

Der Hacker

In den späten 90er Jahren feierte der Begriff des „Hackens“ eine Art Comeback: Sei es als manifesthafte Begründung von Polit-Aktionen oder im Rahmen eines „Information Warfare“ vom computerbestückten Schreibtisch aus, sei es als Terror-Szenario militärnaher Beraterorganisationen oder als Konzeptkunst-Strategie, sei es als Metapher eines real existierenden Dekonstruktivismus oder als Hoffnung eines digitalen Neo-Situationismus, sei es als amtliche Praxis von Geheimdiensten oder nur als globale Liebeserklärung durch einen Virus. Dabei schien es, als hätte der Hacker schon in den späten 80ern nicht nur den Höhepunkt seiner Popularität erreicht, sondern sei auch in eine „ironische“ Phase der Selbstreflexivität eingetreten und habe sich in verschiedenste Gruppen und Lager verloren. *Der* Hacker scheint in der Diversität seiner Aktionen und Zielsetzungen unfaßbar geworden zu sein.

Während er in den achtziger Jahren als genialer, gefährlicher oder rettender Hobbyist, als Schatten einer allorts proklamierten schönen neuen Informationsgesellschaft und als juristisches Gespenst eine zwar kohärente, aber darum nicht unbedingt realistische Gestalt gewann, differenzierten sich innerhalb der Computerszene längst diverse Gruppen mit je eigenen Publikationen, sozialen Codes und Zuständigkeiten aus. Beispielsweise *System Intruders*, die in fremde Rechner(netze) eindringen und *Crasher*, die diese zum Einsturz bringen; *Phreaks*, die Telefonsysteme erforschen; Programmierer von Viren, Trojanern, Worms und Bomben; Piraten und *Cracker*, die Schutzmechanismen entfernen und Software verbreiten; Crypto-Liberalisten, die Verschlüsselungsverfahren knacken und selbst starke Algorithmen schreiben; Anarchisten, die alle Arten von illegaler oder geschützter Information ‘befreien’ (sei es über Bombenbau und Drogenherstellung, über Piratensender und Polizeifrequenzen, über Geldautomaten, Kabel- und Satelliten-TV).¹

Im Gefolge der Anschläge vom 11. September 2001 regten sich allerdings wieder Diskussionen über die Möglichkeiten eines „Information Warfare“ und terroristischer Hacker-Angriffe, die dem Hacker erneut zu einer greifbaren Kontur verhelfen.² In dieser Kontur aber zeigt sich die grundlegende Ambivalenz der Figur zwischen einer subversiven und einer staatstragenden Variante. Schon die Struktur des Internet selbst legt Zeugnis davon ab, mit welchem Aufwand und Erfolg Militärstrategen einst versuchten, sich gegen elektronische Angriffe zu wappnen und Kommunikation zu erhalten. Umgekehrt provozierte dies seit den neunziger Jahren Spekulationen, ob und wie die elektronische - und damit auch die übrige - Infrastruktur potentieller Gegner im Ernstfall lahmzulegen sei. Als Pendant zur Angst vor Hackerangriffen entstand die Idee eines Staatshackertums. Der Hacker tritt dabei sowohl als Gestalt des Angriffs als auch der Abwehr auf, er ist Waffe und Schild, potentieller Feind und geheimstes Instrument der Kriegführung. Schon 1995 hatte beispielsweise die berühmte *RAND Corporation* ein Szenario namens *The Day After* durchgespielt, in dem es iranischen Führern gelungen sein sollte, den indischen Programmierer des Airbus-Flugleitsystems zu bestechen und als Hacker seiner eigenen Software einzusetzen.³ Das Planspiel beschrieb, wie Zivilflugzeuge durch einen polymorphen Virus verseucht und über Chicago zum Absturz gebracht werden könnten. Umgekehrt berichtete die Zeitschrift *Defense Week* 1998, daß die *National Security Agency* und *Defense Information Systems Agency* ein sogenanntes *Defense Information Systems Security Program* betreiben. Darin unternehmen es NSA-Agenten beispiels-

¹ Die maßgeblichen Nachschlagewerke sind *The HACK-FAQ*, Version 2.07 (11.6.1994) und *The on-line hacker Jargon File*, Version 4.3.1, 29. Juni 2001.

² Z.B. *Die Zeit* (Nr. 42 vom 11.11.2001) unter dem Titel „Hacker im Heiligen Krieg“ und bezeichnenderweise im Wirtschaftsteil.

³ Roger C. Molander, Andrew S. Riddile, Peter E. Wilson: *Strategic Information Warfare. A New Face of War*, Santa Monica 1996 (RAND MR-661-OSD).

weise, in NASA-Rechner einzudringen und bis zur Abschlußsteuerung und anderen kritischen Daten vorzudringen. Versuche solcher Hacker im Staatsdienst, nicht nur die Battle-Management-Computer des Pazifik-Kommandos, sondern auch diverse Stromnetze zu beeinträchtigen, wurden bereits erfolgreich durchgeführt. Diese stets kriegerische Einsatzform des Hackers in allen möglichen Varianten des Information Warfare aber steht den Ursprüngen und dem Selbstverständnis der Hacker diametral entgegen.

Die Äußerungen ‚freier‘ und im Selbstverständnis ‚traditioneller‘ Hacker setzen sich drastisch von dem auf Kriegs- und Krisen-Szenarios – auf deren Abwehr wie auf deren Herstellung – fixierten Blick des Hackers im Staatsdienst ab. Bereits 1999 hat sich der deutsche *Chaos Computer Club* zusammen mit einer Koalition internationaler Hackergruppen (*Cult of the Dead Cow*, *2600*, *Loph*, *Phrack* und viele andere) dezidiert gegen den Einsatz der Netze als elektronisches Schlachtfeld ausgesprochen: „Beteiligt euch nicht an kriegerischen Handlungen im sogenannten ‚Cyber-War‘. Haltet die Netze, die für die Kommunikation da sind, am Leben. Sie sind das Nervensystem des menschlichen Fortschritts“, war in einer gemeinsamen Verlautbarung zu lesen. Und als nach den Anschlägen islamistischer Terroristen in der Hackerszene Aufrufe kursierten, Webseiten und andere über das Internet erreichbaren Kommunikationssysteme in islamischen Ländern bzw. bei islamischen Organisationen zu zerstören, appellierte der CCC im Namen der „Informationsfreiheit und eines Menschenrecht auf weltweite ungehinderte Kommunikation“ entschlossen gegen derartige Ambitionen. Der strategische Raum ununterbrochener Kommunikation wird schlicht zum herrschaftsfreien Diskursraum einer globalen ‚bürgerlichen Öffentlichkeit‘ umgewidmet, in dem Kommunikation ebenfalls nie aussetzt. Schon die Notwendigkeit solcher Bekundungen verweist jedoch darauf, daß der Hacker von seiner ganzen Anlage her eine vexierbildhafte Gestalt hat. Natürlich sind es nicht einfach biographische Zufälle, daß Karrieren als Sicherheitsberater in den achtziger Jahren noch auf der Anklagebank in einem Gerichtssaal beginnen konnten. Der Hacker ist – für welchen Gebrauch auch immer – im Besitz einer brisanten Kompetenz. Nirgends offenbaren sich so viele sensible Berührungspunkte zu Terror, Sabotage und kriegerischen Handlungen wie in einer von Digitalrechnern durchwalteten, gesteuerten und kontrollierten Welt und nirgendwo versammeln sich andererseits so viele (und vielleicht letzte) utopische Potentiale wie im Bereich der Computernetze. Die Beispiele reichen von einer fundamentalen Kritik der herrschenden Ökonomie durch die *Open Source*-Bewegung, über das entschlossene Eintreten gegen jede Art von Zensur und den Schutz der Privatsphäre bis hin zu Aufklärungsprojekten für eine computerliterare Gesellschaft und globale Kommunikationsutopien. Um die Gestalt des Hackers als Verkörperung dieses Zwiespalts zu begreifen, muß man sich jedoch seiner Entstehung, seiner Apparate und seiner Geschichte bewußt sein.

