Alexander R. Galloway / RSG

Unser eigener „Carnivore“

Ungehorsam gegen Autorität ist eine der natürlichsten und befreiendsten Handlungen.

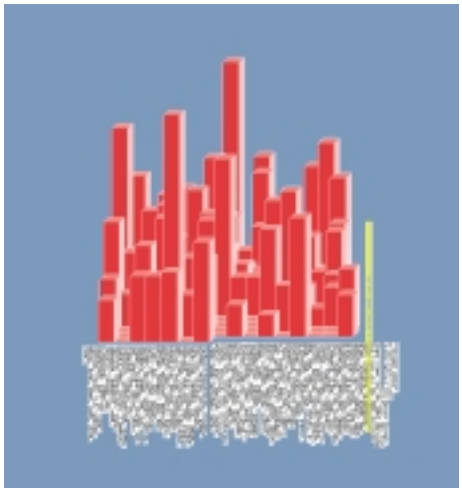
Empire, Hardt & Negri

Ethernet wurde an der Universität von Hawaii erfunden. Anfang der siebziger Jahre standen die dortigen Experten vor einem ganz besonderen Problem: Wie kann man sämtliche, auf jeweils unterschiedlichen Inseln gelegene Campusse miteinander vernetzen?[1] Die Lösung bestand darin, die Daten per Funk durch die Luft – den „Äther“ – zu übertragen. Ohne Kabel. Wie ein Radiosender sandte jeder Knoten Informationen völlig frei übers Meer zu den anderen Inseln. Man entwickelte ein Protokoll, um Kollisionen bei gleichzeitiger Übertragung zu vermeiden. Seit damals basiert Ethernet auf einem offenen Übertragungsmodell. Das Protokoll ließ sich auch für verkabelte Netze leicht einsetzen und ist heute das am weitesten verbreitete lokale Netzwerkprotokoll der Welt. Da Ethernet ein offenes Übertragungsmodell ist, können sich unauffällig Abhörer „einschleichen“ und alle Nachrichten mithören, nicht nur die direkt an sie adressierten. Diese Technik wird als „Packet-Sniffing“ bezeichnet und von Systemadministratoren wie auch Hackern seit Jahrzehnten praktiziert. Ethernet, Sniffer und Hacken sind das Herzstück des Public-Domain-Überwachungspakets *Carnivore,* das von der Radical Software Group (RSG) entwickelt wurde und nun von vielen Künstlern und Wissenschaftlern weltweit in einem zivilen Kontext eingesetzt wird.

Hacken

Heute sagt man Hackern grundsätzlich zwei Dinge nach: Sie sind entweder Terroristen oder Freigeister. Ursprünglich bezeichnete das Wort einen ungelernten Kesselflicker, einen Autodidakten, der zig Lösungen probierte, bis er endlich Erfolg hatte.[2] Nach Bruce Sterling bezeichnet der Begriff Hacker „die ungezügelte intellektuelle Auslotung der äußersten Potenziale von Computersystemen“.[3] Steven Levy wiederum schwärmt von den ersten MIT-Hackern Anfang der sechziger Jahre, dass „sie faszinierende Menschen waren. [...] Hinter ihrem oft unscheinbaren Äußeren waren sie Abenteurer, Visionäre, Draufgänger, Künstler... und diejenigen, die am deutlichsten sahen, was den Computer so revolutionär machte.“[4] Dieser Typ Hacker ist ein Freiheitskämpfer, der nach dem Motto „Daten wollen frei sein“ lebt.[5] Information sollte keinen Besitzer haben; falls doch, so tut ein nicht-invasorisches Schmökern in diesen Informationen niemandem weh. Im Übrigen nutzen Hacker bloß bereits bestehende Lücken in schlecht programmierten Codes.[6] Und erhöht das Aufdecken solcher Lücken nicht die Datensicherheit für alle Beteiligten?

