkt die kodifizierte staatliche Garantie für die Rechtsgültigkeit digitaler Signaturen. Die Staatsgewalt unterscheidet zwischen Signaturen im Geschäftsleben, die prinzipiell auch anonym bleiben dürfen, und dem,

168 Roger Clarke: Conventional Public Key Infrastructure: An Artefact Ill-Fitted to the Needs of the Information Society. Canberra, 2000 ⟨URL: `http://www.anu.edu.au/people/Roger.Clarke/II/PKIMisFit.html`⟩ – Zugriff am 1.5.2003.

169 Stefan Krempl: Kommt die Ausweispflicht fürs Internet? telepolis 2001 ⟨URL: `http://www.heise.de/tp/deutsch/inhalt/te/11014/1.html`⟩ – Zugriff am 1.5.2003.

was sie selbst über alle wissen will, die digital unterschreiben. Konsequenterweise wird die Anonymität der Staatsgewalt selbst gegenüber qua Signaturgesetz ausgeschlossen:

> „§14(2) Bei einem Signaturschlüssel-Inhaber mit Pseudonym hat der Zertifizierungsdiensteanbieter die Daten über dessen Identität auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies [...] erforderlich ist oder soweit Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen.“[170]

Bemerkenswert ist schließlich die Konvergenz zwischen einerseits der marktwirtschaftlichen Kalkulation, Anonymität lohne sich kaum, da das Geschäft mit der digitalen Signatur im Kontext des Rechtsverkehrs gemacht wird, und andererseits der definitive Anspruch der beaufsichtigenden nationalstaatlichen Macht darauf, alle Benutzer der rechtlich normierten digitalen Signatur identifizieren zu können. Nach dem Maßstab der Privacy, wie er im *New Directions*-Aufsatz[171] anklingt und im *PGP(tm) User's Guide*[172] ausformuliert worden war, läge ganz offensichtlich ein Vorteil darin, bei Kaufakten zum Beispiel im Internet ebenso zuverlässig anonym bleiben zu können, wie es der Fall ist, wenn man in einem Laden bar bezahlt. Aber um einen solchen Nutzen geht es bei der digitalen Signatur nicht, sondern vor allem darum, es den Einzelnen zu erleichtern, sich formal freiwillig äußeren Anforderung zu beugen.

Der Rationalisierung von Produktion und Distribution dient die verbesserte Identifizierbarkeit individuellen Handelns auch jenseits der juridischen Sphäre. Ein Beispiel für diese 'softe' Seite der verwalteten Welt, die noch weitgehend ohne Kryptographieanwendung auskommt, ist die Beobachtung der Kunden beim Besuch von Websites durch die elektronische Aufzeichnung ihres Surfverhaltens. Mit den so erhaltenen Daten sollen dann Produktpaletten und Werbung auf die Käuferschaft oder Einzelpersonen maßgeschneidert werden. Was das *Magazin für Computertechnik* (c't) über die Kryptographieanwendung in der Infrastruktur von Bluetooth-Funknetzen schreibt, scheint für Telekommunikations-Dienstleistungen und E-Commerce insgesamt zu gelten:

---

170 Gesetz über Rahmenbedingungen für elektronische Signaturen. BGBl I 16. Mai 2001 ⟨URL: `http://bundesrecht.juris.de/bundesrecht/sigg_2001/`⟩ – Zugriff am 3.4.2003, S. 876 ff.

171 Diffie und Hellman.

172 Zimmermann.

> „Die aktuelle Technik berücksichtigt die Bedürfnisse nach Anonymität und Privatsphäre in den Funknetzen so gut wie gar nicht. [...] Das liegt allerdings wohl auch daran, dass die Industrie geringes Interesse an einem anonymen Kunden hat. Gläsern ist er ihr allemal lieber.“[173]

Abschließend soll das Szenario des Kryptocomputers in jeder Brieftasche noch einmal zu der von Horst Feistel vorgeschlagenen Funktion der Kryptographie für den Schutz zentral gespeicherter persönlichen Informationen vor unbefugtem Zugriff ins Verhältnis gesetzt werden.[174] Vordergründig mag man Feistels Prognose als erfüllt betrachten: Dass es an Regulierungen und Abstufungen der Zugriffsmacht auf Daten fehlte, kann nicht ernsthaft behauptet werden. Interpretiert man Feistel emphatischer, dann hat seine Vision allerdings auch etwas mit der Frage zu tun, wer materiell – ob nun formal berechtigt oder nicht – mit Daten umgehen darf, die aus der Privatsphäre der Einzelnen, wo sie originär ausschließlich hingehören, in die Speicher der vernetzten Computer gelangt sind. Er richtet sein Interesse auf eine Ortsverlagerung der Daten vermittelst zentraler Großrechner und empfiehlt Kryptographie als ein Mittel, um die individuelle Privatsphäre trotz und bei dieser Ortsverlagerung zu respektieren. Die digitale Signatur durch RSA-Chipkarten verwirklicht diese Empfehlung – und stellt sie auf den Kopf: Nun ist die Kryptographie das Mittel, an Millionen kleiner Geräte persönliche Informationen zu erheben, die den zentralen Datensammlungen kaum anders hinzuzufügen wären.

7 Resümee

Whitfield Diffie und Martin Hellman waren keine ausführenden Ingenieure eines großangelegten Geschäftsplans, und sie waren auch keine verbeamteten Kryptologen eines Geheimdienstes. Sie hatten eine technische Utopie: Kein Dritter soll mithören oder -lesen können, was eine Person einer anderen mitzuteilen hat. Wenn es technisch ohne nennenswerten Aufwand möglich wäre, sich vor gegenseitigem Abhören zu schützen – wer würde das wollen? Sicherlich nahezu alle Nutzer der elektronischen Individualkommunikation, oder doch zumindest so viele, dass rasch

173 Michael Schmidt: Maskerade. Drahtlose Anonymität mit Bluetooth 1.2. c't Magazin für Computertechnik 12 2003, S. 224.

174 Vgl. 4.4.

ein Markt für Produkte und Dienstleistungen entstünde, die dieses Bedürfnis befriedigen. Und wenn es mit der gleichen Technik mögliche wäre, eine Entsprechung zur Unterschrift von Hand rein digital zu realisieren – umso besser. Der bisher fehlende Schritt ist die Erfindung selbst. Wenn diese Erfindung einmal gemacht und veröffentlich wäre, könnte und dürfte es bis zur Verwirklichung der Utopie nicht mehr lange dauern. Im Jahr 1976 führten die beiden mit der Veröffentlichung des Schlüsselaustauschs nach Diffie-Hellman öffentlich den Beweis, dass sich eine neuartige Kryptographie, die all das zu leisten vermag, konkret verwirklichen lässt.