*

Ein bedeutsames Datum markiert bis heute das Erscheinen von Steven Levys Buch *Hackers – Heroes of the Computer Revolution* im Jahr 1984.⁴ Levy formulierte vor allem die immer wieder zitierte (und wohl maßgeblich von Richard Stallman soufflierte) Hacker-Ethik aus. Sie lautet sinngemäß: 1. *Hands On Imperative; Access to computers – and anything which might teach you something about the way the world really works – should be unlimited and total.* 2. *All information should be free. (Free might mean without restrictions (freedom of movement = no censorship), without control (freedom of change/evolution = no ownership or authorship, no intellectual property), or without monetary value (no cost).* 3. *Mistrust Authority/Promote Decentralization.* 4. *Hackers should be judged by their hacking, not bogus criteria such as degrees, age, sex, race or position.* 5. *You can create art (truth?) and beauty on a computer;* 6. *Computers can change your life for the better.*

4 Steven Levy, *Hackers. Heroes of the Computer Revolution*, London 1984; in-
zwischen sind u.a. hinzugekommen Paul A. Taylor, *Hackers. Crime in the di-
gital sublime*, London 1999; Pekka Himanen, *Die Hacker-Ethik und der Geist
des Informations-Zeitalters*, München 2001.

Daß der Hacker überhaupt Gegenstand einer solchen Darstellung werden konnte, mag Indiz dafür sein, daß er zu diesem Zeitpunkt schon zu einer historischen und damit aus der Distanz erkennbaren, einigermaßen scharf umrissenen Figur geworden war. Die achtziger Jahre als Jahrzehnt des 'Homecomputers' bildeten den notwendigen Hintergrund für diese Historisierung. Während die Hacker-Ethik forderte, daß Software keine Ware werden solle, zeichnete sich gerade in dieser Zeit erstmals mit ganzer Deutlichkeit ab, daß die Computerbranche alles andere war als eine *final frontier* freier Hacker. Software erschien ganz wortwörtlich produkt- und nicht prozessförmig, und *Apple* führte vor, daß Computer von jedem Laien benutzbar sein können, ohne daß er sie verstehen muss. Als Richard Stallman (ebenfalls 1984) die *Free Software Foundation* und *GNU* ins Leben rief, um die Sourcecodes offen und für jedermann modifizierbar zu halten, war dies schon ein verspäteter Versuch, die Hacker-Ethik zu retten, denn längst hatte sich ein Medienverbund etabliert und ausdifferenziert. Dazu gehörten nicht nur DFÜ-Mailboxen und regionale Computer-Clubs, charmant-dilettantische Messen und Fernsehsendungen zu entlegenen Uhrzeiten, obskure Tauschbörsen und anfangs noch xerokopierte Zeitschriften mit endlosen Listings, Computercamps, Conventions und Bücher mit ROM-Dumps, überquellende Elektronikläden und halbprivate Zubehörbastler, sondern auch Spiele- und Programmhersteller und ihre kaum jüngeren Cracker und Raubkopierer.⁵ Während der Hacker-Traum von einer computerliteraten Generation in einigen schulischen Pascal-Kursen steckenblieb, war das Hacken auf *Sinclair*-, *Commodore*-, *Atari*- oder *Apple*-Rechnern zum juvenilen Volkssport geworden. Schon aufgrund dieser massenhaften Verbreitung und den verschiedensten Kontexten der Computernutzung war ein präziser Begriff des Hackers allenfalls noch retrospektiv möglich: beschränkt auf die universitären Keimzellen der späten fünfziger und sechziger Jahre.

Dort erwies sich der Hacker als eine Figur, die durch eine systemische Schranke der Computertechnologie selbst hervorgebracht wird. Er verdankt sich der technischen Bedingung, daß die Prozesse in digitalen Computern unsichtbar sind und diese Unzugänglichkeit durch eine Hierarchie von Interfaces überwunden werden muß. Denn als die Computer digital wurden, wurden sie auch inkommensurabel. Mit der Umstellung von Messen auf Zählen endete jene Rhetorik der Kinesis, in der die rechnende (Elektro-)Mechanik von Gestängen und Getrieben noch durch bloßes Anschauen verstanden werden konnte. Sie wich diskreten, elektronischen Taktraten, mit denen fortan unwahrnehmbare Signale in übermenschlicher Geschwindigkeit geschaltet wurden. Digitalrechner prozessieren seitdem etwas, das nicht mehr zu sehen ist, und das, was an ihnen zu sehen ist, ist nicht das, was prozessiert wird. Datenverarbeitung und Darstellung sind voneinander entkoppelt und beschreiben eine Grenze der wechselseitigen Kommensurabilität von Mensch und Maschine. Interface heißt fortan all das, was Datenverarbeitung in einer Doppelbewegung zugleich unsichtbar macht und auf andere Weise wieder erscheinen läßt, oder umgekehrt: das, was aus Eingaben Daten macht, und dabei bewirkt, daß die Eingaben nicht mehr die Daten sind. Etwas bleibt also, schon aus systemischen Gründen, immer unsichtbar. Mit dem Digitalrechner entsteht gewissermaßen ein Geheimnis oder ein 'mediales Unbewußtes', etwas, das, da unbeobachtbar, vielleicht 'in Wahrheit' geschieht und daß deshalb an Licht zu ziehen sein könnte, ein Schleier von Oberflächen oder *abstraction layers*, der möglicherweise beiseite gezogen werden könnte. Digitalcomputer eröffnen einen Raum des Verdachts.⁶

Dieser Schranke sind zusätzliche Hürden in Form von Schreib- und Leserechten vorgelagert: Seit nicht mehr nur sogenannte „Techniker“ die Computer benutzten, die sie bestenfalls noch selbst konstruiert hatten, erhalten Benutzer allenfalls Benutzerhandbücher und Techniker eben *Technical Reference Guides*. Benutzer haben das Recht zu Ein- und Ausgaben, die ein

⁵ Die Atmosphäre dieser Zeit beschrieb treffend Matthias Horx, *Chip Generation. Ein Trip durch die Computerszene*, Reinbek 1984.

⁶ Boris Groys, *Unter Verdacht. Eine Phänomenologie der Medien*, München 2000; dazu Claus Pias, „Das Medium ist der Verdacht“, in: *Frankfurter Allgemeine Zeitung* vom 6.3.2000.

bestimmtes Programm erlaubt, Systemverwalter hingegen sind autorisiert, die juristischen Texte der Zugriffsverwaltung zu schreiben, und Programmierer haben Zugriff auf die Sourcecodes selbst. Benutzer haben – kurz und mit Lyotard gesagt – nicht das Recht, sich „metapräskriptiv“ zu äußern.⁷ Sie dürfen Vorschriften (also Programmen) folgen, aber keine schreiben; sie dürfen spielen, aber nicht die Spielregeln verändern; sie dürfen Daten verwalten, aber nicht die Verwaltungsrichtlinien bestimmen. Entscheidend ist damit nicht die absolute, technische Grenze zwischen dem unsichtbaren digitalen und dem sichtbaren analogen Computer, sondern jene programmierten und kontrollierten, bezahlten und geschützten Grenzen, die als Software immer schon regeln, wer Zugriff auf welche Teile des Systems hat, wer also über welche Optionen verfügen darf und was für wen verborgen bleibt. Daraus resultiert die wortwörtliche Doppelgesichtigkeit des Interface: Einerseits ist es unabdingbar, damit digitale Computer überhaupt zugänglich werden, andererseits schafft es zugleich und notwendigerweise immer wieder Unzugänglichkeiten. Die Zusammensetzung des Digitalcomputers aus Hard- und Software selbst ist ein Problem der Organisation von Diskursen und damit ein Machtproblem.

