Claus Pias (Hg.)

Abwehr

Modelle – Strategien – Medien

[transcript]

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Umschlaggestaltung: Kordula Röckenhaus, Bielefeld
Lektorat & Satz: Claus Pias
Druck: Majuskel Medienproduktion GmbH, Wetzlar
ISBN 978-3-89942-876-6

Gedruckt auf alterungsbeständigem Papier mit chlorfrei gebleichtem Zellstoff.

Besuchen Sie uns im Internet: http://www.transcript-verlag.de

Bitte fordern Sie unser Gesamtverzeichnis und andere Broschüren an unter: *info@transcript-verlag.de*

Inhalt

Digital Korrekt: Zwischen Terror und Spiel

Peter Krapp

Während staatliche wie private Maßnahmen weltweit den freien Nutzen von Computern im Netz zunehmend einschränken, droht die die öffentliche Diskussion um die Konsequenzen solcher Schritte zu verkümmern.[1] Soziale Macht ist in der vernetzten Gesellschaft bereits so diffus, daß Adam Smiths Marktmetapher der unsichtbaren Hand zur puren Nostalgie gerät. Im Übergang globaler Organisationen vom Modell der Aktiengesellschaft zum Modell des Netzes verschwindet der Ort der Macht aus dem Blick, und Bürger der planetaren Informationsgesellschaft sehen sich weniger durch konzentrierte Autorität, als durch ideologische Bindungen regiert, die sich in den symbolischen Praktiken und Normen des Cyberspace manifestieren (Mann 1986, Castells 1996, Latour 1999: 204f.). Zugleich wird Medienpolitik zunehmend von profitorientierten Privatinteressen gestaltet, anstatt im Prozeß der repräsentativen Demokratie, was den juridischen und politischen Rahmen der vernetzten Computerkultur im Lauf des letzten Jahrzehnts entscheidend verändert hat. Aufgrund dieser Entwicklungen drohen kritische Medienpraxis und konzeptuelle Computerkunst im Netz zu verschwinden. Sobald das »cyber-terror« Szenario schlicht alles erfaßt, was im Vergleich zum offiziell sanktionierten Interface auch nur irgendwie destablisierend, subversiv, oder unautorisiert erscheint, ist die Rede von Computerkultur als einem Triumph der Bricolage effektiv kriminalisiert. Und so feiert die Populärkultur den Hacker nicht mehr als den harmlosen und gelegentlich sehr profitablen Hobbyisten. Im Fernsehen werden keine verschrullten Talente romantisiert, die Zeitungen verkaufen die Triumphe des digitalen Kapitalismus nicht mehr – stattdessen begegnet einem allenthalben das digitale Schreckgespenst des »Hacktivismus« als eine irreduzible systemische Bedrohung.

1 Der Beitrag basiert auf Peter Krapp, »Terror and Play: Or, what was Hacktivism?«. In: Grey Room, 21 (2005), S. 70-93.

Um die eigentümliche Balance von Geheimnis und Zugangsrechten in der Informationspolitik zu würdigen, bedarf es einer Kombination von psychologischen, theoretischen und technischen Einsichten, wie bereits Shannon betonte (Shannon 1949: 656). Dieser Essay will daher drei der unglücklichsten Mißverstandändnisse ausräumen, die das Bild der neuen Medien allgemein und das der Netzaktion im Besonderen grob verzerren. Zunächst werden Hacker zu oft als unreife Rüpel porträtiert, und Abhilfe soll dann gleich erhöhte polizeiliche Autorität schaffen, mitsamt den unausweichlichen Nebeneffekten solcher Disziplinierung der Computerszene. Sobald dann neue Einschränkungen der freien Rede und der Privatsphäre zum Normalfall werden, wird Aktivismus im Zeitalter von gezielter Datensuche allzu schnell als Cyberterror verkannt, und wer die weniger wünschenswerten Nachwirkungen der Kommerzialisierung des Netzes hinterfragt, erscheint sogleich als Staatsfeind. Drittens ist die allfällige Behauptung, daß größere Geheimniskrämerei mehr Sicherheit bedeute, ganz offenkundig falsch, und der Kult des Verbergens trägt direkt zur Verbreitung aller möglichen irrationalen Verschwörungstheorien im Internet bei. Sobald aber Verschwörungstheorie den Platz kritischer öffentlicher Debatten um Codes und Gesetze einnimmt, ist die Netzkultur gefährlich verarmt.

Netzpolitik

Ausdrucksstarke Politik ist der Freiheitskampf gegen beide Versionen der Ware – ihrer totalisierenden Marktform und ihrer bürokratischen Staatsform.
McKenzie Wark

Wollte man in den vergangenen Jahren über Nuklearforschung in Indien informiert bleiben, dem Schicksal der indianischen Bevölkerung im mexikanischen Chiapas folgen, oder von Protesten gegen die Welthandelsorganisation wissen, dann ging man angesichts der mangelnden Information in Zeitungen, Radiosendern, und Fernsehkanälen ins Netz. Globalisierungs-Skeptiker, Stromaktivisten, Wasserrechtler, Zapatistas und andere Gruppen fanden einander online und suchten Aufmerksamkeit auf ihre Ziele zu lenken, indem sie etwa Websites blockierten oder veränderten, die gewissen indischen Physik-Forschungslaboren oder der Regierung Mexikos oder einem konservativen Think Tank gehörten. Europäische Politiker richteten die Weltaufmerksamkeit auf *Echelon*, eine geheime Installation der USA, die den elektronischen Datenverkehr weltweit überwacht, sei es über Satelliten, Telefone, oder Computernetze. Um den Schleier der Geheimhaltung zu lüften, veranstalteten Aktivisten einen »Jam Echelon Day«, an dem sie versuchten, diese allgegenwärtige Überwachung zu unterlaufen und die Medien zu kritischer Beobachtung aufzurufen. Chinesische Computer griffen amerikanische Websites an, um gegen die NATO Bomben auf die chinesische Botschaft im Kosovo zu protestieren. Ein

