

## Cyberspace

### Die Piraten des 21. Jahrhunderts

Im Kampf gegen den Terror bauen Polizei und Geheimdienste den Überwachungsstaat auf. Doch eine Gruppe von Computergenies führt im Internet einen Datenkrieg gegen die Behörden. Bericht aus der Welt der verschlüsselten Botschaften

Von Thomas Fischermann

Die Kunst der Macht ist die Kunst des Verschwindens. (Paul Virilio)

Eben hat der Computer im Büro der ZEIT gemeldet, dass eine E-Mail des Stadtschreibers eingegangen ist. Der Mann ist für diese Geschichte ein begehrter Informant. Einer, der einen Ruf in der Szene der Kryptografen genießt, der Erfinder und Anwender elektronischer Tarn- und Verschlüsselungstechniken. Doch eine E-Mail des Stadtschreibers kann man nicht einfach anklicken und lesen. Mehrere Minuten hat es gedauert, bis der Computer in die „verteilte Stadt“ aufgenommen ist, ein Untergrundnetzwerk, das tief unter der Oberfläche des Internet versteckt und nur mit den richtigen Codewörtern zu betreten ist.

Die „verteilte Stadt“ sieht auf den ersten Blick nicht anders aus als viele Web-Seiten im Internet. Man kann dort E-Mails versenden, Nachrichten an Schwarze Bretter heften und Chaträume besuchen. Doch anders als im gewöhnlichen Internet können sich Surfer hier auf ihre Anonymität verlassen. Niemand wird ihre Nachrichten abfangen. Eine Reihe von Techniken, die vor einem Vierteljahrhundert höchstens Geheimdiensten zugänglich waren, verschlüsseln elektronische Botschaften bis zur Unkenntlichkeit, lassen sie als vermeintlich sinnlosen Datenstaub um den Globus flitzen, verwischen auf der langen Reise alle Spuren. „aANQR1DBw04D/NSEz31ql+8QEADwytY“, beginnt die Nachricht des Stadtschreibers, das ist „Cyphertext“. Eine mathematisch verschlüsselte Botschaft, die nur ihr vorgesehener Empfänger lesen kann. Ein paar Mausklicks, ein Passwort, und endlich erscheint etwas Lesbares auf dem Bildschirm. „Thomas, lassen Sie mich über die Fragen nachdenken. Ich melde mich morgen wieder.“

Willkommen in der geheimnisvollen Welt der Cypherpunks! Es war im Mai 1992, als Eric Hughes bei seinem Freund Tim May im kalifornischen Santa Cruz auf einen Besuch vorbeischaute – und sich dann irgendwie drei Tage lang festquatschte. Hughes war damals Ende 20 und ein begnadeter Mathematiker von der Universität Berkeley; May war zehn Jahre älter, ein ehemaliger Physiker bei der Chipfirma Intel und ein paar Jahre zuvor mit einem gewaltigen Aktienpaket unterm Arm in „Frührente“ gegangen. Man konnte es schnell merken, dass die beiden Wissenschaftler sich gut verstanden: Sie teilten einen ähnlichen Geschmack für Westernkluft und coole Sonnenbrillen, eine Faszination für Computertechnik und mehr als ein gesundes Maß an Verfolgungswahn. Vor allem teilten sie gemeinsame politische Überzeugungen.

Beide zählten sich zum Umfeld der libertarians, den Anhängern einer ultraliberalen Ideologie, die in der weißen amerikanischen Mittelschicht recht verbreitet ist. Libertäre Amerikaner stehen dem Staat in all seinen Erscheinungsformen besonders skeptisch gegenüber, von der Polizei bis zum Steuereintreiber; nicht wenige von ihnen würden Staaten samt ihren Steuern und Organen am liebsten ganz abschaffen und das Regiment den freien Märkten überlassen. Um solch markiges Gedankengut ging es auch beim Gesprächsmarathon der beiden Freunde in jenem Mai. Es wäre kaum der Rede wert, wenn das Duo nicht auch davon überzeugt gewesen wäre, selber den Schlüssel zu seinen politischen Traumvorstellungen in der Hand zu halten.

Noch im Herbst 1992 bildeten May und Hughes einen losen Zusammenschluss von

Gleichgesinnten, der zu einer der ungewöhnlichsten – und obskursten – politischen Bewegungen aller Zeiten werden sollte. Sie nannten sich die Cypherpunks, frei nach einer Science-Fiction-Stilrichtung, die Ende des 19. Jahrhunderts in Mode gekommen war. Sie waren ein Sammelsurium aus hoch dekorierten Wissenschaftlern und Träumern, Computergenies und politischen Aktivisten, Rechtsanwälten und auch Verbrechern. Rebellen im Cyberspace wollten sie sein, Weltveränderer in Turnschuhen und T-Shirts, die ihre Laptops als Waffen begriffen. Sie würden zu unregelmäßigen „physischen Treffen“ zusammenkommen, ihre Cypherpunk-Mailingliste würde zu einem der heißesten Internet-Debattenplätze mit fast 2000 Abonnenten aufsteigen; sie wollten die technische Elite sein, die die Infrastruktur für einen utopischen, gesetzlosen Cyberspace schafft. Und ausgerechnet heute, zehn Jahre später und nach den Terroranschlägen vom 11. September, sehen einige von ihnen ihre große Stunde gekommen: als letztes Bollwerk gegen die Überwachungsgesellschaft.