Staatlich geförderte, offene Forschungsstrukturen und Großforschungsprojekte wie das junge Internet haben dazu beigetragen, dass die PKC erfunden wurde. Das steht im scharfen Kontrast dazu, dass diejenige staatliche Einrichtung der USA, die sich zunächst am intensivsten für Diffies und Hellmans Erfindung interessierte, ausgerechnet der Militärnachrichtendienst NSA war. Immerhin 15 Jahre lang hat die NSA die Durchsetzung der PKC aktiv behindert. Zwar entstand und wuchs mit dem Internet zugleich ein Medium, das allen Versuchen Hohn sprach, die Verbreitung der PKC aufzuhalten. Aber nicht nur die NSA pflegte bis in die neunziger Jahre hinein die Vorstellung, dieses Netz und sogar die IT-Infrastruktur der USA insgesamt ließen sich nach außen abschotten und zugleich nach innen, für nationale Abhörmaßnahmen, transparent machen.

Diese Kontrollphantasien wurden von Computerfreaks wie Tim Berners-Lee und Phil Zimmermann angefochten, die mit großem erfinderischem Potential das Ideal eines freien Informationsaustauschs ohne zentrale Kontrolle oder Aufsicht verfolgten. Während Berners-Lee 1991 mit HTML die Seitenbeschreibungssprache des World Wide Webs erfand, entwickelte im selben Jahr Zimmermann PGP. Dieses kleine, einfach zu bedienende Computerprogramm sollte allen PC-Nutzern die Möglichkeiten der PKC eröffnen – zumindest für den Gebrauch in der privaten E-Mail.

Die Technik-Praxis und Technik-Politisierung von Zimmermann und der libertären Bürgerrechtsbewegung der Cypherpunks griff die technische Utopie von Diffie und Hellman auf, war aber um historische Erfahrung reicher. Die Veröffentlichung der revolutionären Erfindung PKC bedeutete noch nicht die Realisierung der sozialen Absichten ihrer Erfinder. Um in dieser Richtung voranzukommen, musste die technische Utopie nun also ausbuchstabiert werden: Die Freiheit davor, abgehört und

beaufsichtigt zu werden, lässt sich nur in expliziter Entgegensetzung zum abhörenden Staat wahrnehmen und propagieren. Neben der prinzipiellen Verfügbarkeit kryptographischer Algorithmen zählt deshalb vor allem, dass fertige Anwendungen wie PGP benutzt werden können. Entwicklung und Gebrauch solcher Programmen wurde als kämpferische Wahrnehmung eines Rechts auf Privacy betrachtet, das zugleich immer schon Recht auf Eigentum und Handel ist. Die Hoffnung, PKC werde sowohl dem E-Commerce als auch der Privacy dienen, ist Teil der technische Utopie, von den Cypherpunks ausformuliert als „crypto anarchy".

Dieser Anarchismus inspirierte in den USA eine zunehmend an der Kryptopolitik interessierte liberale Öffentlichkeit. Unter dem Druck ihrer Ideen, der zur Vermarktung drängenden kryptographischen Technologie und des Standortwettbewerbs wandelte sich die Haltung der US-Administration radikal. Sie hatte nicht nur in Erfindungen wie der PKC eine Bedingung für den zukünftigen E-Commerce erkannt, sondern vor allem auch ihre eigene Rolle in diesem Bedingungsverhältnis: Der Staat wurde vom Monopolisierer und Eingrenzer zum Förderer und Beaufsichtiger der Kryptographie. Zu den Phänomenen der Übergangszeit gehörte der Plan, Kryptographiegebrauch zuzulassen, aber sich den Zugriff auf alle geheimen Schlüssel der Bürger zu sichern, eine Absicht, die sowohl in den USA als auch in Europa scheiterte.

Das nationale Interesse an einer Kryptographieentwicklung innerhalb der eigenen Grenzen ist keineswegs neu. Auch in der Welt des Standortwettbewerbs besteht ein Nutzen der Kryptographie weiterhin darin, im Krieg wie im Frieden kritische informationstechnische Infrastrukturen abzusichern. Nun jedoch, da Kryptographie auf dem freien Markt entwickelt wurde, sollte sie sich auch weltweit profitabel verkaufen lassen. Exportbeschränkungen sind seitdem nur noch dann funktional, wenn sie Standortkonkurrenten bei der Ausstattung von deren E-Commerce ökonomisch schaden. Im Übergang von der Handhabung der Kryptographie als einer Waffe hin zur Standortpolitik wird als gemeinsamer Nenner die nach außen gerichtete Agressivität der nationalstaatlichen Ziele deutlich. Als die rot-grüne Regierung in Deutschland mit dem legendären Schritt zur Förderung der freien PKC-Software GnuPG das Interesse und die Fähigkeit ausgedrückt hatte, kryptographische Software autark zu entwickeln, fiel für die Clinton-Regierung, die noch wenige Monate zuvor erwogen hatte, die Nutzung von Kryptographie im Inland zu beschränken,

der Grund weg, Network Associates, Inc. und ähnlichen Firmen die Vermarktung kryptographischer Produkte wie PGP im Ausland zu erschweren.
Nach innen scheint die standortpolitische Funktion der Kryptographie zunächst einmal weniger aggressiv ausgerichtet zu sein. Als notwendige Zutat für die Telekommunikation und elektronische Datenverarbeitung soll sie dabei helfen, die Produktion zu rationalisieren sowie vor allem Zirkulationskosten einzusparen; besonders wichtige Hauptzutat ist dabei die digitale Signatur. Worin liegt der spezifische soziale Effekt dieser Gestalt der Kryptographieanwendung?
Das große Rationalisierungspotential von Kryptographieanwendungen wie der digitalen Signatur liegt darin, Handlungen nicht nur informationstechnisch abbilden zu können, um diese Abbildungen in Datengestalt effektiv speichern, übertragen und verarbeiten zu können, sondern dabei auch die Personengebundenheit der Handlungen zuverlässig mitabbilden zu können, das heisst unbestreitbar durch die jeweiligen Personen. Diese marktwirtschaftliche Gebrauchsgestalt von PKC-Anwendungen steht nicht nur abstrakt im Gegensatz zum Schutz der privaten Individualkommunikation. Vielmehr lässt sie eine Konvergenz entstehen zwischen zwei staatlichen Haltungen zur Kryptographie, die sich historisch zunächst auszuschließen schienen: Einerseits das Nein zur Kryptographie, weil es das Abhören und Beaufsichtigen aller Bürger erschwert, andererseits das Ja zur Kryptographie, weil es das kapitalistische Geschäft erleichtert.
So richtig es ist, dass der E-Commerce-Boom dem Standort-Staat kaum eine Alternative zu einer umfassenden Krypto-Liberalisierung gelassen hat, so falsch wäre es, deshalb einen gleichzeitigen Niedergang der staatlichen Aufsichtsmacht anzunehmen. Die Kryptopolitik behauptet sich nicht nur machtvoll als nationale Politik nach außen, sondern gibt auch ihren Aufsichtsanspruch nach innen keineswegs auf. So wird die digitale Signatur nicht zuletzt als Mittel der technischen Kriminalprävention gefördert und gestaltet; typischer Ausdruck davon ist, dass die technische Infrastruktur der digitalen Signatur keine Pseudonyme vorsieht. Privatisierung der Telekommunikationsdienste und Kryptoliberalisierung gingen außerdem mit einer Reihe kompensierender Gesetzesverschärfungen einher, vom Ausbau der Geheimdienste über die Ausweitung der Abhörbefugnisse der Strafverfolger bis hin zum geplanten Einschnitt ins Zeugnisverweigerungsrecht. Abhörbefugnis mag luftig-hypothetisch klingen, hat jedoch materiell greifbare Folgen: Wechselseitig bestätigt durch internationale Abkommen wie Wassenaar Arrangement und Con-

vention on Cybercrime verhindern die Nationalstaaten durch ihre Gesetze zum Beispiel, dass im wohl größten Bereich der elektronischen Individualkommunikation, der Telefonie, Kryptographie zum Schutz der Privacy eingesetzt wird.