virtueller Sit-in legte im Februar 2000 eine Reihe kommerzieller Websites in den USA lahm. Obwohl diese »Denial of Service«-Attacken nur wenige Stunden dauerten und rein symbolisch angelegt waren, wurden sie zur Titelgeschichte für viele Tageszeitungen und ein halbes Dutzend Wochenzeitschriften (Sandberg/Hayden 2000). Dort waren Journalisten nur zu eifrig, Firmen wie *Yahoo* und *eBay* als Opfer von Vandalen darzustellen, obwohl kein bleibender Schaden an den Websites festzustellen war. Die kleinste Drohung gegen die Verdummung des Internet zu einem gigantischen Werbekanal schien die amerikanische Wirtschaft als Ganze zu unterlaufen: Wann kann ich wieder Geld ausgeben, indem ich auf kleine Pixel klicke? Wer wagt es, meinen virtuellen Konsumrausch zu unterbrechen? Der Gesetzgeber beeilte sich in jedem Fall, das Einkaufen sicherer zu machen, und so verkümmern nichtkommerzielle Anwendungen im Internet unter dem Hammer kaufmännischer Paranoia. Jeglicher Nutzen von Computern im Netz, der keinen Profit abwirft (oder zumindest verspricht), ist somit suspekt geworden: Selbst Universitäten, einst Bastionen des interesselosen Forschens, geraten unverhofft zu Diplomschmieden.

Hacktivismus ist daher ein kontroverser Begriff. Während manche von kritischem Bürgerbewußtsein und sozialer Gerechtigkeit im Computerzeitalter reden, sehen andere nur destruktive Aktionen, die die Sicherheit des Netzes als technische, wirtschaftliche, und politische Plattform erschüttern. Wieder andere denken spezifisch an Menschenrechte, freie Meinungsäußerung und Informationsethik (Vegh 2003, Gunkel 2001). Selbst die Schreibweise dieses Neologismus ist umstritten – wo man ein technisches Erbe betont, schreibt man Hacktivismus und beruft sich auf lernendes Testen und kreatives Problemlösen der Hacker; wo man aber radikalisierte oder militante Aktion sieht, schreibt man *Hacktivismus*... So oder so gibt es keine gemeinsamen Ziele oder Motive, die alle erwähnten Beispiele auf einen Nenner zu reduzieren erlaubten: Es ist jedenfalls unzureichend zu warnen, daß Regierungen die ursprünglich ungemein produktive Hacker-Ethik pervertiert und kriminalisiert haben (Lessig 1999: 40). Netzaktion mag zwar Datenüberwachung bedeuten oder eine Flut von Server-Anfragen, falsche Mirrorsites setzen oder eine Netzpräsenz mit digitalem Graffiti verunstalten – doch diese Sit-ins und virtuellen Blockaden, Emails und Software können mit demselben Recht konzeptuelle Netzkunst genannt werden (Denning 2003: 248, 265, Gordon 1981, Treverton 2003). Das FBI Programm namens »Carnivore« (DCS1000) wird von der *Radical Software Group* zitiert, wobei deren Netzkunst zwar Züge der Netz-Überwachung übernimmt, hier jedoch um Künstlern die Datenströme auf einem lokalen Netz zur Verfügung zu stellen, auf daß sie verschiedene visuelle Repräsentationsformen imaginieren.[2] Ähnlich das Programm »Peekabooty« der Gruppe *Cult of the Dead Cow* (cDc), das Nutzern ermöglicht, Internet-Zensur zu unterlaufen. Das »Electronic Disturbance Theater« wiederum veranstaltete eine Protestwoche parallel zum Republikaner-Nationalkongreß 2004 in New York, indem es konservative Websites zu blockieren suchte

2 Radical Software Group: »Carnivore,« http://rhizome.org/carnivore.

und Sit-ins gegen das Kommunikationsnetz der Republikaner koordinierte (Wray, Dominguez). Andere Hacktivisten demonstrierten gegen Atomforschung in Indien, indem sie auf Computer des *Bhabha Atomic Research Center* zugriffen; oder sie machten ihre Kritik an multinationalen Firmen auf Websites wie McSpotlight.org oder Bhopal.net öffentlich; oder aber sie boten Software-Lösungen zum Unterlaufen der chinesischen Internetzensur an. So kann Hacktivismus eine politisch konstruktive Form des zivilen Ungehorsam oder eine anarchische Geste darstellen, antikapitalistische Agitation bedeuten oder kommerziellen Protektionismus, Abteibungsgegnern oder Befürwortern der Gedankenfreiheit dienen, Weltbürgerschaft im Namen führen oder gegen Weltbank und Welthandel wüten (Jordan/Taylor 2004). Zudem ist das gleiche Vokabular und Instrumentarium von *port scanning* bis *packet sniffing* schon lange von staatlichen Agenturen und internationalen Firmen angeeignet worden. 1995 präsentierte die *RAND Corporation* ein Szenario, in dem der Iran einen Indischen Programmierer des Airbus besticht, so daß er einen Flugzeug-Absturz über Chicago verursachen kann (Molander/Riddile/Wilson 1996). Die Spionage-Agentur NSA sammelte nicht nur tausende von Seiten mit Information über Prinzessin Diana, das große Sicherheitsrisiko, sondern hielt zugleich auch seine Mitarbeiter dazu an, die Computer der Weltraumagentur NASA auf Schwächen zu testen (Enjung Cha 2005).[3] Kanada hat gar ein offizielles Hacktivisten-Team in einem »Citizen Lab« versammelt, wo Politologen und Programmierer die Zensur in Ländern wie China, Kuba, Iran, Saudi-Arabien, und Usbekistan auszuhebeln versuchen, um der Redefreiheit weltweit zur Seite zu stehen. Dieses akademische Team hat auch über Filter und Firewalls in Ländern wie Syrien und die Vereinigten Arabischen Emirate publiziert. Deutschland wiederum hat versucht, Zugriff auf ausländische Server im Netz zu blockieren, sofern sie etwa Neonazi-Material anboten. Außenminister Otto Schily, so wurde berichtet, habe staatliche Interventionen in Betracht gezogen (Dornseif 2003). Dies wiederum, hätte es stattgefunden, wäre von der US-Regierung als Cyberterror betrachtet worden – gewiß ein diplomatischer Skandal. Doch obwohl deutsche Regierungssprecher solche Maßnahmen als legal verteidigten, ist kein konkretes Beispiel deutschen Cyberterrors bekannt. In der Tat ist *cyberterrorism* als Begriff kein einziges Mal in amerikanischen Gerichten verwendet worden, seit es als Tatbestand und Schlagwort im Jahr 2001 eingeführt wurde (McCullagh 2003).