Die Internet-Wirtschaft, wie wir sie heute kennen, steckte zu Beginn der neunziger Jahre noch in ihren Kinderschuhen. Doch in Kreisen der Techniker-Avantgarde, in denen Hughes und May verkehrten, waren Visionen für eine digitale Zukunft schon weit gediehen: An der amerikanischen Westküste debattierte man längst, wie elektronische Post in den kommenden Jahren fast alle Papiersendungen in und zwischen Betrieben ersetzen werde, dass sämtliche Geld- und Aktiengeschäfte von der Bankfiliale in den Cyberspace verlegt würden, dass Produkte wie Musik und Filme und Nachrichten eines Tages bloß noch per Datenleitung ausgeliefert würden. Immer größere Anteile unserer Arbeitsalltage und unserer Freizeit würden sich vor den Bildschirmen abspielen.

Eine Hand voll Bücher und viele Aufsätze erschienen damals zu Themen wie „Das souveräne Individuum“, worunter man jemanden verstand, der sein Leben und seine Geschäfte im Cyberspace organisiert und keinen Staat mehr über sich duldet. Eine Organisation namens Laissez Faire City eröffnete ein vorläufiges Büro in Costa Rica und wollte eine Art virtueller Staatsbürgerschaft anbieten. Politische Begriffe wie Cyber-Anarchie und virtuelle Regionen schafften es damals erstmals in die Seminare politikwissenschaftlicher und juristischer Fakultäten. War es nicht ein Kinderspiel, all diese Daten und Nachrichten und Produkte an staatlichen Lauschern und Kontrolleuren vorbeizuschmuggeln, an Polizisten, Steuereintreibern und Zöllnern? Würde ein solch unregelmäßiger, gesetzloser Cyberspace die verhassten Staaten in die Knie zwingen?

Man mochte über solche Ideologien denken, was man mochte. Tim May erklärte damals ganz offen, dass die Kryptografie auch Mördern und Terroristen, rassistischen Hassrednern und Entführern in die Hände spielen werde; es seien notwendige Übel der neuen Freiheit, sagte er. „Cypherpunks brechen die Gesetze, die ihnen nicht gefallen“, schrieben die Gründer selbstherrlich in einem ihrer Pamphlete. Doch so oder so, technisch galt die Sache damals vielen Experten als machbar – und sogar unausweichlich. Verfahren zur hochgradigen Verschlüsselung von Daten waren in den siebziger und achtziger Jahren den Geheimdiensten entglitten. Machtlos mussten Militärs und Polizei zusehen, wie Programme wie Pretty Good Privacy (PGP) in den neunziger Jahren in aller Welt Verbreitung fanden und kaum noch mit vertretbarem Aufwand zu knacken waren – auch nicht mit den Supercomputern der Geheimdienste selber. „Cypherpunks werden Programme schreiben“, lautete der Schlachtruf, den Eric Hughes der frisch gegründeten Bewegung in einem kleinen Manifest mitgab. Sie würden geheime elektronische Briefkästen anlegen, elektronische Banken gründen und mit elektronischem Geld handeln, ganz praktisch eben ein Netzwerk hochgradig verschlüsselter Kommunikationswege schaffen. „Der Wandel wird nicht politisch kommen“, fügte der Mitgründer Tim May hinzu, „er wird technologisch kommen.“ – „Regierungen der industriellen Welt, Ihr müden Giganten aus Fleisch und Stahl“, hob ein paar Jahre später John Perry Barlow in seiner Unabhängigkeitserklärung des Cyberspace an; der Rancher, frühere Songschreiber der Gruppe Gateful Dead und passionierte Bürgerrechtler war zu einer Ikone der Bewegung aufgestiegen. „Ihr habt keine Souveränität mehr, wo wir uns versammeln.“

Lima, im Mai 2003. Caryn Mladen hatte ihren Trip nach Peru bestens vorbereitet. Doch das Reisegepäck sah für eine kanadische Touristin reichlich ungewöhnlich aus. Laptops. Adapter. Computersoftware. Eine Liste mit den Namen von Bürgerrechtsgruppen, die mit der Polizei oder mit politischen Gegnern in Schwierigkeiten geraten sind. „Peru hat eine Geschichte als besonders wohlorganisierter Überwachungsstaat“, erzählt die 38-jährige Juristin aus Toronto heute über ihre zweieinhalbwöchige Undercover-Reise. „Und obwohl das Land jetzt demokratisch ist, sind viele alte Kräfte noch am Werk. Keiner weiß, ob die alten Überwachungsapparate noch in Gebrauch sind und wer sie bedient.“

Caryn ist eine Computerexpertin mit umfangreichen Kenntnissen in Fragen des Datenschutzes. Sie hat Computerbücher verfasst und eine Zeitungskolumne, ist schon per Anhalter quer durch Afrika gereist, hat während des ersten Golfkrieges einen Syrien-Trip absolviert („Ich fühlte mich dort sicherer als in New York City“) und fernöstliche Massagetechniken studiert. Doch in der jüngsten Zeit, sagt sie, „brauchte ich einfach mal was Neues, eine frische Herausforderung. Und dann, im Dezember 2001, ist es einfach passiert.“ Sie waren fünf Gleichgesinnte, alle vom Datenschutz und von Verschlüsselungstechnologien fasziniert. Drei Rechtsanwälte, ein Arzt und eine Computerspezialistin mit Kontakten in die Cypherpunk-Szene. Die Gruppe gab sich den Namen Privaterra und wollte Entwicklungshilfe der ungewöhnlichen Art leisten. Sie würden Bürgerrechtsgruppen in Entwicklungsländern moderne Instrumente der Verschlüsselungstechnik an die Hand geben – die Waffen der Krypto-Bewegung.