Die Identität des Hackers hat sich Mitte bis Ende der achtziger Jahre in den USA gewandelt: Der Hobby-Computerguru wurde aufgrund einer Mischung aus öffentlicher Technophobie und aggressiver Legislatur zum digitalen Outlaw.[7] So wurde z. B. 1986 das Gesetz gegen Computerbetrug und -missbrauch *(Computer Fraud and Abuse Act)* erlassen, das das Eindringen in Systeme von Bundesbehörden zu einem Kapitalverbrechen macht. Die Hacker waren über ihre neu gewonnene Identität als Gesetzlose zutiefst getroffen, was 1986 im berühmten *Hacker-Manifest* seinen Niederschlag



fand. Verfasst wurde es von jemandem, der sich selbst[8] „The Mentor“ nennt: „Wir sind Entdecker ... und ihr nennt uns Kriminelle. Wir suchen nach Wissen ... und ihr nennt uns Kriminelle.“[9] Aufgrund dieser semantischen Verwandlung werden Hacker heute pauschal als Terroristen bezeichnet, als Taugenichtse, die zur eigenen Bereicherung in Computersysteme einbrechen. Zur Jahrtausendwende hatte der Begriff „Hacker“ seine ursprüngliche Bedeutung völlig verloren. Sagt heute jemand Hacker, so meint er Terrorist.

Die laufende Debatte über Hacker wird durch den Diskurs über modernen Liberalismus erstickt: Sollen Daten als Privateigentum respektiert werden oder soll die Freiheit des Einzelnen kultiviert und der Computeruser sich selbst überlassen werden? Hacken ist bedeutend mehr. Es nimmt eine neue Art des Kulturschaffens vorweg, die RSG mit *Carnivore* zu verkörpern versucht.

Zusammenarbeit

Bruce Sterling schreibt, dass das ausgehende 20. Jahrhundert in der Transformation von einem modernen zentralistisch-hierarchischen Kontrollparadigma zu einem postmodernen horizontal-flexiblen begriffen ist:

> Seit Jahren spekulieren Wirtschafts- und Managementtheoretiker, dass die Flutwelle der Informationsrevolution feste, pyramidenförmige Bürokratien, in denen alles von oben nach unten und zentral gelenkt wird, zerstören könnte. Hochqualifizierte „Angestellte“ erhielten mehr Autonomie, wären initiativ und selbst-motivierend und bewegten sich flink und geschmeidig von Ort zu Ort, von Aufgabe zu Aufgabe. „Ad-Hocratien“ wären an der Macht, wo spontan Menschen quer durch die Organisationsebenen Gruppen bilden, die ein vorliegendes Problem unter Einsatz von immensem computergestütztem Fachwissen anpacken, um sich anschließend wieder genauso schnell aufzulösen.[10]

Von Manuel Castells über Hakim Bey bis Tom Peters wurde diese Phrase immer wieder bemüht. Sterling behauptet sogar, dass sowohl Hacker als auch Gesetzeshüter bei der Verfolgung dieser dem neuen Paradigma folgen: „Sie *alle* agieren wie ‚Tiger-Teams’ oder ‚Benutzergruppen’. Sie sind elektronische Ad-Hocratien, die spontan entstehen und einen Bedarf abzudecken versuchen.“[11] Mit „Tiger-Teams“ meint Sterling Gruppen von Mitarbeitern, die von Firmen eingesetzt werden, um die Sicherheit ihrer Computersysteme zu testen. Im Grunde simulieren Tiger-Teams Hackerattacken, um Sicherheitslücken zu finden und auszumerzen. RSG ist eine Art Tiger-Team.

Hacker sind autonome Agenten, die sich in Kleingruppen zusammenfinden können, um einzelne Probleme anzupacken. Sie verkörpern einen anderen organisatorischen Managementtyp (den man „protokollogisch“ nennen könnte) als Widerstandsgruppen alter Prägung, die „starre, pyramidenförmige Bürokratien“ waren, wie Sterling und andere meinen. Somit kann man sagen, dass sich der Widerstand, während er im modernen Zeitalter auf starren Hierarchien und bürokratischen Machtstrukturen aufbaute, in der Postmoderne um protokollogische Machtzentren in Netzwerken herum bildet.

Code

Der Künstler Sol LeWitt umriss 1967 seine Definition von Konzeptkunst (heißt das nicht Konzeptkunst?) wie folgt:

> In der Konzeptkunst ist die Idee, das Konzept der wichtigste Aspekt der Arbeit. Bedient sich ein Künstler der konzeptuellen Kunstform, so erfolgen die gesamte Planung und die Entscheidungen im Vorfeld und die Ausführung wird zur Nebensache. Die Idee wird zum Vehikel der Kunst.[12]