Im Geiste spielerischer Erkundung enstand die Mehrzahl der Computer-Innovationen über mehrere Jahrzehnte. Bis in die späten 1980er Jahre galt als Hacker jemand, der durch Versuch und Irrtum und ohne Handbuch erfolgreich Software programmierte. Doch nur fünf Jahre später begannen die Medien von gefährlichen und teuren Problemen zu unken (Denning 1990; Denning 1995). Kommentare zur digitalen Kultur, die bislang auf freien Zugriff, interesselose Forschung, allgemeine Meinungsfreiheit und Schutz der Privatsphäre gebaut hatten, schalteten mit einem

3 »The National Security Agency has disclosed that U.S. intelligence is holding 1,056 pages of classified information about the late Princess Diana« (Loeb 1998).

Mal auf eine alarmierende Rhetorik um, die genau diese Stichworte dämonisierte (Denning 2000). Das Netz schien, wie einst die Druckerpresse oder das Radio, ein wahres Kommunikationsmedium zu versprechen (Brecht 1967; Vegh 2002). Doch kurz nachdem der Kalte Krieg neue Medien der Massenzerstreuung in Umlauf gebracht hatte, wurde das weltweite Computernetz dreifach eingeschränkt: durch die Privatisierung des »Rückgrats« oder Basisnetzes, durch das Schließen der Betriebssysteme und durch Zensur. Die Tendenz zur Obskuranz als Pseudo-Sicherheit, nebst Verteufelung allen Hinterfragens solch rabiater Informationspolitik, wurde durch das frühe Versagen des e-Kommerz-Hypes und das politische Scheitern des Clipper Chip nur verschärft, und heute zeigt sich im Hacktivismus eine verzweifelte letzte Hoffnung, der Kontrollgesellschaft zu entschlüpfen, wo dem machtlosen Ort des Einzelnen die ortlose Macht der Medien gegenübersteht. Sobald all unsere Daten und Handlungen, Einkäufe und Vorlieben im Netz gespeichert und zugänglich sind, gemeinsam mit unseren medizinischen und genetischen Angaben, Schul- und Berufsleben, Kreditkarten und Steuerangaben, mag unser letzter Trost darin liegen, daß diese persönliche Inquisition bisher etwa so akkurat ist wie die Konsumenten-Fragebögen im Kaufhaus. Doch für einen wachsenden Teil der Weltbevölkerung ist Anonymität in der Techno-Menge illusorisch (Fuller 2003). Zweifellos ist manches Beispiel des »Hacktivismus« dem gleichen Dilemma geschuldet, das populären Verschwörungstheorien im Internet Futter bietet, indem beide Arten von Reaktion nämlich sich in Phantasien der Manipulation ergehen, die jegliche Gegenmaßnahmen zu rechtfertigen scheinen.

Frankfurter Vorschule

Nur ein Narr verwirft den Bedarf hinter den Schirm zu blicken.
Don DeLillo

Verschwörungstheorien sind im Internet so populär, daß sie praktisch eine Art einheimischen Ausdruck des Denkens im Netz darstellen, und zwar zugleich als Diskurs über das Netz und als Mutmaßung über seine vermeintlichen Ursprünge. Verschwörungstheorien bieten alternative Geschichten, die Geschichte und Politik virtualisieren, wo immer die offizielle Version zu selektiv oder tendentiös erscheint. So muß Verschwörungstheorie als Insistenz auf einer (wenn auch noch so degradierten) Lesbarkeit der Welt und ihrer immer komplexeren Technologien erkannt werden. In der Mediengesellschaft gibt es keinen Blickwinkel, von dem aus die neuen Technologien nicht zu tiefstem Mißtrauen anregen; die verbindliche Abnabelung der Gadgets befördert eine allgemeine Paranoia. Phantasien über die Allmacht von internationalen Firmen einerseits oder schattenhaften Hackern andererseits sind die Kehrseite einer neurotischen Identifizierung mit eine Zentralmacht, die einem die dezentrierte Gesellschaft erklären mag.