Inzwischen war die Gruppe schon in mehreren Ländern Süd- und Mittelamerikas unterwegs, gleichgesinnte Kollegen in verschiedenen Ländern Afrikas. „Die Bedürfnisse sind oft sehr unterschiedlich“, sagt die Aktivistin, „etliche Gruppen haben so wenig technische Ahnung, die brauchen zuerst einmal Dinge wie ein Virenschutzprogramm.“ Computer, E-Mail und das Internet haben sich längst für Menschenrechtsgruppen in aller Welt zum unentbehrlichen Werkzeug entwickelt – bei der Suche nach politischen Gefangenen, bei der Koordination von Kampagnen. Doch der Nachteil ist, dass auf den Computern dieser Organisationen nun Adressen von Aktivisten lagern, vertrauliche Briefe und anderes Beweismaterial.

Caryn und ihre Freunde haben Dutzenden von Bürgerrechtlern beigebracht, wie man solche Daten verschlüsseln, auf der Festplatte verstecken oder komplett auf einem sicheren Ablageplatz im fernen Cyberspace ablegen kann – für den Fall, dass ein Computer von der Polizei beschlagnahmt wird oder bei einem „Einbruch“ abhanden kommt. Sie zeigten den Bürgerrechtlern, wie man sich vor den Angriffen feindlich gesinnter Hacker schützt, die nicht selten auch für Geheimdienste arbeiten. Sie brachte ihnen bei, wie man seine Mitteilungen verschlüsselt und sich in die geheimen Kommunikationsnetzwerke einklinkt, die Krypto-Aktivisten clever unter der Oberfläche des Internet aufgespannt haben, statt eine gewöhnliche E-Mail zu schicken, die auf ihrem Weg jeder lesen könnte wie eine Postkarte. „Wer sind die Gegner, gegen die wir arbeiten?“, hat Caryn schon häufig gefragt und nicht immer eine Antwort bekommen. Manchmal sind es Regierungen, manchmal loyale Mitglieder früherer Regierungen, die noch im Untergrund weiterarbeiten. Privaterra lässt sich freilich von amnesty international, Human Rights Watch und anderen Menschenrechtsgruppen bei der Auswahl ihrer „Kundschaft“ helfen. Damit die Instrumente nicht in falsche Hände geraten.

Gut zehn Jahre nach den Gründungstreffen der Cypherpunks sind manche ihrer politischen Träumereien der Realität näher gerückt als je zuvor. Verschlüsselung von Daten, die kein neugieriger Staatsbeamter mehr knacken kann, ob in Peru oder beim amerikanischen Schnüffeldienst NSA? Eine Fülle solcher Techniken ist heute für jedermann im Internet erhältlich, und Softwareschmieden mit Namen wie Martus Software oder Hacktivismo haben sogar maßgeschneiderte Programme für politische Aktivisten und Bürgerrechtsgruppen im Internet verfasst. Trotzdem mussten Caryn und ihre reisenden Datenrebelln eine schmerzhaft Erkenntnis machen. Die Technik mag funktionieren, doch die Anwendung ist

das viel größere Problem. „Das sind keine Computerexperten, und wir können keine aus ihnen machen“, sagt Caryn. „Aber zugleich können diese Gruppen sich keinen Fehler leisten – ihre Kommunikation muss zu 100 Prozent abhörsicher werden.“

„Die meisten Leute, mit denen wir arbeiten, haben außergewöhnlich gute Gründe für die Geheimhaltung“, sagt sie. Todesdrohungen, unangemeldete Razzien im Morgengrauen, unerklärte Einbrüche in die Büros von Organisationen. Ein „Kunde“ von Privaterra, „irgendwo in Zentralamerika“, wurde später ermordet aufgefunden. Vor ein paar Wochen erst wurde der vietnamesische Aktivist Pham Hong Son wegen „Spionage“ für 13 Jahre hinter Gitter geschickt, weil er mit internationalen Demokratiegruppen E-Mails ausgetauscht hatte. „Das ist hier kein lustiges Abenteuer, am meisten müssen wir aufpassen, dass wir niemandem schaden“, sagt eine Kollegin von Caryn. Als China vor ein paar Jahren einen Wall um das gesamte chinesische Internet ziehen ließ und Polizisten zur Kontrolle Pekinger Internet-Cafés aufmarschierten, schrieb ein Team von Cypherpunks flugs ein Programm zum Durchbrechen der virtuellen Mauer. Doch nach kurzer Begeisterung zogen sie es wieder zurück, weil die Benutzung des Programms selbst verdächtige Spuren im Internet hinterließ – und erst recht Schwierigkeiten gebracht hätte.

Las Vegas, im August 2003. Einmal im Jahr werden die Wände im Alexis-Park-Kongresszentrum mit schwarzen Tüchern verhängt. Kräftige Ordner bauen sich vor den Türen auf, die Polizei schickt Sonderkräfte, und angeblich sondieren gar internationale Geheimdienste das Terrain. Die bunte Gemeinschaft der Hacker fällt in die Wüste von Nevada ein: zur „DefCon“-Konferenz, dem größten Konvent für alle, die sich mit dem Eindringen in fremde Computersysteme auskennen. Horden von Computerfreaks bevölkern dann die Kongresshallen und die Liegestühle am Pool; teigige, bleiche Gestalten in T-Shirts und riesigen Sandalen, trendige Hipster mit Fantasiefrisuren, viele der Gäste haben noch reichlich Pickel um die Nase. Computerkids.

