

## Das Netz der Internet-Punks

### Im Reich der Anarchisten

#### Ein Webführer zu den Krypto-Rebellen

Von Thomas Fischermann

Sie nennen sich Cypherpunks, Krypto-Rebellen oder Krypto-Anarchisten und haben den Datenschutz auf die Spitze getrieben. Sie träumen von einem völlig unbelauschten Austausch von Informationen, einem gesetzeslosen Cyberspace. Die Ohnmacht der Steuer- und Polizeibehörden, ja sogar das Ende der Nationalstaaten sollen folgen. Anfang der 90er Jahre begann der Kult mit einem Manifest: Die Gründungserklärung der Cypherpunks schrieb Eric Hughes

( [www.activism.net/cyberpunk/manifesto.html](http://www.activism.net/cyberpunk/manifesto.html) ). Es folgten Grundsatzserklärungen, verfasst von dem Internetmillionär Tim May ( [www.activism.net/cyberpunk/crypto-anarchy.html](http://www.activism.net/cyberpunk/crypto-anarchy.html) und - ein paar Jahre später - von dem ehemaligen Grateful Dead-Sänger John Perry Barlow ( [www.eff.org/~barlow/Declaration-Final.html](http://www.eff.org/~barlow/Declaration-Final.html) ).

Einen guten Überblick über die Szene bietet die Webseite von Vince Cate, einem Hackers und Cypherpunk, der sich nach Anguilla abgesetzt und am Palmenstrand seine Server aufgestellt hat ( <http://online.offshore.com.ai/security/> ). Der technische Hintergrund wird zum Beispiel hier erläutert: [www.ssh.fi/support/cryptography/index.html](http://www.ssh.fi/support/cryptography/index.html).

Über aktuelle Entwicklungen in der Crypto-Szene halten die Homepage von Bruce Schneier ( [www.schneier.com](http://www.schneier.com) ) und sein Newsletter Crypto-Gram ( [www.counterpane.com/crypto-gram.html](http://www.counterpane.com/crypto-gram.html) ) auf dem Laufenden, sowie die etwas exzentrische Cypherpunk-Publikation <http://cryptome.org/>. Wer selber auf die Mailingliste der Cypherpunks aufgenommen werden will, kann sich unter [www.cyberpunks.to](http://www.cyberpunks.to) die notwendigen Informationen besorgen.

#### Spione im Netz

Die meisten Computerbenutzer haben freilich sehr viel praktischere Probleme mit dem Datenschutz - so weit sie überhaupt von ihnen wissen. Bösertige Hacker, Skript-Kiddies, Diebe von Passwörtern und Kreditkartennummern tummeln sich immer zahlreicher im Netz und kommen mit immer neuen technischen Tricks an ihr Ziel. Ein Grund, warum die Hersteller von Sicherheitsprogrammen für Computer zu den Boombranchen der Internetwirtschaft gehört. So genannte Virenschutzprogramme und Firewalls (siehe zum Beispiel [www.zonelabs.com](http://www.zonelabs.com)) finden für 30, 100, gar 300 Euro im Jahr ihre Abnehmer.

Hackerschutzprogramme

( [www.networkice.com](http://www.networkice.com) ) durchforsten die eingehenden Daten nach verdächtigen Inhalten, Anti-Spyware-, Anti-Cookies- und Anti-Trojan-Programme

( <http://security.kolla.de>, <http://tds.diamondcs.com.au> ) durchsuchen Computer nach unerkannter Schnüffelsoftware. Über solche und andere Sicherheitslücken und Lösungen informiert zum Beispiel regelmäßig der Sicherheitsexperte Steve Gibson ( <http://grc.com/default.htm> ). Er bietet sogar einen kostenlosen Sicherheitstest zum Herunterladen an.

Doch sicher vor Spionen, warnen Datenschutzexperten, machen solche Programme das Internet noch lange nicht. Jede Email flitzt wie eine offene Postkarte durchs Netz und kann mit entsprechenden Computerkenntnissen entlang des Weges gelesen werden. Jeder Internet-Provider, manche Polizeibehörde, interessierte Hacker und sogar geschickte Internet-Marketingexperten können wissen, welche Beiträge ein Surfer in Newsgroups gelesen hat, welche Webseiten er bevorzugt, welche Musik oder Filme er auf Internet-Tauschbörsen

handelt. In einigen prominenten Fällen haben Gesetzeshüter solche Informationen bereits angezapft, in anderen auch private Gruppen wie der Verband der amerikanischen Musikindustrie RIAA, der im Augenblick Tausende Raubkopierer in den USA verklagt ( <http://hiphopdirectory.com/directory-org-primary/categories/news/news-749.html> ).