Studien zur Verschwörungstheorie tendieren in zwei Richtungen: die eine pathologisiert Paranoia, die andere feiert sie als populistischen Ausdruck der Unterdrückung. Das Problem mit einer solchen Gegenüberstellung ist, daß solche wilden Diagnosen gemeinhin von der anderen Seite kommen, als Kritik an der vorangehenden Literatur (Hofstadter 1965; Curryy 1972; Johnson 1983; Pipes 1997; Fenster 1999; Melley 2000; Pratt 2001). Esther Dyson etwa schreibt »das Internet ist ein Medium nicht für Propaganda sondern für Verschwörungen – da fliegt so viel herum, daß keiner die Zeit hat, alle Fehler zu dementieren« (Dyson 1998). Und selbst ein Dementi kann das Gerücht weiter zirkulieren und so legitimieren. Dementsprechend spotten manche, daß Verschwörungstheorien die »Kultiviertheit der Ignoranz« darstellen (Grenier 1992). Doch interessant an Verschwörungstheorien ist nicht nur, daß sie paranoide Phantasien von oft sehr normalen Leuten sind, sondern gerade, daß sie auch und vor allem ein Modus des Theoretisierens sind (Hofstadter 1965: 4).

Natürlich gibt es spöttische Kommentare, die behaupten »im Web kriegen wir, was wir uns wünschten – eine breite Öffentlichkeit – und genau das ist das Problem« (Dean 2000: 63). Dies führt dann entweder zu einem didaktischen Aufruf – »Leider haben wir als Gesellschaft noch nicht genügend ›Net Literacy‹ erlernt«, wie Dyson schreibt – oder zu der Vorstellung, daß das Internet »die Idee der Öffentlichkeit bedroht, weil es die Möglichkeit des Geheimnisses eliminiert« (Dyson 1998: 50). Die Ironie letzterer Position liegt natürlich in der Mahnung, daß die Idee einer Medienöffentlichkeit sich, nach Habermas, aus dem Erbe geheimer Gesellschaften entwikkelt habe (Dean 2000: 71f.). Je amorpher das Netz erscheint, desto insistenter die Hoffnung auf Erlösung: Wenn alle Daten geordnet und verstanden sind, soll Wahrheit und Bedeutung erstehen. Diese uralte Utopie ist allerdings oft begleitet von der Einsicht, daß solche Aufklärung unerreichbar bleibt. Verschwörungsdenken erlaubt in diesem Moment Zuflucht in der kläglichen Gewißheit, daß etwas Wichtiges wohl dennoch immer verborgen bleibt (Harmon 1997).

Jenseits einer unproduktiven Gegenüberstellung von Kontrollgesellschaft und Subkulturen wirft Verschwörungsdenken Licht auf dringende Fragen nach Sicherheit und Geheimhaltung, Meinungsfreiheit und Datenkontrolle. Wie die zahlreichen Verschwörungen um das Attentat auf John F. Kennedy belegen, ist selbst die am weitesten hergeholte Erklärung von einer Art Frankfurter Vorschule ferngesteuert, denn sie verbindet typischerweise einen vulgären Marxismus (es war die Mafia im Bund mit Anti-Castro-Militanz – also uneingeschränkter Kapitalismus und reaktionäre Gruppen) mit vulgärer Psychoanalyse (die ödipale Eifersucht von Lyndon B. Johnson und J. Edgar Hoover verbindet Klassenneid mit sexuellem Ressentiment) (Liu 1998). Dieses Szenario wiederholte sich unlängst als Farce, als der Präsident von Taiwan am 19. März 2004 ein Attentat überlebte: denn während die Warren-Kommission Verschwörungstheorien über Kennedys Tod zu widerlegen suchte, schien das Parlament in Taiwan eher wilde Spekulationen zu ermutigen, daß es in Wirklichkeit vom Präsidenten selbst gestellt gewesen sei. Und ein Computerspiel, das im selben Jahr (zum einundvierzigsten Jahrestag des Kennedy-Attentats) erschien, bie-

tet dem Spieler die Perspektive des Todesschützen in einer detailliert recherchierten Simulation jenes Tags in Dallas. Wenn JFK-Verschwörungen nur aus einem Blickwinkel »verstanden« werden können, den Zapruder nicht sehen konnte, so bleiben jene Symptome, die sich um den Grassy Knoll gebildet haben, auf dem Niveau des Heimvideos, während Verschwörungstheorien nach 9/11 sich in im Netz ausbreiten wie ein Pilz.[4]

Wenn verschwörerisches Denken verspricht, eine uneinsichtige oder unübersichtliche Situation zu meistern, heißt das jedoch nicht, daß dies die einzig authentische populäre Reaktion auf die Realität des dezentralen Netzes darstellt (Jameson 1991: 38). Verschwörungstheorien werden allzu leicht als Gegenpropaganda vereinnahmt, und die typische Kritik kann allzu leicht in herablassende Bemerkungen über Massenkultur abgleiten (Fenster 1999: 12f.). Wahr ist jedoch, daß schon der Ursprung des Internet vor dem Beginn des Kalten Kriegs Verschwörungstheorien installiert. Sowohl Kittler als auch Virilio dokumentieren, wie Truman und Churchill in Potsdam übereinkamen, die wichtigen Erfolge der Colossi in Bletchley Park vor Stalin geheimzuhalten, und ihm statt von Computern und Nachrichtenüberwachung von einem heroischen Spion zu erzählen, einem gewissen General Werther, den die Soviets allerdings nie finden konnten. Und so belauschten die Allierten nach dem Zweiten Weltkrieg eben Moskau und Wladiswostok anstatt Berlin und Tokio (Willmott 1990). Nach diesen Anfängen in der Verbindung zwischen Abhörposten und Computerentschlüsselung umfaßt diese Vertuschung aller V-Days bald verteilte Radarinstallationen, die mit strategischen Waffensystemen per Computer verbunden sind. Es ist allerdings vielleicht ebenso plausibel, auch noch in Kittlers Schluß, daß seit 1941 Krieg der Kampf von Maschinen mit anderem Maschinen ist, am Ende Verschwörungstheorie zu sehen: denn der Paranoide versucht allenthalben, den Beginn der Symptome zu datieren, den fixierenden Moment festzuhalten, und diese Obsession kann selbst zur paranoiden Geste geraten. Die Militärgeschichte der Aufklärung allein, von Radarschirmen und Bildröhren bis hin zu integrierten Schaltkreisen und Glasfaserkabeln, ist gewiß eine unzureichende Kritik der neuen Medien, solange sie nicht zugleich auch die psychologischen Entgleisungen und Zufälle in ihre Geschichte berücksichtigt. Ein Netz oder eine relationale Datenbank kann so effektiv skalieren, daß eine willkürliche Ordnung in eine Monokausalkette zwar willkommene Reduzierung von Komplexität leisten mag, doch nur indem sie grob vereinfacht.