Der Redner, der im Anzug und T-Shirt auf die Bühne tritt, Ende 30 und mit einem grauen Schlapphut auf dem Kopf, mag hier auf den ersten Blick nicht richtig hinpassen. Auch sein Publikum ist älter und ernster als die Masse der Computerkinder; in der mittleren Reihe haben sich ein paar FBI-Agenten unter das Publikum gemischt und ihre Arme erwartungsvoll verschränkt. Kein Wunder bei dem Vortragstitel: Bestraft die Kollaborateure! heißt das Thema von Bill Scannell. Er ist bei diesen Konferenzen ein Veteran: ein bekennender Cypherpunk, wenn auch einer, der nicht sonderlich viel von Technik versteht. Der Power-Redner und Kettenraucher Scannell hat sich als Sprachrohr für eine Reihe von Kryptografiefirmen einen Namen gemacht – zum Beispiel jene Firma The Bunker, die im Westen Englands einen ganzen Atombunker gekauft hat und ihn seither als besonders sicheren Lagerplatz für Daten anpreist. Heute spielt er die Rolle, in der er sich selbst am besten gefällt: die des selbst ernannten Bürgerrechtlers und Krawallbruders. „Wir müssen verhindern, dass George Bush und sein Justizminister John Ashcroft die Vereinigten Staaten in eine Überwachungsgesellschaft verwandeln“, sagt Scannell. Er redet sich auf der Bühne schnell in Rage und erntet dafür gemischte Reaktionen – trotzigen Applaus, ein paar empörte Zuschauer verlassen den Saal. „Wir müssen denjenigen das Leben zur Hölle machen, die uns die Freiheiten unserer Verfassung wegnehmen wollen!“

Es mag an Bill Scannells persönlicher Geschichte liegen, dass ihm Fragen des Datenschutzes und der Privatsphäre zu Herzen gehen. Scannell hat schon als Spion des amerikanischen Geheimdienstes in Ost-Berlin gearbeitet, dann war er jahrelang als Journalist im ehemaligen Ostblock unterwegs. Und er will noch mitbekommen haben, „wie es in totalitären Ländern zugeht. Ich war immer stolz darauf, wie viele Freiheiten ein Amerikaner in Amerika genießt.“

Als die amerikanische Fluggesellschaft Delta im Februar anbot, ein sehr weit gehendes Passagier-Überwachungssystem der amerikanischen Behörden zu testen, da „brannten bei mir ein paar Lampen durch“, sagt Scannell. Wenige Tage später startete er eine Protest-Web-

Seite mit Boykottaufrufen und persönlichen Angriffen auf den Delta-Chefmanager, tourte durch amerikanische Talkshows, reiste zur Delta-Hauptversammlung, schließlich zog das Unternehmen tatsächlich seinen Plan wieder zurück. Im Augenblick gestaltet er eine ähnliche Web-Seite gegen das Flugbuchungssystem Galileo. „Diese Dinge nützen doch kein bisschen gegen Terrorismus“, sagt Scannell, „sie sind ein Instrument der Strafverfolgungsbehörden für alle möglichen anderen Ziele.“

So oder so reklamiert Scannell es als ein „Grundrecht“, unerkannt durchs Land zu reisen. Seit den Terroranschlägen ist das schwieriger geworden, doch wenn er reichlich Extrazeit beim Check-in hat, legt sich Scannell immer mal wieder mit dem Sicherheitspersonal an; er macht sich einen Spaß daraus, ab und zu ein Bus- oder Bahnticket unter falschen Namen einzukaufen („Joe Cypherpunk“). „Kürzlich habe ich am Flughafen mit meiner Schwester telefoniert, über Politik, und da habe ich ein paar klare Meinungen geäußert“, erzählt er. „Und dann habe ich gemerkt, wie mich alle anstarrten, als sei ich ein Terrorist. Da wurde mir klar, dass wir hier allmählich Angst haben müssen, unsere Meinung zu sagen.“

Die frühen Cypherpunks hielten es für eine Art Naturgesetz, dass das Internet-Zeitalter die Behörden der Nationalstaaten einfach entmachten wird; dass sie sich eines Tages geschlagen geben und zur Ruhe setzen. Doch zwei Jahre nach dem 11. September 2001 kommen die „müden Giganten aus Fleisch und Stahl“ wieder zu Kräften. Schon wenige Wochen nach den Terroranschlägen brachte Bush eine Reihe neuer Gesetzespakete auf den Weg. Er rief sogar ein „Amt für Cyberspace-Sicherheit“ ins Leben. Schnell machten Gerüchte die Runde, dass auch Verschlüsselungstechniken aus Hacker- und Cypherpunk-Schmieden Osama bin Ladens Kamikazepiloten bei der Planung ihrer Anschläge geholfen hätten; dass Leute wie die Cypherpunks gar die Anschläge vom 11. September mitzuverantworten hätten.