LeWitts Sichtweise von Konzeptkunst hat wichtige Implikationen für den Code, denn seiner Einschätzung nach ist Konzeptkunst bloß eine Art Code für das Kunstschaffen. LeWitts Kunst ist ein algorithmischer Prozess. Der Algorithmus wird im Vorhinein erstellt und erst später vom Künstler selbst (oder einem anderen Künstler) ausgeführt.
Was unterscheidet den Code so sehr vom bloßen Schreiben? Die Antwort liegt in der einzigartigen Natur des Computercodes. Er ist de facto nicht sub-linguistisch, sondern *hyper*-linguistisch. Code ist eine Sprache, aber eine ganz besondere. *Code ist die einzige Sprache, die ausgeführt werden kann.* Wie Kittler meint, „gibt es kein Wort in irgendeiner normalen Sprache, das tut, was es sagt. Keine Beschreibung einer Maschine setzt diese in Gang.“[13] Der Code ist daher die erste Sprache, die tatsächlich das tut, was sie sagt – er ist eine Maschine, der Bedeutung in Aktion umsetzt.[14] Er besitzt eine semantische Bedeutung, setzt diese Bedeutung aber auch in Szene.

Träume

Frederic Jameson sagte einmal, dass es zu den schwierigsten Dingen im modernen Kapitalismus gehört, sich Utopia vorzustellen. Genau deswegen ist das Träumen so wichtig. Zu entscheiden (und oft dafür zu kämpfen) was möglich ist, ist der erste Schritt zu einer utopischen Vision, die auf unseren Wünschen, auf dem was wir *wollen,* fußt. Eine solch visionäre Stimmung fehlt laut Jameson dem modernen Diskurs in hohem Maß. Utopie und Möglichkeit stehen ganz eng beieinander. Man muss wissen, was man will, um zu wissen, was man denn wollen *kann.* Erst dann lässt sich eine Utopie überhaupt erst vorstellen.
Die anti-kommerzielle Neigung der Hackergemeinde ist eines der wichtigsten Merkmale dieses utopischen Instinkts. Schon lange werden Programme, ohne offenkundiges Profitinteresse des Autors, bloß zu höheren Ehren des Codes selbst, für die Public-Domain-Schiene entwickelt.
Noch bedeutender als der Anti-Kommerzialismus ist jedoch der Pro-Protokollismus. Ein Protokoll ist per definitionem „Open Source“, eine Bezeichnung für Technologien, deren Quellcode frei erhältlich ist. Anders ausgedrückt, ist ein Protokoll nichts anderes als eine ausgeklügelte Liste von Anweisungen, wie eine bestimmte Technologie funktionieren sollte, und zwar von vorne nach hinten und von oben nach unten. Ein Beispiel dafür sind die RFCs oder „Request For Comments“-Dokumente. Während viele Technologien, deren Code nicht frei zugänglich ist, durch ihre oft monopolistische Marktstellung protokollogisch scheinen, kann ein echtes Protokoll niemals proprietär und unzugänglich sein. Es muss am Präsentierteller liegen und von allen angenommen werden. Es profitiert im Laufe der Zeit von seiner technologischen Weiterentwicklung in der

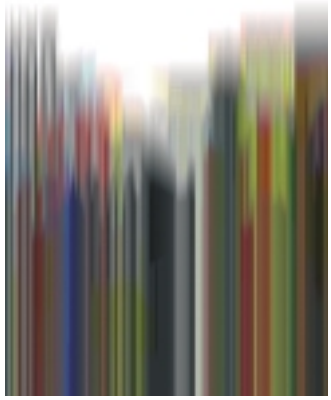
Öffentlichkeit. Sein Code muss rein und transparent sein (oder eine verständliche *Beschreibung* liefern, wie man den Code anpasst). Sobald eine Technologie proprietär ist, ist sie nicht mehr protokollogisch.
Das bringt uns zurück zu *Carnivore* und dem Wunsch, eine Public-Domain-Version des berüchtigten Überwachungstools herauszubringen, das bislang nur Regierungsbehörden zugänglich war. *Carnivore* von RSG gleicht das Spielfeld aus, macht Kunst und Kultur wieder zum Schauplatz eines Konflikts vieler statt einseitiger Dominanz und öffnet so das System für die Zusammenarbeit innerhalb und zwischen Künstler-Clients. Der Code dient dabei zum Umhüllen und Modifizieren der ursprünglichen FBI-Maschinerie.