Doch die Einheit des nationalen Interesses an der Kryptographie neuer Richtung wird nicht nur durch staatlichen Zwang hergestellt. Im Kontext von Kryptographieanwendungen im Rechtsverkehr 'lohnt' es sich selbst nach rein marktwirtschaftlichen Maßstäben kaum, Privacy oder gar Anonymität anzubieten. Und auch jenseits der Kryptographieanwendung im Rechtsverkehr wird die Hoffnung von Datenschützern, die „positive Erfahrung 'privacy sells'" könne für die Unternehmen am Ende des Einbaus „marktwirtschaftlicher Elemente" in den Datenschutz stehen,[175] regelmäßig enttäuscht. Die Gebrauchsgestalt der Public-Key-Cryptography im E-Commerce dient nicht nur anderen Zwecken als der Privacy, sondern die marktwirtschaftlichen Zwecke scheinen sich darüber hinaus mit Privacy auszuschließen.

In den neunziger Jahren haben sich die Industrienationen die Kryptographie erneut zu ihrem Mittel gemacht, weil diese als Public-Key-Cryptography nützlicher Bestandteil alltäglich und massenhaft genutzter informationstechnischer Infrastrukturen werden konnte. Die technisch-utopische Hoffnung, die Diffie und Hellman mit ihrer Erfindung verknüpft hatten, realisierte sich hingegen nicht. Die Politisierung der technischen Utopie Diffies und Hellmans durch Zimmermann und die Cypherpunks konnte das Versprechen der Public-Key-Cryptography ebenfalls nicht erfüllen, und doch blieb auch sie keinesfalls folgenlos. Sie trug wesentlich zur Liberalisierung des Kryptographieeinsatzes bei.

Vom historischen Ergebnis her war die Kryptoliberalisierung in den neunziger Jahren vor allem eine notwendige Bedingung, die für die moderne Indienstnahme der Kryptographie durch das nationale Interesse erfüllt sein musste; als ein Schritt auf dem Weg zur Realisierung der technischen Utopie der Cypherpunks erwies sie sich bisher jedenfalls nicht. Aber die Cypherpunks haben viele Menschen mit einer Seite der Kryptographie vertraut gemacht, die in dieser Indienstnahme nicht vorgesehen ist, sondern bestenfalls als zu beaufsichtigende Randerscheinung in Kauf genommen wird. Dieses Moment autonomer, subversiver Technikaneignung ist mehr als nur ein guter Stoff für Anekdoten. John Schwartz beschreibt in der New York Ti-

175 Helmut Bäumler: Neue Wege im Datenschutz. 2000 ⟨URL: `http://www.datenschutzzentrum.de/material/themen/wirtscha/neuewege.htm`⟩ – Zugriff am 1.5.2003, S. 3.

mes, wie dieses Moment der jüngsten Kryptologiegeschichte praktisch wiederkehrt, wenn hedonistische Technikbegeisterte heute in Peer-to-peer-Netzwerken per Filesharing ihre Lieblingsspielfilme miteinander teilen.[176] Die Lobbies der Filmindustrie, andere Rechteverwerter und mit ihnen kooperierende Softwaregiganten würden sicherlich am liebsten die Entwicklung einer so interessanten Technologie wie die Peer-to-peer-Netzwerke wieder rückgängig machen, wenn das möglich wäre, oder alle einsperren, die etwas so Profitschädigendes entwickeln und verbreiten. Dieser Wunsch wird sich ihnen zwar sicher nicht erfüllen, aber was stattdessen geschehen wird, unterliegt keiner historischen Determination. Vielleicht, wahrscheinlich sogar, wird die Industrie selbst kommerziell vielversprechende Einsatzgebiete für diese neue Technologie finden, vielleicht werden aber auch erneut ein paar selbstbewusste Protagonisten wissen, welche Technik sie zu welchen Zwecken einsetzen wollen – und es einfach tun.

176 John Schwartz: The attack on peer-to-peer software echoes past efforts. The New York Times 22. September 2003.

Glossar

ADK Additional Decryption Key; von Network Associates, Inc. in PGP eingeführte Option, stets mit einem zweiten Public Key zu verschlüsseln, um mit dem dazugehörigen Secret Key, der zum Beispiel bei der Geschäftsleitung hinterlegt sein kann, alle so verschlüsselten Daten jederzeit wieder entschlüsseln zu können; technisch vergleichbar dem EES; vgl. EES, NAI, PGP, Public Key, Secret Key.

AES Advanced Encryption Standard; vom NIST 1999 im Rahmen eines international ausgeschriebenen Wettbewerbs ermitteltes offizielles Standardverfahren der symmetrischen Verschlüsselung; Nachfolger von DES; vgl. DES, NIST, Symmetrischer Verschlüsselungsalgorithmus.

Algorithmus Abfolge von Rechenanweisungen.

Asymmetrischer Verschlüsselungsalgorithmus Verschlüsselungsverfahren wie DH und RSA, bei denen – im Gegensatz zur symmetrischen Verschlüsselung – mit einem Public Key ver- und einem davon verschiedenen Secret Key entschlüsselt wird; da der Sender zur Verschlüsselung nur den Public Key benötigt, muss er sich mit dem Empfänger nicht vorab über einen sicheren Kanal auf einen gemeinsamen Secret Key verständigt haben; dies ist das grundlegende Verfahren der PKC; vgl. Cipher, DH, PKC, Public Key, RSA, Secret Key, Symmetrischer Verschlüsselungsalgorithmus.

Certification Policy Protokoll zur digitalen Zertifizierung eines Public Keys; in einer Certification Policy kann zum Beispiel festgelegt werden, ob der Schlüsselbesitzer ein Mensch oder eine Maschine (zum Beispiel der Webserver eines Onlineshops) sein darf, ob auch Pseudonyme zertifiziert werden, und auf welche Art die Gewissheit über den Schlüsselbesitz erlangt wird; vgl. Zertifikat.

Clipper Kryptographischer Hardware-Baustein für PCs, mit dem die US-Regierung in den neunziger Jahren die Verschlüsselung mit einem den Regierungsbehörden zugänglichen Zweitschlüssel (EES) zum Standard machen wollte; vgl. EES, GAK.

Cipher Verschlüsselungsalgorithmus; vgl. Algorithmus, Asymmetrischer Verschlüsselungsalgorithmus, Symmetrischer Verschlüsselungsalgorithmus, Ciphertext.