Historisch entstand der Hacker an dieser Grenze von Sichtbar und Unsichtbar, von Programmieren und Benutzen, von limitierten Schreib- und Leserechten und von Vor-Schriften alias Programmen, die das Erscheinen bestimmter Aussagen an Computern erst als „sinnvoll“ ermöglichen und andere als „sinnlos“ ausschließen. Er erschien als Schatten oder Wiedergänger des genügsamen Bildschirmarbeiters, als unzufriedener, neugieriger, ungeduldiger, vor allem aber spielender „Benutzer“, noch bevor es den Benutzer im heutigen Sinne überhaupt gab. Noch 1996 sollte man sich in einer US-amerikanischen Kongreßanhörung zum Thema *Security in Cyberspace* an diese anfängliche Bedeutung erinnern: „A hacker is someone who spends many hours with the computer often successfully operating it by trial and error without first referring to the manual.“⁸ Der Hacker ist kein geschulter Techniker oder Programmierer, sondern jemand, der sich sein Wissen selbst zusammensucht. Er ist respektlos gegenüber den willkürlichen Vorschriften von Programmen, Systemverwaltern oder Nutzungskontexten. Die Autorität, die seine autodidaktischen Basteleien legitimiert, ist die je konkrete Technik selbst, die Materialität von Geräten und ihren Leistungsgrenzen. Denn nur die Leistungsgrenze der Maschine ist eine absolute Grenze – eine Grenze, die nicht zu überschreiten ist ohne die eigene Hardwarebasis zu ruinieren, die aber im gelungenen Hack approximiert werden kann. Allerdings ist der Hacker mehr als nur ein Testfahrer, der die Belastungsgrenzen (s)einer Hardware ermittelt. Er ist in seinem innersten Impuls ein *Spieler*, und seine historische Möglichkeitsbedingung ist der Digitalrechner als universale Spielmaschine.

*

Das Erscheinen des Hackers hatte nicht nur technische, sondern auch institutionelle Gründe, denn mit dem Hacker gewann die neue Form des Computerbenutzers überhaupt erst Gestalt, und von ihm aus bestimmt sich erst, was unter Entwicklern noch heute als „dümmster anzunehmender User“ anzusetzen ist. Ab den fünfziger Jahren gab es (beispielsweise am *Stanford Artificial Intelligence Lab* oder dem *Lincoln Lab* des MIT) erstmals Rechner, die Studierenden zugänglich waren. So wenig sich damit in vielen Fällen der physische Standort der Geräte ändern mußte, so drastisch änderte sich der institutionelle Zusammenhang. Denn während des Zweiten Weltkriegs und kurz danach waren die Betreiber der Rechner fast immer zugleich auch deren Konstrukteure und Programmierer gewesen. Selbst die Radaroperatoren an *SAGE* oder die verkabelnden *ENIAC-girls* des *proper programming* galten als bloße „devices“ oder bessere Sekretärinnen, nicht jedoch als Benutzer. Verbunden mit diesem Kontextwechsel der Geräte war auch ein Generationswechsel, denn die Studenten, die nun unter der Aufsicht

⁷ Jean François Lyotard, *Das postmoderne Wissen. Ein Bericht*, Graz / Wien 1986.

⁸ Dorothy E. Denning, *Concerning Hackers Who Break into Computer Systems* (www.cpsr.org/cpsr/privacy/crime/denning_hackers.html).

strenger Systemadministratoren an die Computer drängten, gehörten nicht mehr jener Kriegsgeneration von Mathematikern, Physikern und Elektrotechnikern an, die den Computer als „Werkzeug“ konstruiert hatten, sondern sie fanden (mehr oder minder) eingerichtete Rechner vor und sollten nur im Verfügbaren deren reglementierter Funktionen schalten und walten dürfen. Gleichwohl war der Begriff des Benutzens – schon angesichts der noch gar nicht vorhandenen Standardapplikationen – weiter gefaßt als heute. Benutzen hieß, sich mit den vorgeschriebenen Diskursbedingungen abzufinden – angefangen von den Öffnungszeiten der Computerräume bis hin zu Regeln wie derjenigen, daß Programme binär oder oktal (also in Zweier- oder Achter-Zahlensystemen) einzugeben seien statt über die entlastenden „Mnemonics“ (kleine Merkhilfen aus Buchstaben) eines Assembler.

Entscheidend für die Möglichkeit solcher Programme war eine Veränderung der Hardware selbst. Der TX-0 etwa, der 1959 das MIT erreichte und dort zur bevorzugten Hacker-Maschine wurde, brach mit der umständlichen Prozedur von papiernen Softwarekonzepten, die auf Lochkarten umcodiert werden und deren Ausgaben anschließend aus solchen wieder entziffert werden mußten. Ausgestattet mit einer Tastatur und einem (Radar-)Bildschirm, wie er sonst nur in avancierten Frühwarnsystemen zu finden war, erlaubte der TX-0 eine Art 'interaktiver' Nutzung: Programme konnten eingegeben und sofort zum Laufen gebracht, konnten gegebenenfalls korrigiert werden und sofort noch einmal laufen. Jörg Pflüger hat aus diesem Grund den Beginn der Interaktivität mit der Tätigkeit des Korrigierens von Programmen, dem Debugging, datiert – den Zeitpunkt, ab dem Computer auf Eingaben mit Fehlermeldungen reagieren, auf die wiederum der Benutzer sofort reagieren kann, damit keine Fehlermeldungen mehr erscheinen. Ganz in diesem Sinne waren es die Hacker Jack Dennis und Thomas Stockham, die, als der TX-0-Rechner das MIT erreichte, zuerst einen Assembler namens *MACRO* (zum Schreiben von Programmen) und einen Debugger namens *FLIT* (zur Fehlersuche in Programmen) schrieben, um damit der umständlichen Programmierung in Zahlenkolonnen ein Ende zu machen. Erst diese selbstgebastelten Produktionswerkzeuge sollten es ermöglichen, ohne größeren Codierungsaufwand kleinere Programme zu schreiben, wie etwa eines zur Umrechnung römischer in arabische Ziffern. Genau diese Art der *ad-hoc*-Programmierung nennt Steven Levy „hacken“.