Natürlich ist es ein alter Streitpunkt in der Datenschutzdebatte, ob Verschlüsselungstechniken wirklich ein Bürgerrecht sind oder nur eine Hilfestellung für Terroristen, Halunken und Drogenbarone; ob sie ein modernes Äquivalent für einen versiegelten Briefumschlag darstellen oder ein „waffenäquivalentes Produkt“, wie die US-Regierung zeitweise entschied. Gab es eine optimale Balance zwischen Freiheit und Sicherheit? Der harte Kern um Tim May und ebenso Phil Zimmermann, der Erfinder des Verschlüsselungsprogramms PGP, blieben nach dem 11. September dabei: Schutz für Verbrecher und Terroristen ist ein notwendiger Preis. Die Entwicklung könne ohnehin niemand aufhalten. Und gab es nicht auch genug legitime Anwendungen für die neue Technologie? Schutz für „Cypher-Dissidenten“ in China oder Burma – und sogar in Amerika, wo einige Gruppen zum Beispiel die Namen von „Verschwundenen“ in Guantánamo Bay ins Netz zu stellen planen und zu Recht oder Unrecht politische Reperkussionen fürchteten? „Wenn Kryptografie verboten wird, dann haben eben nur die Verbrecher Kryptografie“, erklärte Phil Zimmermann bei Gelegenheit lapidar.

Doch im Sicherheitsfieber nach dem 11. September fanden solche Sprüche kaum Sympathisanten – und viele Gesetzeshüter und Geheimdienste witterten ihre Chance, ein paar Fakten zu schaffen. Schritt für Schritt werden seither die elektronischen Abhörrechte der Polizei und der Geheimdienste ausgebaut, Behörden legen ihre Datenbanken zusammen, dürfen zunehmend auf die Datenbanken privater Unternehmen zugreifen – in Amerika und auch in Europa und anderen Teilen der Welt. „Wenige Leute haben begriffen, dass eine Überwachung wie bei Orwells Big Brother längst nicht mehr auf die Welt der Bücher und Filme beschränkt ist“, sagt Barry Steinhardt, der Datenschutzexperte der Bürgerrechtsgruppe American Civil Liberties Union.

Trotzdem, es war nicht erst der Schock vom 11. September, der das alte Mantra der Cypherpunk-Gründer von der „Unausweichlichkeit“ einer grenzenlosen Privatsphäre begrub. Es war die technische Entwicklung selber. Mit der explosionsartigen Verbreitung der Computertechnik und des Internet in den Industrienationen ging eine ebenso große Explosion von Schnüffelprogrammen in Computern einher, von vernetzten Überwachungskameras auf

Straßen und Flughäfen, biometrischen Erkennungstechniken und einer Fülle weiterer Technologien. Die wachsende Leistungsfähigkeit von Computersystemen spielte offenbar auch den Schnüfflern in die Hände.

Nie konnten Firmen, staatliche Behörden und hartnäckige Internet-Rechercheure so viel über einen Menschen herausfinden – dank des Internet, das nach den Träumen der Cypherpunks einmal die grenzenlose Freiheit bringen sollte. „Sie haben sowieso null Privatsphäre“, meinte vor ein paar Jahren Scott McNealy, der Chef der kalifornischen Computerfirma Sun Microsystems. „Finden Sie sich damit ab.“

New York City, im Oktober 2003. Der Chefkellner hat eine Sekunde lang die Augenbrauen hochgezogen, als Jo, John und Sean in ihren Turnschuhen und ihrer Freizeitkleidung sein feines Fischlokal betreten haben. Die drei jungen Leute um die 30 mit ihrer schlaksigen Westküsten-Attitüde fallen schon ein bisschen auf zwischen den seriösen Geschäftsleuten, die hier sonst zur Mittagszeit verkehren. Wie kann der Kellner auch wissen, dass er drei künftige Staatschefs vor sich hat?

„Ist der Traum von einem anonymen, staatenlosen Cyberspace geplatzt?“, lautet die Frage. Sean lehnt sich zurück, wiederholt den Satz und nimmt sich ein paar Augenblicke zum Nachdenken. Sean ist eindeutig der Mann für die großen Antworten, der Anführer der Gruppe. Ein untersetzter junger Typ mit einem feisten runden Gesicht. „Es ist alles da, einbruchssichere mathematische Verfahren, anonyme E-Mail-Programme, anonymes Surfen, sogar anonyme Tauschbörsen. Eines der großen Probleme ist nur: Kein Mensch benutzt diese Dinge! Vorerst sind sie einer kleinen Elite vorbehalten.“

Wenn Sean Hastings von kleinen Eliten spricht, versteht sich von selbst: Er selber und seine Freunde zählen dazu. Hastings ist ein Cypherpunk. Keines der verschworenen Gründungsmitglieder, doch ein begnadeter junger Computerprogrammierer mit rebellischer Ader, der die Nationalstaaten am liebsten das Fürchten lehren will. „Wobei, schreiben Sie nicht, dass ich ein Cypherpunk bin“, korrigiert er gleich, „ich mag mich nicht in Schubladen stecken lassen. Schreiben Sie, dass ich der Philosophie der Cypherpunks sehr nahe stehe.“

Hastings hat es zum Kultstatus in der Szene gebracht. Ende der neunziger Jahre war ihm ein veralteter Ratgeber mit dem Titel So starten Sie Ihr eigenes Land in die Finger geraten, und ein paar Monate später kaufte er eine Reihe Computerserver und stellte sie an der Ostküste Englands auf einer rostigen Luftabwehrstation aus dem Zweiten Weltkrieg auf. Damit eröffnete er dort das „erste öffentliche Datenparadies der Welt“. Seine Computer, verkündete er damals, kontrolliere niemand.