Ciphertext Verschlüsselter (Nachrichten-)Text; vgl. Cipher; Plaintext.

COCOM Coordinating Committee for East-West-Trade-Policy; Vertragsorganisation westlicher Industriestaaten, mit der im Kalten Krieg der Export von Waffen, darunter auch kryptographischer Systeme, kontrolliert wurde; vgl. Wassenaar.

Code 1. In Bezug auf Datenverarbeitung: Die in einer von Menschen verstehbaren Programmiersprache wie zum Beispiel C (Quellcode) oder in einer von Computern ausführbaren Sprache (Binärcode) vorliegenden Rechenanweisungen eines Computerprogramms; 2. In Bezug auf Kryptographie: Synonym mit Key; vgl. Key.

Comsec, auch COMSEC Communications Security; Schutz informationstechnischer Infrastrukturen im Inland, neben dem Abhören ausländischen Nachrichtenverkehrs ein Hauptaufgabenbereich von Geheimdiensten wie NSA (USA) und Bundesnachrichtendienst (Deutschland); vgl. NSA.

Cypherpunks Von Jude Milhon an den Begriff Cyberpunk des Romanautors William Gibsons angelehnte Bezeichnung einer libertären US-Bürgerrechtsbewegung in den neunziger Jahren, die durch kryptographische Technologie den staatlichen Eingriff in die private Kommunikation bekämpfte und durch Organisationen wie die EEF meinungsbildend für eine kryptopolitisch liberal eingestellte Öffentlichkeit wurde; vgl. EFF, Privacy.

DES Digital Encryption Standard; 1976 von IBM mit Unterstützung der NSA entwickelter symmetrischer Verschlüsselungsalgorithmus, der bis in die neunziger Jahre im kommerziellen Bereich dominierend war, aufgrund seiner geringen Schlüssellänge jedoch als nicht mehr hinreichend sicher gilt.

DH Erster Algorithmus zum asymmetrischen Schlüsselaustausch; benannt nach Diffie und Hellman, von denen er 1976 veröffentlicht wurde; erster konkreter Nachweise einer neuen Richtung der Kryptographie, der PKC; vgl. Asymmetrischer Verschlüsselungsalgortihmus, PKC.

Digitale Signatur Elektronisches Äquivalent zur Unterschrift von Hand, das durch Verfahren der PKC ermöglicht wird; vgl. PKC.

DMCA Digital Millenium Copyright Act; US-Gesetz von 1998, das vor allem die Umgehung von DRM-Mechanismen in digitalen Medien untersagt; vgl. DRM, TCPA.

DRM Digital Rights Management; Kontrolle über die Bearbeitung und Verbreitung von Werken (meistens digitalen Medien wie zum Beispiel Musik-CDs) durch den Eigentümer der Verwertungsrechte, bei der häufig Verfahren aus dem Bereich der PKC eingesetzt werden, zum Beispiel digitale Signaturen; vgl. Digitale Signatur, PKC.

DSS Ein Verfahren aus dem Bereich der PKC, das digitale Signaturen und Zertifikate, nicht jedoch Verschlüsselung ermöglicht; die NSA versuchte, DSS als Standard im Bereich der digitalen Signatur durchzusetzen; vgl. Digitale Signatur, PKC, NSA, Zertifikate.

ECPA Electronic Communications Privacy Act; US-Gesetz, das seit den achtziger Jahren das Abhören der (elektronischen) Individualkommunikation reguliert: Privatgespräche dürfen nur von Staatsbehörden abgehört werden, Dienstgespräche auch vom Vorgesetzten; bis heute ist diese Art, die Privacy der Individualkommunikation zu regulieren, in den westlichen Industriestaaten modellbildend geblieben; vgl. Privacy.

EES Escrowed Encryption Standard; von der NSA entwickeltes Protokoll zur asymmetrischen Verschlüsselung mit dem Hardware-Baustein Clipper, bei der stets mit einem zweiten Public Key mitverschlüsselt wird, um mit dem dazugehörigen Secret Key, der zum Beispiel bei einer staatlichen Überwachungsbehörde hinterlegt sein kann, alle so verschlüsselten Daten jederzeit wieder entschlüsseln zu können; technisch vergleichbar dem ADK; vgl. ADK, Clipper, GAK, NSA, Public Key, Secret Key.

EFF Elecronic Frontier Foundation; bis heute aktive Bürgerrechtsorganisation aus dem Umfeld der Cypherpunk-Bewegung, die unter anderem Gebrauch und Entwicklung von PGP förderte und gegen Clipper und ähnliche GAK-Pläne protestierte; vgl. Clipper, Cypherpunks, GAK, PGP, Privacy.

FAQ Frequently Asked Questions; Akronym für die im Internet verbreitete Zusammenstellung ‘häufig gestellter Fragen’.

GAK Government Access to Keys; von Peter Gutman geprägter Sammelbegriff für alle kryptographischen Protokolle und Anwendungen, die den Zugriff von Regierungsbehörden auf die verwendeten geheimen Schlüssel vorsehen; prominentestes Beispiel ist Clipper; vgl. Clipper.

GnuPG GNU Privacy Guard; von Werner Koch und anderen 1999 programmierter PGP-Klon, der unter der GPL steht; vgl. GPL, Klon, PGP.

GPL General Public License; von Richard Stallman und anderen entwickelte Softwarelizens, die für quelloffen zugängliche Software.

GSM groupe-speciale-mobile; seit den neunziger Jahren vor allem in Europa verbreitetes, eng an ISDN angelehntes Übertragungsprotokoll für digitalisierte Telefonie in Mobilfunknetzen.

HTML Hypertext Markup Language; von Tim Berners-Lee und anderen 1991 geschaffene Seitenbeschreibungssprache fürs World Wide Web, die über Hyperlinks eine rein „semantische“ Verknüpfung zwischen textlichen und multimedialen Inhalten erlaubt; vgl. HTTP.

HTTP Hyperttext Transfer Protocol; von Webbrowsern verwendetes Protokoll der Übertragung vor allem von HTML-Seiten; vgl. HTML, Protokoll.

ISDN Integrated Services Digital Network; Seit den achtziger Jahren international verbreitetes Übertragungsprotokoll für digitalisierte Telefonie in Festnetzen.

ITAR International Traffic in Arms Regulations; die 1977 auf Drängen der NSA in Kraft getretene Ausdehnung der nationalen US-Waffenexportkontrolle unter anderem auf den Bereich „starker“ kryptographischer Systeme; im Laufe der neunziger Jahre wurde die ITAR gelockert; vgl. COCOM, Key, NSA.

Key Die vom Cipher zur Verschlüsselung eines Plaintexts verwendete Zeichenkette, nur bei asymmetrischen Verfahren wird ein Schlüsselpaar verwendet; die Länge des Keys ist entscheidend für die Unbrechbarkeit der erzielten Verschlüsselung, zum Beispiel unterscheidet die US-Waffenexportkontrolle ITAR

anhand der Schlüssellänge zwischen starker und schwacher Kryptographie; vgl. Cipher, ITAR, PKC, Plaintext.