Carnivore Personal Edition

Am 1. Oktober 2001, drei Wochen nach den Anschlägen vom 11. September, verkündete RSG die Veröffentlichung von *Carnivore,* einer Public-Domain-Variante der berüchtigten FBI-Software DCS1000 (mit dem allgemein bekannten Spitznamen „Carnivore"). Während es das FBI-Programm schon einige Zeit gab und RSG bereits seit Januar 2001 an seiner Version arbeitete, verursachten die Ereignisse vom 11. September ein Auflodern der Überwachungstätigkeit. Es gab Gerüchte, wonach das FBI Carnivore wohl oder übel in zivilen Netzwerken wie Hotmail oder AOL installierte, um einzig und allein terroristische Nachrichten abzufangen. Wie *Wired News* am 12. September 2001 berichtete, hat „ein Netzwerkadministrator eines der wichtigsten Internetprovider erzählt, dass FBI-Beamte am [11. September] an seinem Arbeitsplatz erschienen sind, ‚mit ein paar Carnivores, und haben um Erlaubnis gebeten, sie in unserem Zentrum aufstellen zu dürfen.'" Von leitenden Angestellten bei Hotmail wird berichtet, sie wären bei den Überwachungsanträgen des FBI „kooperativ" gewesen. Durch diese Aktivität angespornt, sollte der *RSG Carnivore* dort fortsetzen, wo das FBI aufgehört hatte, nämlich diese Technologie einer breiten Öffentlichkeit zugänglich zu machen, um die Überwachungsdichte innerhalb der Kultur zu erhöhen. Der erste *RSG Carnivore* lief unter Linux. Ein Open-Source-Schema wurde ins Netz gestellt, damit auch andere es nachbauen konnten. Neue Funktionen wurden hinzugefügt, um die vom FBI entwickelte Technologie zu verbessern (die in Wirklichkeit eine vereinfachte Version von Tools war, die von Systemadministratoren seit Jahren eingesetzt werden).
Die ersten Tests waren erfolgreich und führten zu weiteren Feldversuchen im Princeton Art Museum (wo *Carnivore* wie ein Virus in seinem eigenen Subnetz in Quarantäne gehalten wurde) und im New Museum in New York. Am Wochenende um den 1. Februar 2002 wurde *Carnivore* bei Eyebeam eingesetzt, um die gegen das Weltwirtschaftsforum protestierenden Hacktivisten zu überwachen.
Wegen der geringen Marktchancen eines reinen Linux-Programms, brachte RSG am 6. April 2002 *Carnivore Personal Edition* (PE) für Windows heraus. *Carnivore PE* verfügte nun über eine neue verteilte Architektur, da nun jeder PC-Benutzer den eigenen Netzwerkverkehr analysieren und diagnostizieren konnte. Jeder Künstler oder Wissenschaftler kann *Carnivore* als Überwachungs-Engine für seinen interpretierenden „Client" einsetzen. Schon bald verwandelten *Carnivore*-Clients den Netzwerkverkehr in Klänge, Animation und sogar 3D-Welten, während die Technologie über das Netzwerk verteilt wurde. Der Gedanke, die originale FBI-Software rückzuentwickeln, war für RSG nicht reizvoll. Durch gesetzliche und ethische Beschränkungen verkrüppelt, erforderte das FBI-Programm eine Verbesserung und nicht eine Emulation. Daher bietet *Carnivore PE* eine Reihe außergewöhnlicher Funktionen, wie z. B. künstlerisch gestaltete Diagnose-Clients, Fernzugriff, vollständige Betreffsuche, vollständige Datensuche, Laufwerkspuffer,

Transportprotokollfilter und eine Open-Source-Programmlizenz. RSG wollte nicht bloß das FBI-Programm mit all seinen Unzulänglichkeiten kopieren. Vielmehr schwebte RSG vor, dem Packet-Sniffing, einer grundlegend destabilisierenden und transformierenden Technologie, neue progressive Politik einzuimpfen. Unser Ziel ist es, einen neuen Verwendungszweck für die Datenüberwachung zu erfinden, der aus dem Dilemma Held / Terrorist ausbricht und stattdessen von einer zukünftigen Nutzung vernetzter Daten träumt.

Aus dem Amerikanischen von Michael Kaufmann



1 An der Universität von Hawaii nannte man das von Norman Abramson entwickelte System ALOHAnet. Später wurde es von Robert Metcalfe bei Xerox PARC weiterentwickelt und als „Ethernet“ bezeichnet.