Es entstand eine Reihe solcher „Hacks“, die aufgrund ihrer Unangemessenheit in bezug auf das, was auf einem so teuren Rechner allgemein als angemessen erschien, alle mit „expensive“ begannen. Da beispielsweise die Hausaufgaben der Analysis-Kurse auf dem Papier oder mit elektromechanischen Kalkulatoren zu lösen waren, schrieb Bob Wagner ein Programm namens *Expensive Calculator*, das aus dem TX-0 einen Taschenrechner im heutigen Sinne machte und fiel durch die entsprechende Prüfung, gerade *weil* er einen Computer benutzt hatte. Mit *Expensive Typewriter* folgte die Emulation eines weiteren Bürogerätes. Daß Rechner, Schreibmaschinen und Spiele als Hacks galten, als geradezu situationistisches *détournement*, zeigt, wie wenig von den Potentialen einer universalen Maschine als sinnvolle Anwendung damals evaluiert und diskursiv begründbar war. Es sind Erfindungen der Programmierertechnik selbst, deren Verwendung noch nicht erfunden war. In diesem Sinne wiesen die Hacker nicht zuletzt darauf hin, daß der Computer eine Maschine ist, die alle anderen symbolischen Maschinen sein kann, aber noch nicht ist. Und der Weg dorthin führte zunächst einmal gar nicht in die Arkana ökonomischer, militärischer oder postalischer Schaltstellen, sondern in den verschlossenen Bereich des Wissens um die Funktionalität und Materialität der Geräte selbst. Hacken war eine Form des Herumspielens. Dieses Herumspielen war allerdings nicht nur „wild pleasure“, wie es bei Levy heißt. Hacken ist kein Spiel des Rausches, sondern ein völlig ökonomisches und erzeugt allenfalls einen Rausch des Funktionierens. Denn auf der Innenseite eines Hacks, dem Programmcode, läuft „es“, wie es besser nicht laufen könnte.

Ein Hack mag zwar im Ergebnis sinnlos erscheinen, ist aber in seinem Entstehen durch eine Strategie der Optimierung und Maximierung gesteuert. Er entspringt dem Spiel aller Computerspiele, dem Programmieren selbst. Das Spiel des Hackers ist einer Kombinatorik mit vielen Kompossiblen verpflichtet und bestimmt sich als diejenige Organisation von Ele-

menten, in der die meisten Möglichkeiten auf kleinsten Raum (kürzester Code) und kleinster Zeit (schnellster Code) implementiert sind. Dies unterschied den „freien“ Hacker auch vom lohnschreibenden Programmierer, der beispielsweise bei *IBM* jahrzehntelang nach Zeilenhonorar bezahlt wurde, was der Eleganz des Codes nicht eben zuträglich war. Den Hacker interessierte, geschwindigkeits- und speicherplatzoptimierten Code zu schreiben, Hochsprachen zu umgehen und alle Hardware-Kapazitäten durch proprietäre oder illegale Verfahren auszureizen, um damit etwas zu erzeugen, das kaum einen anderen Sinn zu machen scheint als den, daß „es läuft“. Im Experiment seines kombinatorischen Spiel sucht (und findet) der Hacker nicht nur das, was Konstrukteure vorgesehen hatten und Handbücher schon wußten, sondern vor allem das, wovon diese nie zu träumen gewagt hätten.

*

Weniger sinnlos als Spiele und Schreibmaschinen war der Hack von Capt'n Crunch, hinter dem sich der *National Semiconductor*-Ingenieur John Draper verbirgt. Draper ist eine der populärsten Figuren des „phreaking“, jener Line des Hackens, die sich mit Telefonnetzen beschäftigt.⁹ Erstmals hatte sich Joe Engressia, ein blinder Hacker, mit dem Verfahren der Tonwahl beschäftigt und diverse Steuerfrequenzen herausgefunden. Auch Draper erinnert sich, daß er die Anregung zum *phreaking* aus einem Kreis musikbegeisterter, blinder Adoleszenten erhalten habe. Diese hatten nicht nur die Wahlfrequenzen richtig erkannt und konnten durch die Intonation kleiner Melodien auf Heimorgeln Telefonnummern wählen. Ihren sensiblen Gehören war auch nicht entgangen, daß kostenlose Schleifen für Telefontechniker über bestimmte Töne geschaltet werden konnten. Draper begann, diese Tonfolgen mit einem selbstgebauten Frequenzgenerator (später als *blue-box* bekannt geworden) durchzutesten. Er stieß dabei nicht nur auf jene legendären 2600Hz, die eine ruhende Verbindung signalisieren und daher Gebührenzähler ausschalten können, sondern auch auf Test- und Servicenummern aller Art, auf kostenlose Konferenzschaltungen und tote Leitungen. Engressia und Draper hatten damit jene Grenze verletzt, die präskriptive und metapräskriptive Aussagen auseinanderhält, oder einfacher: die die verwaltete Rede von Telefongesprächen und die Signale zur Verwaltung dieser Telefongespräche selbst trennt.

Draper war sich – anders als die softwareschreibenden Hacker des *MIT* – wohl bewußt, daß er damit nicht nur eine technische Grenze unterlaufen hatte, die Techniker und Telefonierende trennt, sondern daß er zugleich auch eine juristische und ökonomische Grenze verletzt hatte, die zahlende Telefonkunden und Netzbetreiber erst erzeugt und erhält. Denn nicht der Computer war sein Ziel, sondern ein bereits etabliertes und marktwirtschaftlich funktionierendes Übertragungsnetz. Als Draper in einer Beilage von *Capt'n Crunch*-Frühstücksflocken eine Plastiktrompete fand, deren 2,6kHz-Schall alle nicht vorhandenen Sicherheits-Mauern von *AT&T* zum Einsturz brachte, war ein landesweites Phreaking nicht mehr aufzuhalten. Nachdem es um 1970 bereits zu einem freundschaftlichen Einvernehmen zwischen Servicetechnikern und jenen Phreakern gekommen war, die Netzwerkkarten zeichneten und defekte Leitungen anonym meldeten, wurde Draper im Mai 1972 verhaftet. Die Hacker-Ergebnisse wurden im renommierten *Bell Systems Technical Journal* veröffentlicht und lösten eine studentische Bastelwelle aus, an der sich auch „Berkeley Blue“ und „Oak Toebark“ (besser bekannt als Steve Jobs und Steve Wozniak) beteiligten und nicht zuletzt durch den Verkauf von *blue-boxes* eine andere Bastelei namens *Apple*-Computer finanzierten.

*

Drapers Signalverarbeitung wurde nicht zuletzt problematisch, weil der Status des Hacks ungeklärt blieb: Handelte es sich um einen Angriff auf kapitalistische Zugangsbedingungen im Allgemeinen oder um eine Demo gegen überhöhte Telefongebühren im Besonderen, ging es um die Möglichkeit, selbst billig zu telefonieren, oder darum, alle billig telefonieren zu lassen? Die Hacker-Ethik bezieht sich lediglich auf die Offenlegung aller Information, läßt aber das, was der Einzelne mit dieser Information anfängt, völlig unbestimmt. Schon aus diesem

⁹ *History of Capt'n Crunch*
(www.webcrunchers.com/crunch/Play/history/home.html).

Grund kann der Hacker zwischen gut und böse oszillieren und – wie etliche Biographien zeigen – leicht die Seiten wechseln. Auch Draper betreibt, wie viele andere, inzwischen eine Sicherheitsfirma. Nun sind aber Telefone etwas anderes als Computer. Drapers und Engressias Hacks beziehen sich gerade nicht auf das Telefon, sondern auf die symbolverarbeitenden Maschinen der Vermittlungsstellen. Trotz der originellen und unerwarteten Allianzen, die Objekte wie Heimorgeln, Tonbänder und Spielzeugtrompeten unter Hackerhänden mit Telefonen eingehen, markiert das *Programmieren* den maßgeblichen Aspekt. Entscheidend ist, daß diskrete Steuersignale gesendet werden, die nicht das Telefon verändern, sondern in die Spielregeln des Telefonierens eingreifen.