Klon In Bezug auf Datenverarbeitung: Funktionsgleicher Nachbau eines Computerprogramms ohne Verwendung von dessen Quellcode; vgl. Quellcode.

Kryptanalyse Untersuchung kryptographischer Verfahren auf Möglichkeiten, diese zu brechen; vgl. Kryptographie, Kryptologie.

Kryptographie Lehre von der Entwicklung und Anwendung von Ciphern, mit denen sich ein Plaintext so in einen Ciphertext verschlüsseln lässt, dass ohne Wissen über den verwendeten Key die Verschlüsselung kaum rückgängig zu machen ist; vgl. Cipher, Key, Kryptanalyse, Kryptologie, Plaintext.

Kryptologie Einheit von Kryptographie und Kryptanalyse; vgl. Kryptanalyse, Kryptographie.

Mix Protokoll des Kryptologen David Chaum; durch die Weitergabe einer Nachricht über voneinander unabhängig operierende Vermittler nach dem Mix-Protokoll wird die Herkunft der Nachricht gezielt verschleiert.

NAI Network Associates, Inc.; vermarktete Mitte bis Ende der neunziger Jahre PGP und führte unter anderem den ADK ein; vgl. ADK, PGP.

NIST National Institute of Science and Technology; aus dem National Science Board hervorgegangene US-Behörde für technische Normen.

NSA National Security Agency; US-Militärnachrichtendienst, der in den fünfziger bis siebziger Jahren in der Kryptologieentwicklung weltweit führend war und diese Technologie weitgehend geheim zu halten versuchte; spätere wichtige Entwicklungen, an denen der NSA beteiligt war, waren unter anderem DES, DSS und Clipper; vgl. Clipper, DES, DSS.

OTP One Time Pad; von Gilbert Vernam 1918 erfundener symmetrischer Verschlüsselungsalgorithmus, bei dem der Key eine für nur einen einzigen Verschlüsselungsvorgang verwendete, zufällige Zeichenkette ist, die genau so lang ist wie der zu verschlüsselnde Plaintext; gilt als der einzige beweisbar sichere

Verschlüsselungsalgorithmus; vgl. Key, Plaintext, Symmetrischer Verschlüsselungsalgorithmus.

PGP Pretty Good Privacy; vom US-Amerikaner Phil Zimmermann 1991 geschriebenes Computerprogramm, das asymmetrischen Schlüsselaustausch, Ver- und Entschlüsselung, digitale Signatur sowie Zertifizierung eigener und fremder Schlüssel beherrscht und für verschiedene Computerprozessoren und Betriebssysteme verfügbar ist; PGP hat sich als Protokoll zur asymmetrischen Verschlüsselung und digitalen Signatur vor allem von E-Mails weltweit verbreitet; vgl. Asymmetrischer Verschlüsselungsalgorithmus, Digitale Signatur, PKC, Protokoll.

PKC Public-Key-Cryptography; durch asymmetrische Verfahren zum Schlüsselaustausch ermöglichte neue Richtung der Kryptographie, die spontane kryptographisch geschützte Nachrichtenübermittlung sowie digitale Signaturen zwischen beliebig vielen, einander unbekannten Teilnehmern erlaubt; sie hat die Kryptographie potentiell zu einem Mittel jeder elektronischen Individualkommunikation gemacht; vgl. Asymmetrischer Verschlüsselungsalgorithmus, Digitale Signatur, Kryptographie, PKI, Public Key, Secret Key.

Plaintext Unverschlüsselter (Nachrichten-)Text, vgl. Ciphertext.

PKI Public-Key-Infrastructure; konsistentes System aus Zertifikaten und Certification Policies; eine besondere PKI ist das Web Of Trust; vgl. Certification Policy, Digitale Signatur, PKC, Web of Trust, Zertifikat.

Privacy In der englischen Sprache: (Das Recht darauf) frei zu sein von der Teilnahme Dritter, zum Beispiel Individualkommunikation ohne staatliches Abhören.

Protokoll In Bezug auf Datenverarbeitung: Konvention über die genaue Weise der Verarbeitung von Daten, im Bereich der Kryptographie zum Beispiel der Einsatz bestimmter Verschlüsselungsalgorithmen mit betimmten Schlüssellängen.

Public Domain Werk, das ohne verwertungsrechtliche Beschränkung der Allgemeinheit zur Verfügung gestellt wird; im Gegensatz zu GPL-lizensierten Wer-

ken darf Public Domain auch in einer Gestalt bearbeitet und verbreitet werden, die einem Dritten die weitere Bearbeitung und Verbreitung unmöglich macht – zum Beispiel durch Weitergabe eines Programms nur als Binärcode, unter Geheimhaltung des Quellcodes; vgl. Code, GPL.

Public Key Der öffentliche Teil der in den asymmetrischen Verschlüsselungsverfahren der PKC angewendeten Schlüsselpaare; vgl. Asymmetrische Verschlüsselungsverfahren, Key, PKC, Secret Key.

RFC Request for Comment; seit 1969 werden Bezeichnungen und Protokolle für den Gebrauch im Internet in den RFCs öffentlich vorgeschlagen und nach einem Stadium des Peer Review durch internationale Standardisierungsgremien als sogenannte Internet Standards verabschiedet.

RSA Asymmetrischer Verschlüsselungs- und Signaturalgorithmus, der 1978 von Ronald Rivest, Adi Shamir und Richard Adleman erfunden wurde – und nach ihnen benannt – wurde; wurde von der Firma RSA Data Security, Inc. vermarktet und ist bis heute der am häufigsten angewendete asymmetrische Verschlüsselungsalgorithmus; vgl. Asymmetrischer Verschlüsselungsalgorithmus, Digitale Signatur.

Secret Key Der geheime Teil der in den asymmetrischen Verschlüsselungsverfahren der PKC angewendeten Schlüsselpaare; vgl. Asymmetrische Verschlüsselungsverfahren, Key, PKC, Public Key.

SIM Subscriber Identity Module; auswechselbarer Chip im Mobiltelefon zur Identifikation des Telefonbesitzers gegenüber dem Mobiltelefonnetzbetreiber.

SSL Secure Socket Layer; PKC-Protokoll, das im Internet eingesetzt wird, zum Beispiel bei der Übertragung von Zahlungsinformationen zu Onlineshops; vgl. PKC, Protokoll.

Symmetrischer Verschlüsselungsalgorithmus Verschlüsselungsverfahren, bei dem – im Gegensatz zur asymmetrischen Verschlüsselung – mit dem selben Schlüssel ver- und entschlüsselt wird; auf diesen einen geheimen Schlüssel müssen sich Sender und Empfänger vorab über einen sicheren Kanal verständigt ha-

ben; vgl. AES, Asymmetrischer Verschlüsselungsalgorithmus, Cipher, DES, OTP.

TKG Telekommunikationsgesetz; Umfassende gesetzliche Regulierung des Telekommunikationsdienstebereichs in Deutschland, aus der unter anderem die Anforderungen an die Abhörbarkeit der Vermittlungsstellen hervorgehen.