Es überrascht in diesem Kontext kaum, daß Paranoia und ihre Therapie schon früh als Modelle für Computerkultur herangezogen wurden. Um 1965 entstand am MIT in Cambridge, Massachusetts ein natursprachliches Experiment, das als *Eliza* oder *The Doctor* bekannt wurde und noch heute in verschiedenen Varianten von Unix verfügbar ist. Die rekursiven Muster seiner generativen Grammatik imitieren

4 »Other centuries have only dabbled in conspiracy like amateurs. It is our century which has established conspiracy as a system of thought and a method of action« (Moskovici 1987: 153).

bestimmte Phrasen, die man mit einem Psychotherapeuten assoziiert, wenn ein Patient zum Reden gebracht werden soll – eine unwiderstehliche Einladung zum Turing-Test (Weizenbaum 1966). Ungefähr zur gleichen Zeit versuchten Psychiater an der Universität Stanford, paranoides Benehmen in ein ähnliches Programm zu codieren, und schrieben *Parry* (Colby 1971; Colby 1981). Im Jahr 1973, als das ARPAnet nicht mehr als vierzig Computer in den USA umfaßte, verbanden die beiden Universitäten *Parry*, den simulierten Paranoiden aus Stanford, über das »packet-switching communications network« nach Boston über Los Angeles mit *Eliza*, dem simulierten Doktor (Cerf 1973). Die amüsanten Dialoge der beiden Programme, stolze Vorfahren der heutigen Bots und Agenten, die das Computernetz beleben und aufrecht erhalten, sind zur Legende geworden. Gewiß muß man hinzufügen, daß sowohl Paranoia als auch Psychotherapie modelliert werden konnten, weil es sich in beiden Fällen um geschlossene Systeme handelt, die am Ende ihr eigenes Verderben sind – doch andererseits ist es auch wahr, daß rekursive Muster nirgendwo so nützlich sind, als wenn es um die Entlastung des menschlichen Gehirns durch Computer geht: »Der einzige Grund, warum wir noch nicht alle Aspekte der Welt formalisiert haben«, versprach Elizas Vater, Joseph Weizenbaum, »ist daß es uns bislang an einem starken logischen Kalkül fehlte« (Weizenbaum 1984). Doch ist es diese ideologische Tendenz, die uns in instrumentelle Wiederholungsmuster der Gewohnheit und Regelmäßigkeit preßt (Fuller 1003: 93). So war Weizenbaums *Eliza* nur insofern ein Doktor, als sie in den »magischen Mantel der Wissenschaft« gekleidet schien, wie er später zugeben mußte (Weizenbaum 1984: 191). Man will glauben, daß Computer vernünftiger sein werden als wir, wenn sie endlich miteinander sprechen, doch diese Erwartung selbst ist unvernünftig. Sobald ein Verständnis unserer Medienwelt nur noch durch technische Medien möglich scheint, muß kritische Reflexion weitergehen als die paranoide »Assertitude«, daß die Macht der Medien nicht mehr lokalisiert, addressiert, oder direkt kontrolliert ist.

Der Vorteil für Verschwörungstheoriker ist, daß man vermeidet, als naiv zu gelten, indem man Verdacht hegt. Die Verbindung zwischen Bildschirm und Tastatur, Ordner und Dokument, Client und Server, Code und Compiler und so weiter zeigt sich nur als Apparat. So ist der Verdacht, wie Groys mahnt, eine unerschöpfliche Quelle der Medientheorien, da Zeichen und Bilder immer zugleich zeigen und verbergen (Groys 2000). Hinter dem Datenträger liegt Technik (Papier, Zelluloid, Silikon), hinter jener Produktionsprozesse, Elektrizität, Wirtschaft; und dahinter mag man je weiteres vermuten. Die Seiten und Lettern eines Buchs verstecken, was seine Produktion ermöglichte, der Computer verhüllt, was auf seinem Chip-Satz ruht, hinter Fernsehprogrammen vermutet man politische wie technische Programme, und so weiter – die dunkle Seite der Medien erlaubt ein endloses Rätseln. Ereignis, Biomacht, Globalisierung – von Baudrillards fröhlichen Verbrechen bis zu Hardt und Negris militanter Resignation konstruieren Medientheorien ihre Geschichten verdeckter Manipulation (Popper 1963: 341f.). Doch um diese Frankfurter Vorschule zu absolvieren, sollten Medientheoretiker Konzepte anbieten, die Kultur und Indu-

strie dann vielleicht doch nicht immer schon im Geheimbund mit dunklen Interessen wissen. Selbst wenn man annimmt, daß ein Zeichen die Bedingungen seines Erscheinen verdeckt, wird nicht jede Art der Ablenkung und Zerstreuung automatisch Blendung bedeuten (Benjamin 1969: 240). Wie produktiv paranoide Symptome sind, zeigt sich im Kino: Während Hollywood sich bereits seit langem digitaler Technologie bedient, wird sie von *Desk Set* bis zum heutigen Tag im Film ausnahmlos verteufelt. So ist es die höchste Ironie, daß die *Matrix*-Trilogie als ultimative Hacker-Fantasie als einzige in diesem Genre eine realistische Szene zu bieten hat.[5] Hier findet man keinen pickeligen Halbstarken, sondern eine erwachsene Frau, und nicht in einem neonbeleuchteten Datenmanhattan, sondern vor einem schlichten Laptop; und sie nutzt ein Programm, das tatsächlich existiert – sie testet die Sicherheit eines Stromversorgers mit »nmap« in der Kommandozeile.