2 Robert Graham führt die Etymologie des Begriffs auf den Golfsport zurück: „Das Wort ‚Hacker‘ bezeichnete im 14. Jahrhundert einen unerfahrenen oder für eine bestimmte Aktivität unbegabten Menschen (wie z. B. den Golf-Hacker). Um 1970 bezeichneten Computerenthusiasten sich selbst als ‚Hacker‘. Das zeigte auch den Zugang dieser Enthusiasten zum Computer: Sie mieden eine formelle Ausbildung und spielten so lange mit dem Computer herum, bis sie ihn zum Laufen brachten. (Das ähnelt ziemlich der Art wie Golf-Hacker auf den Golfball eindreschen, bis er im Loch ist.)“ *(www.robertgraham.com/pubs/hacking-dict.html).*

3 Bruce Sterling, *The Hacker Crackdown,* S. 51. Bantam, New York 1992.

4 Steven Levy, *Hackers: Heroes of the Computer Revolution,* S. ix. Anchor Press / Doubleday, New York 1984.

5 Dieser Ausspruch wird Stewart Brand zugeschrieben, der meinte, dass „die Information einerseits teuer sein will, weil sie so wertvoll ist. Die richtige Information am richtigen Ort verändert dein Leben. Andererseits möchte Information frei sein, denn die Kosten, um sie herauszubringen, sinken beständig. Daher stehen diese beiden im Widerstreit.“ Vgl. *Whole Earth Review,* S. 49, Mai 1985.

6 Viele Hacker sind der Ansicht, dass kommerzielle Computerprogramme weniger sorgfältig entwickelt werden und daher leichter auszunutzen sind. Das vielleicht berühmt-berüchtigste Beispiel ist das Programm „Back Orifice“ der Hackergruppe Cult of the Dead Cow, die damit die wachsende Kommerzialisierung anprangern. Als eine Satire auf die „Back Office“-Programmsuite von Microsoft fungiert Back Orifice als Trojaner und ermöglicht den Fernzugriff auf PCs, die unter dem Betriebssystem Microsoft Windows laufen.

7 Eine hervorragende geschichtliche Analyse dieser Umwandlung findet sich in Sterlings *The Hacker Crackdown.* Andrew Ross erklärt diese Verwandlung, so wie Sterling und andere auch, mit der Zunahme von Computerviren Ende der Achtziger, allen voran „die vom Hacker Robert Morris von der Cornell University im November 1988 initiierte Virusattacke auf das Internet. [...] Während er wenig echten Datenschaden anrichtete [...], so haben die Auswirkungen dieses Internet-Viruses geholfen, eine moralische Panik zu erzeugen, die die tägliche ‚Computerkultur‘ nachhaltig verändert hat.“ Vgl. Andrew Ross. *Strange Weather: Culture, Science, and Technology in the Age of Limits,* S. 75. Verso, New York 1991.

8 Während die meisten Hacker geschlechtsneutrale Pseudonyme verwenden, zeichnete sich das Online-Magazin *Phrack,* mit dem The Mentor assoziiert war, durch seine ausgeprägt männliche Belegschaft und Leserschaft aus. Für eine soziologische Erklärung des Geschlechterungleichgewichts in der Hackergemeinde, vgl. Paul Taylor. *Hackers: Crime in the digital sublime,* S. 32–42. Routledge, New York 1999.

9 The Mentor, „The Conscience of a Hacker“, in *Phrack,* Bd. 1, Nr. 7, Datei 3. *www.iit.edu/~beberg/manifesto.html*

10 Sterling, *The Hacker Crackdown,* S. 184.

11 Ibid.

12 Sol LeWitt, „Paragraphs on Conceptual Art“, in Alberro, et al., Hgs., *Conceptual Art: A Critical Anthology,* S. 12. MIT Press, Cambridge, 1999. Danke an Mark Tribes, der mich auf diese Passage aufmerksam gemacht hat.

13 Friedrich Kittler, „On the Implementation of Knowledge – Toward a Theory of Hardware“, in *nettime (www.nettime.org/nettime.w3archive/199902/msg00038.html).*

14 Ein interessanter Kommentar zur ästhetischen Dimension dieser Tatsache findet sich bei Geoff Cox, Alex McLean, Adrian Ward. *The Aesthetics of Generative Code (http://sidestream.org/papers/aesthetics/)*