Gegen solche Übergriffe helfen nur die Techniken der Krypto-Rebellen und Cypherpunks. Verschlüsselte Email zum Beispiel ( [www.hushmail.com](http://www.hushmail.com) , [www.mailvault.com](http://www.mailvault.com) , [www.pgp.com](http://www.pgp.com) ). Trickreiche Emailsysteme wie der "Remailer" der Cypherpunks auf Tonga ( [www.cypherpunks.to](http://www.cypherpunks.to) ) oder anderer Betreiber ( [www.stack.nl/~galactus/remailers/index-cpunk.html](http://www.stack.nl/~galactus/remailers/index-cpunk.html) ), die eine Nachricht erst durch mehrere Computer rings um den Erdball jagen und dabei alle Spuren verwischen. Elektronische Tarnkappen wie [www.anonymizer.com](http://www.anonymizer.com) . Technisch versierte Benutzer können ihr Surfen selber über so genannte anonyme Proxys betreiben und dabei ebenfalls alle Spuren verwischen ( <http://webveil.com/matrix.html> ), doch Vorsicht: Das ist Expertensache! Für den Tausch von Musik empfehlen sich inzwischen weit gehend anonyme Tauschbörsen wie [www.blubster.com](http://www.blubster.com) , aber auch das geschieht auf eigene Gefahr. Der Tausch copyright-geschützter Titel ist natürlich auch in diesen Diensten illegal.

All diese Dinge bleiben ein Katz-und-Maus-Spiel. Viele virtuelle Tarnkappentechniken sind noch davon abhängig, dass ihre Betreiber die sensiblen Daten wirklich vernichten oder für sich behalten. Was tun sie, wenn plötzlich die Polizei mit einer einstweiligen Verfügung vor der Tür steht? Ein Remailer in Finnland musste einmal die Identität seiner Kundschaft bekannt geben, bloß weil die Sekte Scientology geklagt hatte ( [www.xs4all.nl/~kspaink/cos/rnewman/anon/penet.html](http://www.xs4all.nl/~kspaink/cos/rnewman/anon/penet.html) ). In einigen Jurisdiktionen wie den USA dürften die Betreiber solcher "Privatsphären-Dienstleistungen" nicht mal ihren Kunden mitteilen, wenn sich eine Behörde für deren Surfgewohnheiten interessiert. Da man für einige Anonymitäts-Dienste mit Kreditkarten bezahlen muss, ist es mit deren Anonymität ohnehin selten weit her. Schließlich ist der Besitzer einer Kreditkarte einfach zu finden. Wirklich anonyme Zahlungsmittel im Internet, ein Traum der Cypherpunk-Szene, stecken noch in ihren Kinderschuhen.

## **Geld aus Staub**

Allerdings: Es wird daran gearbeitet. Als der Erfinder des digital cash - des Cybergeldes, das nur noch aus Datenstaub besteht - gilt der Mathematiker und Computerwissenschaftler David Chaum ( [www.chaum.com](http://www.chaum.com) ). Seit seinen richtungweisenden Veröffentlichungen in den 80er Jahren ist eine Fülle von Konzepten und sogar funktionsfähigen Tauschsystemen entstanden. Mit den ökonomischen Auswirkungen dieser Entwicklungen beschäftigt sich zum Beispiel der kalifornische Ökonom Hal Varian ( [www.sims.berkeley.edu/resources/infoecon/Commerce.html](http://www.sims.berkeley.edu/resources/infoecon/Commerce.html) ). Der Geldexperte Orlin Grabbe stellt auf seiner Homepage [www.aci.net/kalliste](http://www.aci.net/kalliste) (Vorsicht, die Liste enthält exzentrischerweise außerdem pornographische Abbildungen) regelmäßig neue Entwicklungen des Cybergeldes dar und betreibt sogar ein eigenes Tauschsystem. Die International Financial Cryptography Association ( <http://ifca.ai/> ) ist der führende Branchenverband zur Finanzkryptographie und zum elektronischen und stellt eine Fülle von Informationen bereit. Freilich: So richtig erfolgreich war noch keines dieser Systeme.

Mit dem Cybergeld, mit dem persönlichen Datenschutz, mit rechtlichen Fragen rings um die Privatsphäre im Internet und mit dem Aufstieg der "Überwachungsgesellschaft" haben sich inzwischen auch etliche wissenschaftliche Institute und Denkfabriken auseinander gesetzt. Siehe zum Beispiel <http://qsilver.queensu.ca/sociology/Surveillance/intro.htm> oder die Seite <http://cyber.law.harvard.edu/home/> oder <http://cyberlaw.stanford.edu/> , <http://www.temple.edu/lawschool/dpost/writings.html> ; ebenso das Center for Democracy and Technology ( [www.cdt.org](http://www.cdt.org) ), die Electronic Frontier Foundation ( [www.eff.org](http://www.eff.org) ) und die American Civil Liberties Union ( [www.aclu.org](http://www.aclu.org) ). Die EU informiert

unter [http://europa.eu.int/comm/internal\\_market/privacy/index\\_de.htm](http://europa.eu.int/comm/internal_market/privacy/index_de.htm).