Boris Gröndahl bemerkte zuletzt, daß es „keine Chemie-Hacker, Atom-Hacker, Gen-Hacker oder Auto-Hacker [gebe]. Selbst die tollsten Heckspoiler, Kotflügel und Rennfahrergurte machen aus einem Autobastler noch keinen Hacker.“¹⁰ Das Hacken kann nur an jenen Systemstellen ansetzen, an denen Programmierungen stattfinden. Und dies war bei den hergebrachten Maschinen nicht möglich. In der Welt der energetischen Maschinen beispielsweise könnte eine Dampfmaschine nur dann zu einem Kühlschranks werden, wenn die Gesetze der Thermodynamik selbst umgekehrt werden könnten. In der Welt der elektromagnetischen Maschinen konnte ein Elektromotor immerhin zu einem Dynamo werden oder auch ein „Distributions- in einen Kommunikationsapparat verwandelt“ werden, wie Brecht es in seiner *Radiotheorie* gefordert hatte.¹¹ Doch diese Umkehrungen bleiben binär oder spiegelsymmetrisch. Aus einem Radioempfänger mag zwar ein Radiosender werden können, aber bestimmt kein Fernseher oder Taschenrechner. Elektrische Schreibmaschinen zugleich als Drucker zu benutzen ist zwar eine wahrhaft Brecht'sche Umwidmung von Empfängern zu Sendern aber noch kein Hack. Den Prozessor und den Arbeitsspeicher eines Laserdruckers aber als ungenutzten zweiten Rechner zu erkennen und ihn für ganz andere Kalkulationen zu benutzen als die Skalierung von Schriften und Grafiken dagegen sehr wohl.¹² In der Welt der Computer gibt es also keine einfachen Umkehroperationen mehr. Wofür ein Computer verwendet ist, bleibt einfach so lange unklar, bis ein bestimmtes Programm in Laufzeit übergeht. Der Hacker ist eine Erfindung des Computers – ein Spieler mit digitalem a priori. Seine Existenz und Tätigkeit sind besonderen Spielmitteln und ihrer Kombinatorik geschuldet. Dies schließt nicht aus, daß diese Spiele Verbindungen mit anderen technischen Objekten wie Telefonen, Heimorgeln, Tonbändern oder Schreibmaschinen eingehen. Das Entscheidende (beispielsweise des Hacks von Capt'n Crunch) sind nicht die benutzten Mittel, sondern der Wechsel auf die steuerungstechnische Ebene. Draper vertauschte den belanglosen Strom von Menschenrede in diskrete und für Schaltzentralen intelligible Signale. Und dabei war es gleichgültig, ob diese Steuerungsinformation von einer Trompete, einem Tonband, einer Heimorgel oder einem geübten Gaumen herrührten.

Der entscheidende Aspekt liegt dabei in der Universalität von Turingmaschinen selbst. Jede symbolische Operation eines Computers ist eine „richtige“ Benutzung, und in diesem Sinne gibt es keine „anderen“ oder „falschen“ Verwendungen, sondern nur unaktualisierte Virtualitäten. Jedes Programm das läuft ist legitim – welche Fragen der Legalität es auch immer eröffnen mag. Es gibt es keine falschen Spiele im wahren, sondern allenfalls Spielabbrüche und Programmabstürze. Jede Verwendung kann erst und nur innerhalb eines Kontextes als Mißbrauch erscheinen, der durch Recht oder Ökonomie begrenzt, durch Normalität codiert oder durch Institutionen tradiert ist. Und jede neue Verwendung erfindet und exploriert zugleich das Gebiet dieser Überschreitungen. Hacken unterläuft die Begriffe von richtiger oder falscher Verwendung, es dekonstruiert gewissermaßen den „Mißbrauch“ selbst, indem es aufzeigt, daß ein Begriff von technischer Funktion, der an eine menschliche Intentionalität von Zwecken gebunden ist, an Computern keinen Sinn macht. Daran ändert auch die Tatsa-

¹⁰ Boris Gröndahl, *Hacker*, Hamburg 2000.

¹¹ Bertolt Brecht, „Der Rundfunk als Kommunikationsapparat“, in: *Gesammelte Schriften*, Bd. 18, Frankfurt a.M. 1967, S. 117-134.

¹² Ein Hinweis von Georg Trogemann, Köln.

che nichts, daß alle Technik gegen ihre Nutzung neutral und nur ein Abkömmling der Technikgeschichte selbst zu sein scheint. Daß fast jede Technologie sich bei ihrem Erscheinen aus heterogenen Praktiken speist und verschiedenste Anwendungsweisen findet, bevor sich dann eine davon zur schlichten Unauffälligkeit und illusorischen Angemessenheit von Normalität verfestigt, ist in der Geschichte der Medien keine neue Einsicht.¹³ Neu am Computer ist jedoch, daß er diese „Unentscheidbarkeit“ in sich selbst, seiner Theorie und dem mathematischen Beweis seiner Möglichkeitsbedingung selbst trägt.

*

Der entscheidende Punkt für die Handlungsmöglichkeiten und Seinsweisen des Hackers liegt darin, daß die Virtualität zu einer unausgemachten Zahl von Spielen im Computer selbst begründet ist. *Einerseits* erzeugt die kombinatorische Logik des Kalküls neues Wissen, das in der mathematischen Theorie keine realweltlichen Bezüge und Folgen haben muß. Neue Sätze (oder Programme) könnten einfach solange geschrieben werden, bis endlich alle geschrieben sind und die Geschichte der Mathematik (oder der Programmierung) beendet ist. Und da sie allesamt nur formallogische Existenz haben, sind keine Risiken und Nebenwirkungen zu befürchten außer Tintenstrichen auf Papier oder flimmernden Buchstaben auf Monitoren. *Andererseits* greift dieses Symbolspiel, kaum daß es die materialisierte Form von Computern angenommen hat, massiv in unsere Existenz ein: von Kriegen und Finanzmärkten bis hinab Waschmaschinen mit Diskettenlaufwerk produzieren Symbolspiele Flugzeugabschüsse und Börsencrashes oder bestenfalls überschwemmte Keller. Dem Kalkül aber ist keine Grenze außer der Widerspruchsfreiheit gesetzt. Für die Existenz des Programms ist nur seine Lauffähigkeit entscheidend und nicht etwa, ob es für uns ein Computerspiel oder eine Textverarbeitung ist, ob es den Verkehr von Geschossen oder Geld lenkt, ob es die elektronischen Fesseln von Freigängern oder die Signaturen von Büchern verwaltet. Computer sind konsequent amoralisch. Von hier aus wird auch einsichtig, warum der Hacker nicht nur weniger klar bestimmbar ist als alle anderen Figuren „politischer Subversion“, sondern warum er mit seinen Maschinen und Kompetenzen auch in unterschiedlichen Kontexten ebensolcher Grenzüberschreitungen gefragt ist und angetroffen werden kann.

Genau hier kommen auch die Grenzen ins Spiel, an die der Hacker stößt, die er überschreitet und zugleich immer wieder neu erfindet und provoziert. Es sind (zumindest anfangs) nicht die territorialen und daher widersprüchlichen von Nationalstaaten, sondern erheblich näherliegende juristische, politische oder moralische Grenzen, die jene Flut möglicher Spiele begrenzen sollen, die auf der rein (techno-)logischen Ebene durch nichts zu halten wäre. Während die Optimierung des Spiels nur an die absolute (Hardware-)Grenze der Geräte stößt, geht es beim spielerischen Hacken selbst um die relativen Grenzen des Sinns, um Benutzerrechte und -freiheiten. Hacken erweitert ununterbrochen das Territorium der Symbolspiele, und zwar bevorzugt an seinen kritischen Rändern. Die Hacker-Ethik kann darum als eine Ethik des Spiels gelesen werden: Jeder darf und soll mitspielen, alle Spieler sind gleich, die Spielregeln und -elemente sollen frei zugänglich sein, das Spiel der anderen soll respektiert und geschützt werden, und das alles soll zu einer besseren Welt führen. Hacker gründen in diesem Sinne einen „ästhetischen Staat“ auf der Basis von Turingmaschinen.