Die verlassene Militärstation war im Jahr 1967 von dem pensionierten Offizier Paddy Roy Bates „erobert“ und für unabhängig erklärt worden. Bates vertrieb die Royal Navy einmal mit gezielten Schüssen vor den Bug. Seither hält sich Bates für den Kronprinzen von „Sealand“, und Hastings war ein paar Jahre lang sein offizieller Staatsunternehmer. Hastings, seine Frau Jo und eine Hand voll Hacker zur See quetschten sich in fensterlose Kajüten und waren mächtig verschwiegen. Der Kronprinz ließ seine Finger von den Computern, und Hastings verriet niemandem, welche Kunden auf seinen Computern ihre Web-Seiten und Datenbanken anlegten. Schließlich sollte Sealand ja erstmals in der Geschichte die völlige Unantastbarkeit solcher Daten garantieren.

„Wir waren uns damals in vielen Gesprächen einig geworden, dass ein anonymes Cyberspace ein gewisses Maß an physischer Sicherheit benötigt“, erzählt Hastings. Verschlüsselte Botschaften mögen immer schwerer zu knacken sein, elektronische Tarnkappen mögen immer effektiver werden. Doch irgendwo auf der Welt, in irgendeinem Computer, müssen all die geheimen Daten dennoch lagern und ins Internet eingespeist werden. Irgendwo sitzen die Geheimniskrämer der Welt vor ihren Rechnern und wissen, wie sie ihre Daten im Klartext zu

Gesicht bekommen können – verschwiegene Unternehmer aus Kiew, Steuerhinterzieher aus den USA, heimliche Online-Kasinospieler aus Brüssel, Fremdgänger aus Wien, Händler verbotener Nacktbilder aus Würzburg, Lösegeldraper aus Bogotá und Drogenkuriere aus Luzern. Und überall dort können unliebsame Staaten Leitungen kappen, Festplatten beschlagnahmen oder ihre Besitzer zur Herausgabe von Schlüsseln verurteilen. Als vor ein paar Jahren auf der Internet-Sicherheitsmesse RSA ein blasierter Jungprogrammierer all die „ultrasicheren“ Schutzprogramme seines Computers aufzählte, platzte einem anwesenden Vertreter der Polizei der Kragen: „Und was ist, wenn ich deine Tür eintrete und dir eine Knarre an den Kopf halte? Sind deine Daten dann auch noch sicher?“

So richtig sicher, sagt Sean Hastings, hätte auch Sealand die Träume der Cypherpunk-Bewegung nicht gemacht: „Die Sache funktioniert erst richtig, wenn wir Computer überall auf der Welt haben und verschlüsselte Daten in kleinen Häppchen auf all diesen Geräten verteilen.“ Darum plant er schon wieder einen neuen Computer-Stellplatz: eine gewaltige schwimmende Plattform in den internationalen Gewässern vor Gibraltar. „Vielleicht begründen wir da eine ganz neue Lebensform“, träumt er und hat eine Web-Seite über das „Leben zur See“ eingerichtet. Details über die Geschäftspläne sind bisher nicht zu bekommen, aber Ingenieure will Hastings schon angestellt haben, die ersten Finanzierungsquellen seien angezapft, und auch „Waffen zur Selbstverteidigung“ werde die junge Nation an Bord haben. „Wasser-zu-Luft-Raketen“, setzt seine Ehefrau Jo ein und lacht. Ein Scherz? Das ist nicht so ganz klar.

„Ich ziehe da übrigens nicht hin“, fügt Jo noch hinzu, und Sean verzieht den Mund und nickt. Die Sache ist im Hause Hastings offenbar nicht zum ersten Mal kontrovers diskutiert worden. „Sie wird wahrscheinlich zu Besuch kommen“, sagt er. Damals, in den Kajüten von Sealand, mussten die vaterlandslosen Gesellen monatelang mit aufgefangenem Regenwasser duschen, durften aus Sicherheitsgründen nie oben auf dem Deck schlafen, und das ewige Brummen der Diesgeneratoren bereitete schlaflose Nächte. „Sealand hat meinen Bedarf an einem Leben auf merkwürdigen Seekonstruktionen ein für allemal gedeckt“, sagt Jo.

Was machen Krypto-Rebellen, die es nicht auf ferne Inseln oder rostige Plattformen im Ozean verschlagen hat? Über den Cypherpunk-Gründer Tim May erzählen mehrere seiner Kollegen, dass er sich als bärtiger Einsiedler zurückgezogen habe und ein stattliches Waffenarsenal besitze – für Bestätigungen oder Dementis ist May nicht zu gewinnen. Über einen namhaften Krypto-Pionier an der amerikanischen Ostküste wird in der Szene gemunkelt, dass er sich nebenbei bei der Mafia verdungen habe – für die er fälschungssichere, hochgradig verschlüsselte Wettsysteme programmierte. Das Cypherpunk-Gründungsmitglied Jim Bell aus Vancouver wurde 2001 sogar zum ersten offiziellen „Krypto-Kriminellen“ der Szene: Ein Richter urteilte, dass ein wirrer Aufsatz des Meisters mit dem Titel Hinrichtungspolitik einem Aufruf zu Anschlägen gleichkomme. Bell hatte ein verschlüsseltes Wettsystem mit digitaler Währung und garantierter Anonymität konstruiert, und die Teilnehmer konnten auf das Ableben gewisser Steuerbeamter aus dem Großraum Vancouver spekulieren. Wer den Zeitpunkt des Todes am besten vorhersagen konnte, gewann den Jackpot.