Geheimniskrämer

In der Welt der vernetzten Computer ist Sicherheit durch Geheimhaltung allgemein ineffektiv. Algorithmen und Programmcode zu verbergen mag anfangs wirken, doch am Ende wird der Schleier des Geheimnisses gelüftet.
Greg Newby

Das Geheimnis besteht in der Regulierung von Mitteilung und Bewahrung. Während technische Mediennetze totale Überwachung und unmittelbare Aufklärung ermöglichen, beinhaltet ihre Struktur zugleich das kryptographische Imaginäre. Die Asymmetrie von privat und öffentlich, Verbreitung und Archivierung bedeutet, daß die soziale Macht des Geheimen anders dekodiert werden muß als es verschlüsselt wurde; Ausschluß wird im Eingeschlossenen als Exteriorität markiert. Als Shannon verkündete, daß ein System nur dann bedingungslos sicher ist, wenn seine a priori Distribution identisch mit seiner a posteriori Distribution ist, dann hieß dies, daß der sicherste Schlüssel die selbe Länge hat wie die Botschaft, die es zu verschlüsseln gilt (Shannon 1949). Daher will der Kryptograph zwischen einem absolut sicheren System und einem praktisch sicheren System unterscheiden. Und trotz hartnäckiger Gerüchte um die vermeintlich postnuklear angelegten Pläne für das Internet handelt es sich hier nicht um ein strikt militärisches Szenario (es war wohl bekannt, daß elektromagnetische Impulse einer atomaren Explosion solche Datennetze lahmlegen würden), sondern um ein praktisches System der Kompatibilität knapper Ressourcen (Hafner/Lyon 1998). Ursprungsvergessenheit ist allerdings immer ein Nebeneffekt des Mythologisierens.

5 *Desk Set* (USA 1957); *The Matrix Reloaded* (USA 2003).

Interessanterweise üben die ersten Entwürfe für ein sicheres verteiltes Netz bereits scharfe Kritik an Geheimniskrämerei, wie Paul Baran in seinem Vorschlag für ein *Distributed Adaptive Message Block Network* schreibt: »Gegenwärtige Sicherheitsbegriffe scheinen auf der Annahme zu beruhen, daß man jeder eingeweihten Person vertraut, und daß jede uneingeweihte Person ein möglicher Spion ist.« Trotz seiner hochrangigen Stellung bei der *RAND Corporation* wollte er daher keine persönliche Sicherheitsgenehmigung, da diese es ihm unmöglich machen würde, seine Forschung zu betreiben. Stattdessen forderte er öffentlich zum *Hacken* auf:

> »We are concerned lest a clever and determined enemy find an Achilles heel. As an acid test, we elicit and encourage a response from the reader who will ›don the hat of an enemy agent‹ and try to discover weak spots in the proposed implementation. Such an enemy is assumed to have a limited number of highly competent cohorts plus all the equipment he can transport. Further, it is assumed that the fundamental human inadequacies of our, or any security clearance system will permit infiltration by some at least minimal number of enemy agents who will gain a complete and detailed understanding of the workings of the system. Inasmuch as few people have ready access to the crypto keys and since the keys are changed on a short-time basis, it can be assumed that the subversive agent will generally not have access to more than a portion of the key—unless he resorts to force in obtaining the key, thereby tipping his hat.« (Baran 1964)

Dies bedeutet allerdings nicht, daß man das Spektrum des *Hacktivismus* schlicht als Erproben neuer Technologie im Test, als lose überwachte Forschung, oder als eine Art unkonventionelles Training vereinnahmen kann. Doch solange der Gesetzgeber mit dem Begriff des »nicht autorisierten« Zugangs operiert, ist niemandem wirklich gedient. Wäre es nicht besser, wenn manche ihre eigenen Computer gut genug verstünden, um sie reparieren zu können? Wäre nicht allen gedient, wenn man versuchen darf, neuen Nutzen aus den etablierten Technologien zu schlagen? Wäre es nicht produktiver, wenn das Werkzeug verbessert und kritisiert werden könnte? Die politisch naiven Annahmen, die die Schließung von Betriebssystemen und Datenträgern untermauern, entziehen der Öffentlichkeit das rudimentärste Wissen um die Möglichkeit von Kultur unter den Bedingungen digitaler Technik. So mag man Hacktivismus als kollektiven computerisierten Widerstand sehen, oder als unvermeidlichen Auswuchs derselben Tendenz zur technokratischen Geheimniskrämerei, wie Studien über die sozialen Dimensionen des Internet im allgemeinen und die Bandbreite des Aktivismus im Netz im besonderen zeigen (Lessig 1999: 36-40; Carpenter 1996). Die Gruppe organisiert sich um einen Technofetisch: Die gruppenpsychologische Bedeutung des Geheimen ist eine Beziehung zwischen Wissen und Unwissen, und in den neuesten Gadgets erkennt man die uralte, fetischistische Logik der hinausgezögerten Enthüllung (Marin 1992: 195). Wie bereits C.P. Snow bemerkte, macht die Euphorie der Geheimhaltung ebenso trunken wie die Euphorie der technischen Spielerei mit Gadgets (Snow 1961: 73; Bok 1987: 283). Nun geht Kritik

am Fetischismus meist davon aus, daß er als notwendige Illusion entlarvt werden soll, die die wahren Verhältnisse verschleiert. Doch dieses Argument ist selbst der Logik des Fetisch verhaftet, indem es die kritische Entlarvung zum letzten Fetisch macht, in einem endlosen Schleiertanz. Wenn daher Computersysteme die letzte Apotheose der Automation darstellen, deren unentrückbare Undurchsichtigkeit an Selbstverschleierung grenzt, dann schließen sie den Nutzer aller Interfaces aus und verbergen so am Ende ihr eigentliches Wissen, ihren wissenschaftlichen und kulturellen Wert, in der Illusion der Innerlichkeit – das ganze Netz als eine *black box*.