Damit bekommt der Hacker *erstens* einen sozialutopischen Impetus und eine politisch-pädagogische Mission. Es geht darum, der prinzipiellen Freiheit und Eigensinnigkeit der Technik zu einer noch unausgemachten Zahl von Spielen auch eine entsprechende Freiheit ihrer Benutzer gegenüberzustellen, alle diese Spiele spielen zu dürfen. Es geht also um eine Form der Erschließung von vorhandenen, aber noch nicht genutzten Möglichkeiten, die jedoch nur mit hinreichender technischer Kompetenz möglich ist. Das Volk der Computerbenutzer muß gewissermaßen aufgeklärt werden, um seine Geschicke selbst in die Hand nehmen zu können. Die Freiheit er-

¹³ Vgl. z.B. für das Radio Wolfgang Hagen, *Radio Schreiber. Der ‚moderne Spiritismus‘ und die Sprache der Medien*, Weimar 2001, für das Telefon S. Munker, A. Roesler (Hrsg.): *Telefonbuch*, Frankfurt a.M. 2000.

fährt der User dort, wo er spielt, d.h. selbst programmiert, statt nur fremden Programmen zu folgen. Das bedeutet umgekehrt aber nur: Wer nicht mit seinen Geräten spielt, sondern sie zu trivialen Maschinen degradiert, hat folglich einen unzureichenden Begriff seiner Tätigkeit und wird zum Objekt einer Pädagogisierung.

Zweitens entwickelt sich jedoch aus der Frage nach dem Spielraum möglicher Anwendungen die gesamte Paradoxie des Hackers. Denn das Spielen mit der Technik exploriert deren Grenzen, die dabei zugleich immer aufgelöst und woanders wieder fixiert werden. Schon was als Spielergebnis der frühen Hacker in den extraspielerischen Raum abfiel, war – und dies ist gar kein Widerspruch zur „Freiheit“ des Spiels – bezeichnenderweise alles andere als unverwertbar. Es gibt seitdem Musiksoftware und Textverarbeitungen, Kalkulationsprogramme und Computerspiele. Und es gibt Betriebssysteme. Nicht zufällig sind Dennis Ritchie und Ken Thompson noch heute in der *Hacker Hall of Fame* zu finden, weil ihr UNIX schlicht als Spiel seinen Anfang nahm. Mit jedem Hack verschwindet umgekehrt also eine Möglichkeit zu hacken. Auch was noch so abseitig beginnt, kann überraschend schnell zur Standardapplikation werden, die Usern wiederum die Faulheit oder Verblendung erlaubt, nicht (mehr) hacken zu müssen. Der Hacker schleppt also die Grenze, die er zu überwinden scheint, immer mit und zieht sie ununterbrochen neu. Wo immer durch ihn offensichtlich Spiele möglich werden, die vorher nicht da waren, erzeugt er selbst nicht nur einen ökonomischen, juristischen oder moralischen Regelungsbedarf, sondern auch einen hackerfreien Raum.

Die Hacks von Capt'n Crunch und seine Verurteilung zu fünf Jahren Haft waren schon deshalb von anderer Qualität als die Assembler-Virtuositäten am *MIT*, weil sie nicht in einem juristisch wie privatwirtschaftlich weitgehend Bereich, irgendwo an der *final frontier* eines entlegenen universitären Computerraums stattfanden, sondern an einem technisch wie ökonomisch durchorganisierten und umfassenden Medienverbund namens Telefon ansetzten. Das Telefon lernte durch Draper, was das Radio schon wußte: Man konnte zwar vieles, durfte aber längst nicht alles senden. Beispielsweise keine Steuersignale. Paradoxerweise führte dieses neue Wissen sofort zu einem neuen Nicht-Wissen, oder besser: zur Abschaffung dessen, was man wissen könnte. Denn indem Draper den Spielraum des Telefonbenutzers erweiterte, sorgte er zugleich für die Schließung des gerade eröffneten Territoriums; indem er herausfand, was man über Telefonsysteme noch alles wissen kann, half er zugleich, dieses neue Wissen als Eigentum und Herrschaftswissen von Telefongesellschaften zu markieren; indem er unregulierte Optionen aktualisierte, schaffte er zugleich Präzedenzfälle der Illegalität und ermöglichte technische Umstellungen in den Vermittlungszentralen, die die Möglichkeit zur dieser spezifischen Illegalität selbst abschaffen. Der Hacker erscheint damit als janusköpfige, als ebenso subversive wie staatstragende Figur, die zwischen einem Robin Hood des Datenschungels und einem finstern Cyber-Terroristen schwankt, der, je nachdem, Weltherrschaft oder Weltuntergang anstrebt.

Weil der Hacker diese Ambivalenz in sich trägt, kann er sich auch selbst entscheiden, ob er sich als Aufklärer oder Zerstörer betätigt, ob er Utopist oder Zyniker wird, Pädagoge oder Sicherheitsberater. Die utopische Linie wurde vor allem gespeist durch Campus-Unruhen, Friedensbewegung und durch die simple Tatsache, daß um 1970 beiden Seiten – den Regierungsbehörden und Unternehmen einerseits, den Hackern andererseits – augenfällig wurde, welche kulturelle, politische und ökonomische Bedeutung dem Computer in Zukunft zukommen könnte. Die Entwicklung von Netzwerken in den 60er Jahren war nicht nur kriegstechnisch ratsam, sondern offerierte zugleich neue, gewissermaßen unterirdische Kommunikationswege, über die es möglich schien, ganz neue Öffentlichkeiten herzustellen. Die Informationspolitik während

des Vietnamkriegs hatte einmal mehr gelehrt, Autoritäten zu mißtrauen, Zugangsbedingungen nicht zu akzeptieren, Verbote zu umgehen oder, in der Diktion der Ideologiekritik gesagt, dahinter Selbsterhaltungsbestrebungen eines Systems zu vermuten, das auf Profit durch Wissensbeschränkung ausgelegt ist. Durch beide Faktoren bekamen die Hacker-Gebote „Mißtraue Autoritäten“ und „Befördere Dezentralisierung“ enorme Bedeutung.

Nicht der Computer (der seit dieser Zeit gerne als „Medium“ bezeichnet wird) steht also in Frage, sondern nur noch das, was man mit ihm macht. Und diesen Möglichkeitsraum zu ermessen, war und ist Aufgabe der Hacker. Und deren erste Zielgruppe war, schon aus der eigenen, akademischen Computersozialisierung heraus, die nächstfolgende Studentengeneration. Daher konnte ihr Motto erst einmal nur lauten: „Let the student program the computer, not the other way around“. Als politisch galt dabei nicht nur das simple Drucken von Flugblättern auf Universitätsrechnern, sondern schon das spielende Programmieren selbst und darum gleich doppelt das Programmieren von Computerspielen. Dieses vielleicht naive ‘Spielen für den Frieden’ stellte die durchaus erstgemeinte Frage nach einem herrschaftsfreien Raum, in dem es stattfinden kann, oder genauer: nach einem Raum, in dem nicht jeder Hack sofort neue Reglementierungen mit sich bringt. Mit anderen Worten: Es stellt die entscheidende Frage, ob die tragische Situation des Hackers zwischen Grenzüberschreiter und Grenzzieher irgendwo oder irgendwann zu entparadoxieren wäre. Wie bei allen modernen Utopien liegt auch hier die Antwort nicht an einem fernen Ort, sondern in einer fernen Zeit. Und der Sendbote dieser neuen Zeit, das Referenzobjekt der Personal-Computing-Bewegung ist – fast zwangsläufig – das Kind. Siebzig Jahre nachdem eine lebensreformbewegte Ellen Key das „Jahrhundert des Kindes“ ausgerufen hatte, echote Alan Kay schlicht mit der nächsten Generation von „power users“. Das Kind erscheint als Metonymie des Hackers, weil es die Stärke der Respektlosigkeit gegenüber tradierten Rechts- und Nutzungszusammenhängen besitzt, weil es keine Angst vor Computern hat und weil es hohe, unerwartete und allzu ‘menschliche’ Ansprüche stellt. Das Kind ist – wie der Hacker – ein unbekümmerter Autodidakt, der die Dinge spielerisch erforscht und in dessen Spiel die Elemente ihrer Kontexte entbunden werden, um überraschende Vereinigungen einzugehen.¹⁴