Trustcenter Kommerzielle oder behördliche Einrichtung, die unter Befolgung einer Certification Policy kryptographische Zertifikate ausstellt und verwaltet; vgl. Certification Policy, Zertifikat.

Wassenaar Stadt in den Niederlanden, namensgebend für den Nachfolgevertrag von COCOM, an dem auch alle großen nicht-westlichen Industriestaaten teilnehmen; vgl. COCOM.

Web of Trust Freie, nicht notwendig hierarchische PKI ohne explizite Certification Policy, bei der sich alle Schlüsselbesitzer gegenseitig Zertifikate ausstellen; vgl. Certification Policy, PGP, PKI, Zertifikat.

Zertifikat Im Zusammenhang mit Public-Key-Cryptography: Digitale Signatur, mit der die Zugehörigkeit eines Public Key zu seinem Besitzer bestätigt wird; was genau Gegenstand der Zertifizierung ist, wird spezifiziert durch die Certification Policy; vgl. Certification Policy, Digitale Signatur, PKC, PKI.

Literatur

The Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technologies. ⟨URL: http://www.wassenaar.org/⟩ – Zugriff am 1.5.2003 (zitiert: Wassenaar Arrangement)

Telekommunikationsgesetz. BGBl I 25. Juli 1996 ⟨URL: http://bundesrecht.juris.de/bundesrecht/tkg/⟩ – Zugriff am 3.4.2003 (zitiert: TKG)

Gesetz über Rahmenbedingungen für elektronische Signaturen. BGBl I 16. Mai 2001 ⟨URL: http://bundesrecht.juris.de/bundesrecht/sigg_2001/⟩ – Zugriff am 3.4.2003 (zitiert: SigG)

Telekommunikations-Überwachungsverordnung. BGBl I 28. Januar 2002 ⟨URL: http://www.bmwi.de/Redaktion/Inhalte/Downloads/TKUEV1,property=pdf.pdf⟩ – Zugriff am 3.4.2003 (zitiert: TKÜV)

Adorno, Theodor W.: Negative Dialektik. Frankfurt/Main, 1970 (zitiert: Adorno)

Anderson, Ross J.: Crypto in Europe – Markets, Law and Policy. Juli 1995 ⟨URL: http://www.cl.cam.ac.uk/ftp/users/rja14/queensland.pdf⟩ – Zugriff am 3.4.2003 (zitiert: Anderson)

Back, Adam: Adam Back's home page. 2003 ⟨URL: http://cypherspace.org/~adam/⟩ – Zugriff am 3.4.2003 (zitiert: Back)

Bank, David: The Keys to the Kingdom – the government wants to be able to see private computer communications. San Jose Mercury News 27. Juni 1994 ⟨URL: http://www.interesting-people.org/archives/interesting-people/199406/msg00078.html⟩ – Zugriff am 3.4.2003 (zitiert: Bank)

Barley, Nigel: Du sollst keine anderen Firmen neben mir haben. NZZ Folio. Die Zeitschrift der Neuen Zürcher Zeitung November 2000 ⟨URL: http://www-x.nzz.ch/folio/archiv/2000/11/articles/barley.html⟩ – Zugriff am 1.5.2003 (zitiert: Barley)

Baumgärtel, Tilman: Am Anfang war alle Software frei. Microsoft, Linux und die Rache der Hacker. In **Roesler, Alexander und Stiegler, Bernd (Hrsg.):** Microsoft. Medien, Macht, Monopol. Frankfurt/Main, 2002, S. 103–129 (zitiert: Baumgärtel)

Blaze, Matt: Cryptography Policy and the Information Economy. 1996 ⟨URL: `http://secinf.net/uplarticle/4/policy.txt`⟩ – Zugriff am 1.5.2003 (zitiert: Blaze)

Bradner, S.: The Internet Standards Process – Revision 3, RFC 2026. 1996 ⟨URL: `ftp://ftp.isi.edu/in-notes/rfc2026.txt`⟩ – Zugriff am 1.5.2003 (zitiert: Bradner)

Bulkeley, William M.: Cipher Probe: Popularity Overseas Of Encryption Code Has the U.S. Worried. The Wall Street Journal LXXV 28. April 1994, Nr. 138 ⟨URL: `http://www.interesting-people.org/archives/interesting-people/199405/msg00000.html`⟩ – Zugriff am 3.4.2003 (zitiert: Bulkeley)

Bäumler, Helmut: Neue Wege im Datenschutz. 2000 ⟨URL: `http://www.datenschutzzentrum.de/material/themen/wirtscha/neuewege.htm`⟩ – Zugriff am 1.5.2003 (zitiert: Bäumler)

Chaos Computer Club: CCC klont D2 Kundenkarte. 1998 ⟨URL: `http://www.ccc.de:8080/thema/gsm/`⟩ – Zugriff am 1.5.2003 (zitiert: Chaos Computer Club)

Chaum, David: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24 1981, Nr. 2 ⟨URL: `http://world.std.com/~franl/crypto/chaum-acm-1981.html`⟩ – Zugriff am 3.4.2003 (zitiert: Chaum)

Clarke, Roger: Conventional Public Key Infrastructure: An Artefact Ill-Fitted to the Needs of the Information Society. Canberra, 2000 ⟨URL: `http://www.anu.edu.au/people/Roger.Clarke/II/PKIMisFit.html`⟩ – Zugriff am 1.5.2003 (zitiert: Clarke)

Council of Europe, Treaty Office: Convention on Cybercrime. ETS No. 185. 2001 ⟨URL: http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185⟩ – Zugriff am 1.5.2003 (zitiert: Council of Europe, Treaty Office)

Dam, Kenneth W. und Lin, Herbert S. (Hrsg.): Cryptography's Role in Securing the Information Society. Washington, D.C., 1996 ⟨URL: http://www.nap.edu/books/0309054753/html/⟩ – Zugriff am 1.5.2003 (zitiert: Dam und Lin)

DeLeon, David: The American as Anarchist. Baltimore, 1978 (zitiert: DeLeon)

Diffie, Whitfield: The First Ten Years of Public-Key Cryptography. Proceedings of the IEEE 76 1988, Nr. 5 (zitiert: Diffie)

Diffie, Whitfield und Hellman, Martin E.: New Directions in Cryptography. IEEE Transactions on Information Theory IT-22 1976, Nr. 6, S. 644–654 ⟨URL: http://www.cs.rutgers.edu/~tdnguyen/classes/cs671/presentations/Arvind-NEWDIRS.pdf⟩ – Zugriff am 1.5.2003 (zitiert: Diffie und Hellman)

Engemann, Christoph: Electronic Government – vom User zum Bürger. Zur kritischen Theorie des Internet. Bielefeld, 2003 (zitiert: Engemann)

Europäisches Parlament, Nichtständiger Ausschuss über das Abhörsystem Echelon: Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON). 2001 ⟨URL: http://www.europarl.eu.int/tempcom/echelon/pdf/rapport_echelon_de.pdf⟩ – Zugriff am 1.5.2003 (zitiert: Europäisches Parlament, Nichtständiger Ausschuss über das Abhörsystem Echelon)

Feistel, Horst: Cryptography and Computer Privacy. Scientific American 228 Mai 1973, Nr. 5, S. 15–23 (zitiert: Feistel)

Fox, Dirk: Taube Ohren? Europa ahmt US-Lauschinitiative nach. c't Magazin für Computertechnik 1995, Nr. 12, S. 43 ff. (zitiert: Fox)

Förderverein Informationstechnik und Gesellschaft (FITUG e.V.): FITUG: US-amerikanische Krypto-Kontrollpolitk kein Vorbild für Europa.