Zu den aktuellen Reizthemen der Szene gehört der mangelnde Datenschutz im Flugverkehr, dem die Webseite [www.dontspyon.us](http://www.dontspyon.us) gewidmet ist. Die Montage von Überwachungschips auf Konsumprodukten hat eine andere Gruppierung auf die Barrikaden getrieben: [www.spychips.com](http://www.spychips.com). Und unter dem Druck von Datenschutzgruppen musste die Firma Diebold gerade einen argen Dämpfer einstecken ([www.eff.org/Legal/ISP\\_liability/OPG\\_v\\_Diebold/20031201\\_eff\\_pr.php](http://www.eff.org/Legal/ISP_liability/OPG_v_Diebold/20031201_eff_pr.php)): Sie wollte Hacker verklagen, die Bauanleitungen und Sicherheitslücken ihrer Registriergeräte für US-Wahlen ins Internet gestellt hatten. Sie ist gescheitert.

### Weiterführende Literatur

Weiterführende Informationen über Verschlüsselungs- und Sicherheitsfragen bietet die führende Internet-Sicherheitsmesse RSA, im Internet zu finden unter [www.rsasecurity.com](http://www.rsasecurity.com). Wer noch tiefer in die Welt der Kryptographie und der wirtschaftlichen und sozialen Fragen ringsherum einsteigen will, kann natürlich auch "offline" gehen - und sich ein Buch kaufen.

### Vorschläge:

#### Bruce Schneier: Applied Cryptography

1996 - Umfassende technische Einführung in die moderne Kryptographie

John Wiley & Sons, Januar 1996, 784 Seiten

( [www.schneier.com/book-applied.html](http://www.schneier.com/book-applied.html) )

#### David Kahn: The Code-Breakers

1967 - Klassische, unterhaltsam lesbare Einführung in die Kryptographie  
Scribner Book Company, Revised 1996, 1200 Seiten, ISBN: 0684831309

#### Steven Levy: Crypto

2001 - Die spannende Fortsetzung des Kahn'schen Klassikers  
Penguin Putnam, Januar 2001, 355 Seiten, ISBN: 0670859508

#### Jay Stanley und Barry Steinhardt: Bigger Monster, Weaker Chains

2003 - Zusammenstellung der jüngsten amerikanischen Antiterrorgesetze und ihrer Auswirkungen auf die Privatsphäre

( [www.aclu.org/Privacy/Privacylist.cfm?c=39](http://www.aclu.org/Privacy/Privacylist.cfm?c=39) )

#### David Lyon: Surveillance Society

2001 - Umfassender Überblick über die wachsende "Überwachungsgesellschaft"  
Open University Press, 2001, 192 Seiten, ISBN: 033520547X

(Hinweis auf ein älteres Buch des Autors unter

[www.rochester.edu/College/FS/Publications/Lyon.html](http://www.rochester.edu/College/FS/Publications/Lyon.html) )

#### James Bamford: The Puzzle Palace

1982 - Investigative Reports über die amerikanische Abhör- und Spionageagentur NSA, den Erzfeind der Cypherpunk-Bewegung

Penguin Books, Reprint September 1983, 655 Seiten, ISBN: 0140067485

( [www.randomhouse.com/features/bamford/author.html](http://www.randomhouse.com/features/bamford/author.html) )

#### James Bamford: Body of Secrets

Doubleday Books, April 2001, 736 Seiten, ISBN: 0385499078

#### Neal Stephenson: Cryptonomicon

2003 in deutscher Übersetzung - Amüsant geschriebener Thriller rings um einige Ideen der

Krypto-Rebellen, verfasst vom Cypherpunk-Hofschreiber persönlich  
Englische Ausgabe, Avon Books, November 2002, 1152 Seiten, ISBN: 0060512806  
( [www.cryptonomicon.com](http://www.cryptonomicon.com) )

**Thomas Fischermann: Next Economy**

2003 - Einführung in die "nächste" Internetwirtschaft mit einem ausführlichen Kapitel über das raumlose Wirtschaften, den Datenschutz und die Kriege der Cypherpunks

( [www.berlinverlag.de/Catalogue/details2.asp?section=3&isbn=3833300485&p=1](http://www.berlinverlag.de/Catalogue/details2.asp?section=3&isbn=3833300485&p=1) )

Quelle: ZEIT.de