Leider begegnet man dem Hacker in der Populärkultur meist als jugendlichem Einzelgänger (Thomas 2002). Der Grund für die beliebte Analogie zwischen ödipalen Problemen und dem Erproben und Aushebeln technischer Einschränkungen ist mythologischer Art. Diese Lektüre suggeriert, daß es im Netz um die Verbindung mit lang Abwesendem geht (Rickels 1998: 191). In dieser Überschneidung von Kulturtheorie, Massenmedien und Gruppenpsychologie dient der Computerfreak oder *nerd*, dessen privilegierte Beziehung zur Technik hier fokussiert wird, als Maskottchen der Mediengesellschaft. Das Begehren nach Gleichgesinnten gestaltet sich anhand verschiedener Prothesen – Alias, Avatar, Pseudonym –, und die Verbindungen knistern unter der Statik der Hemmungen. Totemische Asexualität erlaubt eine anonyme Geselligkeit, während man *Dungeons and Dragons* spielt oder Unix und Java programmiert (McLuhan 1966: 36f.). Diese mythologisierende Lesart erlaubt drei stereotype Repräsentationen des ödipalen Begehrens im Netz: *phone phreaks* wollen eine kostenlose Verbindung in die Welt, *warez crackers* unterlaufen der Tauschwert von intellektuellem Eigentum in einer ruinösen Kultur der Gabe, und *hackers* retten jede Art von Information vor der Geheimhaltung, zu der eine zentralisierte Datenverwaltung sie zu verdammen scheint. In allen drei Versionen geht die Fantasie auf eine melancholisch-futuristische Umkehrung der Verhältnisse im coolen Metamedium der Computernetze. Andersherum diagnostiziert jedoch Žižek, daß diese Mythen des Cyberspace uns erlauben, mit solchen Phantasien zu spielen, also eine minimale kritische Distanz aufrechtzuerhalten, anstatt sie als ein dominantes Programm zu sehen (Žižek 2002: 121). Solch ödipale Konstruktionen des psychotischen Eintauchens oder der neurotischen Vermittlung sollten also nicht von der Hand gewiesen werden, ohne darauf hinzuweisen, daß sie leisten, was Mythen immer schon zu leisten vermochten: ein Umschalten von Angst auf Erzählung, und von semiotischem Spiel auf kritische Beobachtung.

Umschalten

Von Anfang an ist zu etablieren, daß der Mythos ein Kommunikationsystem ist, eine Botschaft.
Roland Barthes

In der Antinomie von lähmender Angst und motivierendem Freiraum, von Terror und Spiel, kann die mythologische Formation der öffentlichen Diskussion über Aktivismus im Netz erkennbar werden. Man mag am *Hacktivismus* gerade schätzen, was andere bedrohlich finden: eine entspannte, unorthodoxe Herangehensweise an Technologien der Kontrolle und Kommunikation. Die Zwangsherrschaft geschlossener Systeme ist am effektivsten underwandert von der Möglichkeit radikaler Lesbarkeit, die kreative Ader der Programmierer ist Füllhorn der Zukunft oder Polizeigewalt mit anderen Mitteln. Die gruppenpsychologische Wirksamkeit des Mythos ist unbestreitbar die einer sekundären Oralität.[6] Denn Mythen verbreiten sich in mündlichen Kulturen, und Schriftlichkeit kompliziert die Vertraulichkeit jeder Mitteilung (Goody/Watt 1968). Schriftlichkeit ist allerdings nicht nur für die Rekonstruktion von einer vermeintlich vorgängigen Mündlichkeit, sondern vor allem für ihre Interpretation unabdingbar (Havelock 1984). Folglich kann die Diagnose einer sekundären Oralität auf den geschwätzigen Charakter der Netzkultur ausgedehnt werden (Ong 1982). Versionenkontrolle, Authentifikation, und Datenintegrität sind nicht unter den Kernaspekten dieser Struktur: Sie ist vielmehr charakterisiert von Hörensagen, Gerüchten, und Geschichtenerzählen. Und so scheint es wie folgt: Je weiter ein Netz gespannt ist, desto niedriger seine Sättigung mit Information, und je differenzierter die Information, desto konzentierter ihre tatsächliche Verbreitung. Je mehr ein Medium Lärm mit Profit und Profit mit Lärm korreliert, auch und gerade beim höchsten Produktionswert, desto leerer wird es. Und so können militärische oder akademische Netze hohe Integrität bewahren, doch die breitere Öffentlichkeit bleibt ausgeschlossen. Kritiker des Hacktivismus mögen die Abwesenheit einer klaren Ordnung bedauern und als politisch unreife Geste abtun, was Verschwörungstheoretiker ihrerseits als Versuch begrüßen, eine Krise im Netz herbeizuführen. Auf beiden Seiten der Debatte wird jedoch vorschnell angenommen, daß es sich im Netz entweder um Gehorsam oder um Subversion handelt. Das älteste dokumentierte Beispiel einer Netzaktion war der virtuelle Sit-in des italienischen *Strano Network* im Jahr 1995 gegen die französische Regierung – ein erklärter Streik (*grève en réseau*), kein Terror.[7] Eine der bekanntesten Netzaktionen war die Modifizierung indonesischer Websites mit Aufrufen zur Befreiung Osttimors im Jahr 1998 durch portugiesische Hacker, doch handelt es sich dabei bloß um eine Art Graffiti.