München, 1998 ⟨URL: http://www.fitug.de/news/aaron.html⟩ – Zugriff am 1.5.2003 (zitiert: Förderverein Informationstechnik und Gesellschaft (FITUG e.V.))

General Accounting Office: Communications Privacy – Federal Policy and Actions – Report to the Honorable Jack Brooks, Chairman, Committee on the Judiciary, House of Representatives. 1993 ⟨URL: http://www.epic.org/crypto/reports/gao_comm_privacy.html⟩ – Zugriff am 1.5.2003 (zitiert: General Accounting Office)

Gerling, Rainer W. und Kelm, Stefan: PGP, quo vadis? Die Zukunft von PGP, GnuPG und OpenPGP. DuD – Datenschutz und Datensicherheit 2001, Nr. 25 ⟨URL: http://www.lrz-muenchen.de/~rgerling/pdf/dud2001_336.pdf⟩ – Zugriff am 1.5.2003 (zitiert: Gerling und Kelm)

Gilmore, John: Privacy, Technology, and the Open Society. 1991 ⟨URL: http://www.cpsr.org/conferences/cfp91/gilmore.html⟩ – Zugriff am 1.5.2003 (zitiert: Gilmore)

Godwin, Mike: A Brief Analysis of the 'Super DMCA' (the Draft Model Communications Security Act). 2003 ⟨URL: http://www.politechbot.com/docs/godwin.state.dmca.041603.pdf⟩ – Zugriff am 1.5.2003 (zitiert: Godwin)

Goldberg, Ian und Briceno, Marc: GSM Cloning. 1998 ⟨URL: http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html⟩ – Zugriff am 1.5.2003 (zitiert: Goldberg und Briceno)

Graff, Bernd: Der Krypto-Komplex. Warum das Internet und E-mail den Minister Kanther ärgern. Süddeutsche Zeitung 9. Mai 1997, Nr. 105 (zitiert: Graff)

Gröndahl, Boris: Die Entdeckung der Public-Key-Kryptographie. telepolis 1998 ⟨URL: http://www.heise.de/tp/deutsch/special/krypto/1381/1.html⟩ – Zugriff am 1.5.2003 (zitiert: Gröndahl)

Gutmann, Peter: An Open-source Cryptographic Coprocessor. In Proceedings of the 9th USENIX Security Symposium. Denver, Colorado, 2000 ⟨URL: http://www.usenix.org/publications/library/

proceedings/sec2000/full_papers/gutmann/gutmann_html/⟩ – Zugriff am 3.4.2003, S. 97–112 (zitiert: Gutmann: Cryptographic Coprocessor)

Gutmann, Peter: Encryption and Security Tutorial, Part 1. Auckland, 2001 ⟨URL: http://www.cryptoapps.com/~peter/part1.pdf⟩ – Zugriff am 3.4.2003 (zitiert: Gutmann: Encryption Tutorial)

Hafner, Katie und Lyon, Matthew: Die Geschichte des Internet. Heidelberg, 2000 (zitiert: Hafner und Lyon)

Hammill, Chuck: From Crossbows to Cryptography: Thwarting the State via Technology. Culver City, 1987 ⟨URL: http://www.t0.or.at/crypto/crossbow.htm⟩ – Zugriff am 1.5.2003 (zitiert: Hammill)

Heuser, Ansgar: Prävention durch Informationssicherheit. Internetdokumentation Deutscher Präventionstag 2003 ⟨URL: http://www.praeventionstag.de/content/5_praev/doku/heuser/praevention1.pdf⟩ – Zugriff am 1.5.2003 (zitiert: Heuser)

Hughes, Eric: A Cypherpunk's Manifesto. 1993 ⟨URL: http://www.activism.net/cypherpunk/manifesto.html⟩ – Zugriff am 1.5.2003 (zitiert: Hughes)

Jones International and Jones Digital Century: Family Educational Rights and Privacy Act of 1974 (FERPA). 1999 ⟨URL: http://pioneer.nactc.cc.ar.us/cup_additional.htm⟩ – Zugriff am 1.5.2003 (zitiert: Jones International and Jones Digital Century)

Kahn, David: The Codebreakers. The Story of Secret Writing. New York, 1967 (zitiert: Kahn)

Koops, Bert-Jaap: Crypto Law Survey. ⟨URL: http://rechten.kub.nl/koops/cryptolaw/⟩ – Zugriff am 1.5.2003 (zitiert: Koops)

Krempl, Stefan: Kommt die Ausweispflicht fürs Internet? telepolis 2001 ⟨URL: http://www.heise.de/tp/deutsch/inhalt/te/11014/1.html⟩ – Zugriff am 1.5.2003 (zitiert: Krempl)

Köhntopp, Kristian, Köhntopp, Marit und Pfitzmann, Andreas: Sicherheit durch Open Source? Chancen und Grenzen. DuD – Datenschutz und Datensicherheit 2000, Nr. 24, S. 508–513 (zitiert: Köhntopp, Köhntopp und Pfitzmann)

Leuthardt, Beat: Leben online. Von der Chipkarte bis zum Europol-Netz: Der Mensch unter ständigem Verdacht. Reinbek bei Hamburg, 1996 (zitiert: Leuthardt)

Levy, Steven: Crypto Rebels. Wired Mai/Juni 1993, Nr. 1.02 ⟨URL: `http://www.wired.com/wired/archive/1.02/crypto.rebels.html`⟩ – Zugriff am 1.5.2003 (zitiert: Levy: Crypto Rebels)

Levy, Steven: Crypto. how the code rebels beat the government, saving privacy in the digital age. New York, 2001 (zitiert: Levy: Crypto. beat)

May, Timothy C.: The Crypto Anarchist Manifesto. 1992 ⟨URL: `http://www.activism.net/cypherpunk/crypto-anarchy.html`⟩ – Zugriff am 1.5.2003 (zitiert: May: Crypto Anarchist Manifesto)

May, Timothy C.: The Cyphernomicon: Cypherpunks FAQ and More, Version 0.666. 1994 ⟨URL: `http://www.swiss.ai.mit.edu/6805/articles/crypto/cypherpunks/cyphernomicon/CP-FAQ`⟩ – Zugriff am 1.5.2003 (zitiert: May: The Cyphernomicon)

Mayer, Franz C.: Recht und Cyberspace. Neue Juristische Wochenschrift 1996, S. 1782 ff. (zitiert: Mayer)