„Viele haben heute nicht einmal mehr etwas mit der libertären Ideologie zu tun“, sagt ein Insider der Szene, „der kleinste gemeinsame Nenner scheint manchmal bloß noch zu sein, dass maximaler Datenschutz eine gute Sache ist.“ Etliche Cypherpunks nennen sich nicht einmal mehr Cypherpunks, nicht zuletzt wegen der eigenartigen Selbstdarstellung mancher Gründer. Manche Rebellen kommen inzwischen reichlich bürgerlich daher.

So gibt es inzwischen einige Firmen, die Programme und Systeme für das anonyme Surfen und den anonymen Versand von E-Mail im Netz anbieten – sicher vor dem Schnüffeln von Behörden, des eigenen Arbeitgebers und auch vor der Datensammelwut von Werbefirmen, konstruiert mit den Technologien der Krypto-Rebellen und manchmal von bekennenden Cypherpunks betrieben. Sie tragen Namen wie Zero Knowledge, Hushmail, Anonymizer oder

ZipLip. Eine New Yorker Firma namens iPrivacy wollte zwischenzeitlich sogar den Warenkauf im Internet anonymisieren: Ihre Kunden hätten unerkant irgendwo im Internet einkaufen können, und iPrivacy wickelte die Transaktion samt Warenlieferung anonym ab. Nicht einmal die ausliefernden Firmen hätten die Identität des Käufers erfahren. Doch iPrivacy ist inzwischen bankrott, etliche solcher Firmen stecken in wirtschaftlichen Schwierigkeiten, und die Nachfrage nach ihren Produkten ist bislang flau geblieben.

Eine Reihe von Aktivisten aus dem Umfeld der Cypherpunks hat sich daher in den vergangenen Jahren vom Programmieren aufs offene Debattieren verlegt. Viele Cypherpunks, sagt ein Gründungsmitglied, „sind geradezu zu Missionaren geworden, verstehen sich als Aufklärer“. Inzwischen gibt es eine Fülle akademischer Projekte wie die OpenNet-Initiative der Universitäten Harvard, Cambridge und der Universität Toronto: Es stellt laufend einen Überblick über Internet-Zensur in aller Welt zusammen.

Die Electronic Frontier Foundation (EFF), 1990 von einer Hand voll Aktivisten der Verschlüsselungstechnik gegründet, ist heute als politische Denkfabrik eine der lautesten Stimmen zu Datenschutzfragen in den USA. Diese Gruppe beschäftigt auch Anwälte, die regelmäßig Hackern, Datenschützern und Verschlüsselungskünstlern juristische Schützenhilfe geben – und amerikanische Geheimdienste dazu zwingen, Verschlüsselungstechniken herauszurücken oder diese von ihrer Liste der exportgesperrten „Waffen“ zu nehmen.

Für die meisten privaten Nutzer sind die Datenschutzprogramme auf dem Markt bislang einfach noch zu teuer und zu kompliziert zu benutzen. Für das „anonyme Surfen“ bei der Firma Anonymizer aus San Diego zum Beispiel sind ab 30 Dollar im Jahr zu zahlen – mit dem Nachteil, dass die Web-Seiten dann langsamer laden als zuvor, und in vielen Situationen ist eine Reihe von Extraklicks nötig. Und während die einfach benutzbaren Musiktauschprogramme Napster und Kazaa gewaltige Erfolge verzeichneten, setzten sich kompliziertere Cypherpunk-Alternativen wie Mojo Nation nie durch. Ist die Sache der Datenschützer doch eher eine kulturelle als eine technische Aufgabe? „Die meisten Leute akzeptieren das Internet einfach noch so, wie es ist“, sagt resigniert John Perry Barlow, Autor der erwähnten „Unabhängigkeitserklärung im Cyberspace“. „Uns fehlt einfach noch die Killerapplikation“, meint Lee Tien, ein Rechtsexperte bei EFF.

Panama-City, im Oktober 2003. Das Büro von Sandy Sandfort ist in einem weiß gestrichenen Wohnblock untergebracht. Balkon über Balkon. Welcher davon Sandy gehört, lässt sich schon vom Bürgersteig aus erahnen: der mit der gewaltigen Satellitenschüssel vor dem Fenster. Denn Sandy Sandfort ist zum Arbeiten hier im sonnigen Panama City. „Verax, Inc.“ ist auf dem Schild an seiner Tür zu lesen, und drinnen stehen in einem kahlen Raum ein paar Schreibtische, ein Sofa, eine Reihe Computer, ein surrender Ventilator. „Wir sind hier ein Post-Venture-Capital-Business“, sagt der Firmenchef und lacht. Ein Unternehmen, das kein Startkapital bekommen hat außer dem Geld, das Sandy privat aufgetrieben hat. Wenn alles nach Plan läuft, will Sandy Sandfort in seinen spartanischen Büroräumen Geschichte schreiben: In Panama City soll ein neuartiges Bezahlungssystem für Online-Einkäufe entstehen. Eine Art Zentralbank mit einer neuen Art von elektronischem Geld, das superdiskrete, supersichere Zahlungen per Internet erlaubt. Einer der ältesten Träume der Cypherpunk-Gemeinde soll endlich wahr werden – wirtschaftliche Freiheit im Internet.

Sandy Sandfort ist jetzt 57 Jahre alt und hat schon als Rechtsanwalt in Arizona gearbeitet und als Englischlehrer, in Costa Rica war er der Star einer Seifenoper („Ich war der Böse“). Er gehörte auch zu den ersten Mitgliedern der Cypherpunk-Bewegung. In Panama wohnt er seit vergangemem Jahr, und er hatte gute Gründe für den Ortswechsel. Das Zahlungssystem, das er aufbauen will, wäre in seiner amerikanischen Heimat niemals legal zu betreiben.