Der Hacker der vorangegangenen Generation wird daher aber zum Spielzeugmacher und Pädagogen der folgenden, der die Sprachen und Geräte bereitstellt, mit und in denen dieses Spiel stattfinden soll. Das „gebunden-freie“ Experimentieren der Reformpädagogik scheint in Kays „new programming paradigm“ namens *Smalltalk* wiederzukehren, und Maria Montessoris Selbstunterricht am abstrakten Formengut feiert bei Samuel Paperts *Logo* seine Wiederkehr unter Computerbedingungen.¹⁵ Fragmente dieser Bewegung sind noch heute sichtbar, wenn gestandene Hacker sich in „Schulen ans Netz“-Kampagnen engagieren statt die Telekom zu schröpfen oder EC-Karten zu decodieren. Die Hacker dieser mittleren Periode öffneten also vor allem die Medienfunktionen des Computers. Sie scheuten – mit den Worten Enzensbergers – nicht die „Schmutzigkeit“ elektronischer Medien, sondern versuchten genau darin ihre „Produktivkraft“ zu erkennen.¹⁶ Das Paradox dieser Phase bestand jedoch darin, daß der

¹⁴ Alan Kay / Adele Goldberg, „Personal Dynamic Media“, in: *Computer*, March 1977.

¹⁵ Benedict Dugan, *Simula and Smalltalk. A Social and Political History* (www.cs.washington.edu/homes/brd/history.html).

¹⁶ Hans Magnus Enzensberger, „Baukasten zu einer Theorie der Medien“, in: *Palaver. Politische Überlegungen (1967-1973)*, Frankfurt a.M. 19xx, S. 91-128.

Hacker zu diesem Zweck mit einem pädagogischen Programm auftrat, das seine Selbstaflösung implizierte. Er suchte gewissermaßen die diskursive Grundausstattung einer Computerkultur zu liefern, um anschließend in dieser zu verschwinden.

*

Wegen und gegen diese(r) hochfliegenden Hoffnungen brachten die achtziger Jahre eine junge, homecomputersozialisierte Generation von Hackern hervor wie beispielsweise den 19-Jährigen Ronald Austin, der sich 1983 ins Pentagon hackte, die 414GANG, die seit 1982 nicht nur in die Militärbasis von Los Alamos, sondern auch in 60 andere Institutionen eindrang und danach vom FBI ausgehoben wurde oder auch Kevin Mitnick (alias Condor), der schon mit 17 erstmals inhaftiert wurde.¹⁷ Legendärerweise hatte Mitnick das Verteidigungssystem NORAD gehackt und damit den 1983 entstandenen Film *War Games* inspiriert, der bis zu einer Kongreßanhörung führte. Das Novum dieser Überschreitungen bestand in ihrer Distanz, darin, daß sie eben nicht mehr ortsgebunden waren, sondern gerade und dringlich erst die Frage des Ortes stellten und eine Klärung derselben im rechtlichen und ökonomischen Sinne provozierten. Neu an der Existenz privat zugänglicher DFÜ-Netzwerke (längst vor dem heutigen Internet) war, daß es nicht mehr nur um die Grenzen und Möglichkeiten des nur eine Armlänge entfernten, eigenen Rechners ging. Überschreitungen spielten sich nunmehr an geographisch fernen, systemisch unsichtbaren oder sonstwie schwer zu ermittelnden und unbefestigten Grenzen ab. Sie betrafen Grenzen, die nicht mehr in nationalstaatlichen Kategorien zu fassen waren, diese in vieler Hinsicht unterliefen, jedenfalls aber nicht neutral zu ihnen waren. Die Heimeligkeit des seitdem oft beschworenen „globalen Dorfes“ mußte zwangsläufig mit den territorial gebundenen Gesetzen in Konflikt geraten. Noch heute, trotz zahlloser Regelungen, sind diese Fragen derart ungeklärt, daß eine permanente Migration politisch mißliebiger, ökonomisch zwielfichtiger oder sonstwie indizierter Inhalte von Server zu Server, von Land zu Land, stattfindet und die Gesetzgebungen ihrer Staubwolke folgt. Dabei gilt es jedoch genau zu unterscheiden, was von solchen Aktionen den Hacker überhaupt berührt. Bloßes Umkopieren – seien es nun Absurditäten von Holocaust-Gegnern, Anleitungen zum Bombenbau oder inkriminierte politische, religiöse und pornographische Inhalte aller Art – ist noch keine Hackertat, sondern befindet sich allenfalls im Einklang mit der Hacker-Ideologie einer radikal-liberalen Öffentlichkeitspolitik. Das gleiche gilt für die Praktiken zivilen Ungehorsams wie virtuelle Sit-ins, massenhaft an eine Adresse verschickte mails und ähnliche Protestformen.¹⁸ Sie bedürfen keiner Computerkenntnis oder technischen Virtuosität, sondern sind nur ins Netz kopierte und mit einem Knopfdruck abrufbare Abbilder traditioneller Demos und Protestbriefe. Interessant für Hacker wird es erst, wenn Umleitungen aus Kriegs- oder Krisengebieten zu schalten sind, um gegen die Störungsversuche eines Aggressors die Kommunikation aufrecht zu erhalten, wenn Server mit politisch zensierten Inhalten frei- oder Server mit mißliebigen Inhalten sabotiert werden sollen, wenn es gilt, die Unsicherheit von Verschlüsselungsverfahren bloßzustellen oder die Mustererkennung einer Rasterfahndung in die Ratlosigkeit zu treiben. Erst und nur unter solchen Bedingungen führt sogenannter „Hacktivism“ ins eigenste Gebiet des Hackers, gleichwohl er auch technisch banale Taten politisch oder moralisch unterstützen mag. Und erst in diesem Moment verbindet sich wieder die Virtuosität eines technischen Grenzgangs mit juristischen, ökonomischen und politischen Grenzgängen.

¹⁷ Geschichten wie diese geben natürlich Stoff für Romane, z.B.: Clifford Stoll, *Kuckucksei. Die Jagd auf die deutschen Hacker, die das Pentagon knackten*, Frankfurt a.M. 1989 oder Tsutomu Shimomura, *Data Zone. Die Hackerjagd im Internet*, München 1996.

¹⁸ Stefan Wray, *Electronic Civil Disobedience and the World Wide Web of Hacktivism. A Mapping of Extraparliamentarian Direct Action Net Politics* (www.nyu.edu/projects/wray/wwwhack.html); Aspects of Hacker Culture (www.du.edu/~mbrittai/4200/socio_criminal.htm).