Menezes, Alfred J., Oorschot, Paul C. van und Vanstone, Scott A.: Handbook of Applied Cryptography. Boca Raton, 1996 ⟨URL: `http://www.cacr.math.uwaterloo.ca/hac/`⟩ – Zugriff am 1.5.2003 (zitiert: Menezes, van Oorschot und Vanstone)

Meyer, Angela: Schweizer Datenschutzbeauftragter übt harte Kritik an den USA. Heise News-Ticker Juli 2003 ⟨URL: `http://www.heise.de/newsticker/data/anm-01.07.03-000/`⟩ – Zugriff am 1.7.2003 (zitiert: Meyer)

Network Associates, Inc.: PGP Corporate Desktop Privacy Products. 2001 ⟨URL: http://www.omicron.ch/new/produkte/DataSheets/PGPsecurity/pgp-corporatedesktop.pdf⟩ – Zugriff am 1.5.2003 (zitiert: Network Associates)

Nielsen//NetRatings: Nielsen//NetRatings finds Strong Global Internet Growth in Monthly Internet Sessions and Time spent Online between April 2001 and April 2002. 2002 ⟨URL: http://www.nielsen-netratings.com/pr/pr_020610_global.pdf⟩ – Zugriff am 1.5.2003 (zitiert: Nielsen//NetRatings)

NIST: Advanced Encryption Standard (AES) Home Page. ⟨URL: http://www.nist.gov/aes⟩ – Zugriff am 1.5.2003 (zitiert: NIST)

Pfitzmann, A., Pfitzmann, B. und Waidner, M.: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2*64 + 16)-kbit/s -Teilnehmeranschluß. Datenschutz und Datensicherung DuD 12 1989, S. 605–622 ⟨URL: http://www.semper.org/sirene/publ/PfPW1_89TelMixeDuD.ps.gz⟩ (zitiert: Pfitzmann, Pfitzmann und Waidner)

Raven, Kai: Deutsche Anleitung zu GnuPG & PGP. ⟨URL: http://kai.iks-jena.de/pgp/⟩ – Zugriff am 1.5.2003 (zitiert: Raven)

Rilling, Rainer: Rüstung und Wissenschaftsfreiheit in den USA (2). Informationsdienst Wissenschaft und Frieden 1984, Nr. 4, S. 15–19 ⟨URL: http://www.rainer-rilling.de/texte/8440600m.htm⟩ – Zugriff am 1.5.2003 (zitiert: Rilling)

Rivest, R., Shamir, A. und Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM 21 Februar 1978, Nr. 2, S. 120–126 ⟨URL: http://theory.lcs.mit.edu/~rivest/rsapaper.ps⟩ – Zugriff am 1.5.2003 (zitiert: Rivest, Shamir und Adleman)

RSA Data Security, Inc.: RSAREF License. Redwood, 5. Januar 1993 ⟨URL: http://bs.mit.edu/pgp/rsalicen.html⟩ – Zugriff am 1.5.2003 (zitiert: RSA Data Security)

Schmeh, Klaus: Kryptografie und Public-Key-Infrastrukturen im Internet. 2. Auflage. Heidelberg, 2001 (zitiert: Schmeh)

Schmidt, Michael: Maskerade. Drahtlose Anonymität mit Bluetooth 1.2. c't Magazin für Computertechnik 12 2003, S. 222–224 (zitiert: Schmidt)

Schneier, Bruce: Applied Cryptography: Protocols, Algorithms, and Source Code in C. New York, 1994 (zitiert: Schneier: Applied Crypto)

Schneier, Bruce: Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2. Auflage. New York, 1996 (zitiert: Schneier: Applied Crypto, 2. Auflage)

Schneier, Bruce: Software Complexity and Security. Crypto-Gram Newsletter März 2000 ⟨URL: `http://www.counterpane.com/crypto-gram-0003.html#SoftwareComplexityandSecurity`⟩ – Zugriff am 1.5.2003 (zitiert: Schneier: Software Complexity and Security)

Schulzki-Haddouti, Christiane: Umrüstung. Kryptographie gilt weiterhin als Waffe. c't Magazin für Computertechnik 1998, Nr. 26, S. 52 ⟨URL: `http://www.heise.de/ct/98/26/052/`⟩ – Zugriff am 1.5.2003 (zitiert: Schulzki-Haddouti)

Schwartz, John: The attack on peer-to-peer software echoes past efforts. The New York Times 22. September 2003, S. 3 (zitiert: Schwartz)

Schöne, Bernd: Schlüssel für den dritten Mann. Die Verschlüsselungs-Software PGP hat ein Sicherheits-Leck. Süddeutsche Zeitung September 2000, Nr. 204 (zitiert: Schöne)

Shearer, Jenny und Gutmann, Peter: Government, Cryptography, and the Right To Privacy. Journal of Universal Computer Science 2 März 1996, Nr. 3, S. 113 ff. ⟨URL: `http://www.jucs.org/jucs_2_3/government_cryptography_and_the/paper.pdf`⟩ – Zugriff am 1.5.2003 (zitiert: Shearer und Gutmann)

'Sicherheit im Internet' (BMWi, BMI und BSI): Gute und schlechte Nachrichten zur eMail-Verschlüsselung. 1999 ⟨URL: `http://www.`

sicherheit-im-internet.de/themes/print.phtml?tdid=38⟩ – Zugriff am 3.4.2003 (zitiert: 'Sicherheit im Internet' (BMWi, BMI und BSI))

Simmons, Gustavus J.: Introduction. In **Simmons, Gustavus J. (Hrsg.):** Secure Communications and Asymmetric Cryptosystems. Boulder, 1982, AAAS Selected Symposia (new series), S. 1–8 (zitiert: Simmons)

Singh, Simon: Geheime Botschaften. München, Wien, deutsch 2000 (zitiert: Singh)

Stephenson, Neal: Cryptonomicon. München, 2001 (zitiert: Stephenson)

Streib, M. Drew: Key Analysis begun 12 Jun 2001. 2001 ⟨URL: http://dtype.org/keyanalyze/200106.php⟩ – Zugriff am 1.5.2003 (zitiert: Streib)

Weber, Arnd: Soziale Alternativen in Zahlungsnetzen. Frankfurt/Main, New York, 1997 (zitiert: Weber)

Weil, Nancy: United States grants PGP encryption export license. InfoWorld.com Dezember 1999 ⟨URL: http://archive.infoworld.com/articles/en/xml/99/12/13/991213enpgp.xml⟩ – Zugriff am 1.5.2003 (zitiert: Weil)

Weizenbaum, Joseph: Die Macht der Computer und die Ohnmacht der Vernunft. Frankfurt/Main, 1978 (zitiert: Weizenbaum)

Wobst, Reinhard: Abenteuer Kryptologie. Methoden, Risiken und Nutzen der Datenverschlüsselung. 3. Auflage. München, 2001 (zitiert: Wobst)

World Wide Web Consortium (W3C): Semantic Web. 2001 ⟨URL: http://www.w3.org/2001/sw/⟩ – Zugriff am 1.5.2003 (zitiert: World Wide Web Consortium (W3C))

Zimmermann, Philip: PGP(tm) User's Guide. Boulder, Colorado, 1994 (zitiert: Zimmermann)