Neue Zahlungssysteme für das Internet – für Aktivisten der Verschlüsselungstechnik galt das stets als die Königsdisziplin. Web-Seiten um Web-Seiten haben sie mit Konzepten für eine

neue Währungswelt gefüllt, mit dem Internet-Dollar und dem eGold, mit vorbezahlten Internet-Zahlungsmitteln zum Kauf an Kiosken und elaborierten Geldwäschermethoden. Sie sollten endlich Schluss machen mit dem Zugriff der Steuerämter und anderer Behörden. Etliche elegante Schemata für virtuelle Tauschringe und Digital Cash sind längst entwickelt, und viele von ihnen gelten in der Szene als viel eleganter und besser durchdacht als Sandys System namens Neuclear. Nur wirtschaftliche Erfolge wurden nie daraus.

Sandy rechnet sich aus anderen Gründen einen Vorteil aus: Seine Verax Inc. bringt neben dem Zahlungssystem gleich eine eigene „Killerapplikation“ mit. Sandy Sandfort kennt sich nämlich auch bestens in der Szene des Glücksspiels aus – nicht mit traditionellem Roulette oder Canasta in Kasinos, sondern mit Cyber-Gambling im Internet. Einschlägige Glücksspiel-Web-Seiten gehören seit Jahren zu den größten Einnahmequellen der digitalen Wirtschaft, aber sie haben ein Problem: In vielen Ländern sind sie verboten. Manche Strafverfolgungsbehörden, darunter die der USA, durchforsten bereits die Kreditkartenabrechnungen ihrer Staatsbürger nach verdächtigen Transaktionen mit Cyber-Kasinos. Kein Wunder, dass sich viele Glücksspieler in aller Welt nach einer Alternative sehnen.

„Wir wollen hier das neue Zahlungssystem für das Internet werden“, sagt Sandy Sandfort und ruckelt auf seinem wackligen Schreibtischstuhl hin und her, als könne er es plötzlich kaum noch erwarten. „Und zwar eines, bei dem es keine Schwierigkeiten gibt, wenn jemand Glücksspiel-Chips, Waffen oder was auch immer einkaufen will.“ Grob vereinfacht ausgedrückt: Kunden werden eines Tages Geld an Verax überweisen, per Bank, Postanweisung und womöglich sogar bar. Bei Verax bekommen sie dafür ein Guthaben eingeräumt und können fortan in Kasinos wetten. In Panama gibt es gegen diese Methode keine Gesetze. Die wahre Identität eines Spielers behalten Sandfort und seine Kollegen dabei für sich; neue Krypto-Technologien sollen sicherstellen, dass der Spieler anonym bleibt und dass trotzdem keiner pfuschen kann.

Aber was passiert, wenn die amerikanischen Behörden Überweisungen an Verax eines Tages genauso verbieten wie an die Spielkasinos? Sandy lacht. „Allein aus diesem Grund wollen wir möglichst schnell dafür sorgen, dass unser Zahlungsmittel von möglichst vielen Händlern im Internet akzeptiert wird, auch von Hotels, Reisefirmen, vielleicht sogar eines Tages von Amazon.com. Für was genau der Kunde sein Geld ausgegeben hat, das ist in unserem System nicht mehr nachvollziehbar. Er kann dann immer plausibel abstreiten, es fürs Cyber-Glücksspiel verwendet zu haben.“

Wenn das Zahlungssystem erst läuft, will Sandfort es vielleicht auch für andere Anbieter lizenzieren; sein Programmierer Pelle, ein 33-jährige Däne, hat dazu schon allerlei Gedankenexperimente gemacht. „Neuclear funktioniert wie uralte Tauschsysteme“, sagt er, „nur mit High-Tech-Methoden durchgeführt. Sie können mit diesem System theoretisch alle möglichen Währungssysteme aufbauen. Wenn Sie wollen, bauen Sie eine Cyber-Währung auf, die auf Gold als Sicherheit basiert. Oder besser noch auf Opium. Ich würde mich kaputt lachen, wenn das jemand probieren würde.“ Ein Scherz. Und längst arbeitet der Programmierer Pelle schon an einer Version seines Bankprogramms, das gar nicht mehr auf einem einzelnen Computer untergebracht ist – sondern verteilt auf viele, viele Einzelcomputer auf der ganzen Welt. Wenn das erst funktioniert, welche Bankengesetze können dann überhaupt noch zum Einsatz kommen? Entstehen auf diesem Weg bald perfekte digitale Finanzoasen im Cyberspace? Parallele Wirtschaftsräume, mit denen man seine Handels-, Wertpapier- und Glücksspielgeschäfte ein für alle Mal verheimlichen kann?

„Ach, wissen Sie, das ist das Problem mit allen Cypherpunkts“, sagt Sandy Sandfort. „Die haben diese Vision, dass sie völlig in eine parallele Welt verschwinden wollen. Meistens funktioniert die Welt nicht so.“ Sagt es, geht zu seinem Schreibtisch herüber und deutet an die Decke. „Schauen Sie, ich könnte hier mit der besten Sicherheitssoftware der Welt sitzen – und

dann könnte irgendein Spion oder die Polizei eine winzige Kamera in der Lampe eingebaut haben, die alles aufnimmt, was ich tippe. Glauben Sie mir: Wir werden noch viele Fortschritte machen. Aber ganz unsichtbar werden Sie im Cyberspace niemals sein.“

Quelle: ZEIT.de