Historisch zeigte sich schon an den jungen Hackern der 80er Jahre, daß man mit DFÜ und Computer noch ganz andere Dinge machen konnte als die Unbekümmertheit der vorangegangenen Generation sich träumen ließ – Dinge, die weder durch Sicherheitstechniker zu unterbinden, noch durch gutmenschlichen Common-Sense auszuschließen oder durch kommunikative Vernunft wegzuziehen waren. Erst in diesem Moment der Entwicklung war es notwendig, eine bislang selbstverständliche Hacker-Ethik auszuformulieren. Der Hacker mußte eine Grenze ziehen, die durch ihn selbst hindurchgeht, indem er einen „bösen“ Teil abspaltet. Dabei distanziert sich der gute (und vermeintlich auch ‘traditionelle’) Hacker durch seinen Ehrencodex von dem *hacker for profit*, den Banalitäten von *script-kids* ohne nennenswerte Programmierkenntnisse und den Destruktionen der *crasher*, die den gleichen Technologien entspringen. Der gute Hacker war fortan Sozialutopist mit medientechnischem Apriori. Sein Ziel sollte es sein, „gegen die Angst- und Verdummungspolitik in bezug auf Computer sowie die Zensurmaßnahmen von internationalen Konzernen, Postmonopolen und Regierungen anzustinken“, wie Wau Holland in der ersten *Datenschleuder*, dem Organ des ausge-rechnet im Orwell-Jahr 1984 gegründeten *ChaosComputerClub* schrieb. Nach der Terrorismus-Paranoia und Herolds massivem Computereinsatz in der Rasterfahndung, nach Volkszählung, Magnetkarten und *BTX* bezog der Hacker speziell in Deutschland seine moralische Legitimation aus der Freiheit der öffentlichen und der Sicherheit der privaten Information: „Private Daten schützen, öffentliche Daten nützen“, lautete daher der Ergänzungsparagraph der Hacker-Ethik.

Daß im Feld der technologischen Gleichmöglichkeit nun eine explizite Leitdifferenz von gut und böse verlegt wurde, half jedoch nicht unbedingt, die Lage des Hackers zu entparadoxieren. Nicht nur wird jede Sicherheits- oder Gesetzeslücke, die der „gute“ Hacker öffnet, bald geschlossen sein – vielmehr bestimmt es der Hacker jetzt als seine eigenste Aufgabe, auf solche Lücken zum Zwecke ihrer Schließung erst hinzuweisen. Er wird zum Helfer desjenigen Wissensregimes als dessen radikalliberaler Herausforderer er sich zugleich versteht. Und zusätzlich muß er dabei noch mit seinem eigenen Spiegelbild fechten, nämlich gegen jene anderen Hacker antreten, die sich nicht an die Grenzen einer vereinbarten Ethik, einer aufklärerischen Gewissenhaftigkeit oder freiwilligen Selbstkontrolle halten, sondern weiter amoralisch alles das auch tun, was mit und an nunmehr vernetzten Universalmaschinen getan werden kann.

Im Hacker selbst herrscht damit eine Form von Krieg, die zum Motor eines ganz realen Krieges ausgebaut werden kann. Ein Memorandum des U.S. Generalstabs vom 17. Juli 1990 konstatiert: „C2W [Command and Control Warfare] is the military strategy that implements Information Warfare. Within C2W ..., there are five principal military actions in support: Operations Security (OPSEC), military deception, psychological operations (PSYOPS), electronic warfare (EW), and physical destruction.“¹⁹ Rekruten für diese Tätigkeit dürfte es genug geben, denn das Internet beschleunigte und globalisierte ab 1993 die Zirkulation des Hacker-

¹⁹ *Security in Cyberspace*, U.S. Senate, Permanent Subcommittee on Investigations, Congressional Hearing 5.6.1996; Lon M. Yearly, *Hackerwar and Its Influence on the Marine Expeditionary Force Commander*, Executive Summary, 6.5.1996; vgl. Dorothy E. Denning, *Activism, Hactivism, and Cyberterrorism. The Internet as a Tool for Influencing Foreign Policy* (www.nautilus.org/info-policy/workshop/papers/denning.html). Zur Diskussion des „Infowar“, die hier zu weit führen würde vgl. James Adams, *The Next World War. Computers are the weapons and the Front Line is everywhere*, London 1998; David S. Alberts, Jahn J. Garstka, Frederick P. Stein, *Network Centric Warfare. Developing and Leveraging Information Superiority*, Washington 1999; Gerfried Stocker, Christine Schöpf (Hrsg.), *Information. Macht. Krieg*, Wien / New York 1998 (ars electronica 98); Stefan Kaufmann, „Vom industrialisierten zum informatisierten Schlachtfeld: Der Körper in der ‚Materialschlacht‘ und im ‚Information Warfare‘“, in: *Ästhetik und Kommunikation* xx(2001), S. xx-xx.

wissens.²⁰ Die weltweiten Liebesgrüße von *script-kids*, die schon wegen ihrer Programmierkenntnisse von gestandenen Hackern nur verachtet werden können,²¹ sind inzwischen notorisch geworden. Downloadbare *Virus construction kits*, die allen Hacker-Geboten des Repertoires zum Trotz an jeden mißliebigen Nachbarn oder Kollegen gemailt werden können, unterlaufen auch noch die ausgefeiltesten Virens Scanner. *Warez*, *crackz* und *serialz* sind über jede Suchmaschine zu Tausenden zu finden, während 'anständige' Hacker sich seit fast zwanzig Jahren darum bemühen, endlich freier Software die gebührende Anerkennung und Seriosität zu verschaffen. So nimmt es nicht wunder, daß Hacker in den 90ern in nahezu alle Server eindringen, darunter die des US-Justizministeriums, der *Air Force*, der *CIA* oder der *NASA*. Allein das *General Accounting Office* des U.S. Verteidigungsministeriums registrierte 1995 250.000 Attacken, und die Gruppe *Loph* drohte zwischenzeitlich mit einem landesweiten Internet-Shutdown binnen 30 Minuten.²² Das Internet lehrte, daß amerikanische Banken auch von St. Petersburg aus betrogen werden können, daß man auch von Israel aus mit Administratorrechten auf amerikanische Militärserver zugreifen kann oder daß ein selbsternannter Robin Hood schon einmal 20.000 Kreditkartennummern unter Volk bringen kann.

Die Szenarien der militärischen und politischen Beraterinstitutionen haben daraufhin bekanntlich ihre Szenarien von nuklearen Erst- und Zweitschlägen umgestellt auf die Simulation eines „Cyberterrorismus“ abstürzender Airbusse, zusammenbrechender Strom-, Wasser-, Telefon- und Datennetze oder immaterieller Handelskriege, bei dem die Grenzen der Front nicht mehr auszumachen und die Parteien an ihren Computern nicht mehr aufzufinden sind. Da aber schon in den klassischen Kriegsspielen, ebenso wie in den Szenarien des Kalten Krieges, der Feind stets die Gestalt der eigenen Frage war, kann dies nichts anderes bedeuten, als selbst zum Hacker zu werden. Daß sich dementsprechend Regierungsbehörden gegenseitig selbst hacken und Hacker zu Beamten werden, ist vielleicht nur das notwendige Gegenstück dazu, daß Hacken andererseits als Kunst inszeniert und der Hacker als neue Leitfigur des Intellektuellen apostrophiert wird.

²⁰ Steven Mizrach, *Is there a Hacker Ethic for 90s Hackers?* (www.attrition.org/~modify/texts/ethics/is.there.a.hacker.ethic.for.90s.hackers.html).

²¹ Libby Copeland, „Script Kiddies Ruin Our Image – Hackers“, in: *Washington Post* vom 18.2.2000.

²² Debora Halbert, „Discourses of Danger and the Computer Hacker“, in: *The Information Society* 13(1997), S. 361-374.