6 »In nonliterate cultures the task of education could be described as putting the whole community into a formulaic state of mind« (Havelock 1963: 140); »Lengthy verbal performances in oral cultures are never analytic but formulaic« (Ong 1971: 2).

7 Tatiana Bazzichelli, http://www.ecn.org/aha/map.htm.

Die Schlagzeilen, die solche Aktionen machten, erklären nur selten politische Argumente und konstruieren lieber Phantome digitaler Selbstjustiz. Es ist gewiß nicht unzulässig, die Drohung des Cyberterror ernst zu nehmen und journalistisch aufzubereiten – aber es ist unverantwortlich, zwischen einem Sit-in oder Streik einerseits und dem Versagen einer Kette von Bankautomaten andererseits nicht klar zu unterscheiden. Es ist schlicht zynisch, Netzkunst mit Attacken auf die Stromversorgung von Krankenhäusern gleichzustellen, oder eine Kabelfernsehpanne mit dem möglichen Schaden einer Bombe zu vergleichen. Flugsicherheitsnetze sind jedoch separat von den Werbeseiten der Fluglinien, und Cyberterror mag real sein, genau wie Flugzeugentführungen – doch haben sie nichts mit Verbraucherprotesten gegen Monopolwebseiten im kommerziellen Netz gemeinsam. Solche Einkaufscomputer als »kritische Knoten« des Netzes zu bezeichnen und glaubhaft zu machen, »bösartige« Programme könnten das gesamte Internet gefährden, ist schlicht albern – denn die Einrichtung des dezentral verteilten Netzes erlaubt gerade, um einen abgeschalteten Knoten herum immer noch, über ein Dutzend verschiedener Wege, zum selben Zielpunkt verbunden zu bleiben (Gellman 2002; Weber 2004). Gewiß gehören Computer zum Arsenal des 21. Jahrhunderts, auch und gerade für militärische Aufklärung und Spionage sowie für psychologische Kriegsführung (Walters 2001: 191; Weber 2005). Doch was Hacktivismus als Reaktion auf Konflikte von Tschetschenien bis Chiapas oder von Hong Kong bis Hamburg auch immer sein mag, es hat noch keine Bomben ausgelöst und noch keine Menschenleben gekostet. Netzaktivisten sind weder Spione noch Soldaten, weder Terroristen noch pickelige Jugendliche im Keller, die ihren Allmachtsphantasien per Modem anhängen – es sind vielmehr Gruppen, die Medienaufmerksamkeit auf ihre Interessen zu leiten suchen. Ihre Demonstrationen, Sit-ins, Streiks, und Pamphlete zu kriminalisieren, bloß weil sie am offiziell sanktionierten Nutzen von vernetzten Computern als Einkaufskanal und Schreibmaschine vorbeimanövrieren, ist schlicht albern. Wenn jemand einen Computer für fünf Minuten lahmlegt, indem in jeder dieser 300 Sekunden ein Prozeß angefragt aber nicht komplettiert wird, dann ist dies weniger eine »Attacke« als eine sehr langsame Interaktion: eine Blockade, die eher einem Streikposten ähnelt als dem vermeintlichen Cyberterror.[8] Netzaktionen haben bislang immer vermieden, größeren Schaden anzurichten – allein schon aus taktischen Gründen, denn die Sichtbarkeit der Aktion (gleich ob als Netzkunst oder als politischer Protest) hängt entscheidend davon ab, daß genügend Zeugen mitbekommen, daß hier eine bestimmte Adresse im Netz zeitweise unverfügbar oder verändert ist. Letzten Endes ist der Mythos eine Rückkehr zu den ältesten Strukturen und Programmen, die zwar auf analytischem Denken beruhen, aber die Mehrheit in ein formelhaftes Denken zwängen. Doch die Insistenz auf dem Verbergen von Code und anderer di-

8 Zum »Cyber Storm« der Amerikanischen Homeland Security, siehe http://www.dhs.gov/xlibrary/assets/prep_cyberstormreport_sep06.pdf, sowie http://www.siliconvalley.com/security/ci_8126437.

gitaler Datenschreibe wird die Adressaten immer neu motivieren, diese Apotheose der Automaten zu unterbrechen und zu interpretieren.

Literatur

Baran, Paul (1964): »On Distributed Communications: IX Security, Secrecy, and Tamper-Free Considerations«, Memorandum RM-3765-PR. Santa Monica: RAND Corporation, http://www.rand.org/publications/RM/RM3765/RM3765.chapter5.html.

Benjamin, Walter (1969): »The Work of Art in the Age of Mechanical Reproduction«. In: Illuminations. New York: Schocken Books, S. 217-251.

Bok, Sissela (1982): Secrets: On the Ethics of Concealment and Revelation. New York: Pantheon.

Brecht, Bertolt (1967): »Der Rundfunk als Kommunikationsapparat«. In: Gesammelte Schriften, Frankfurt a.M.: Suhrkamp, Bd. 18, S. 117-134

Carpenter, Brian (1996): »Request for Comments: 1958, Architectural Principles of the Internet«. Network Working Group, http://www.ietf.org/rfc/rfc1958.txt.

Castells, Manuel (1996): The Rise of Network Society. Oxford, UK: Oxford University Press.

Cerf, Vint (1973): »Parry Encounters the Doctor«. In: Datamation, July, S. 62-64.

Colby, Kenneth Mark (1971): »Artificial Paranoia«. In: Artificial Intelligence, 2, S. 1-25

Colby, Kenneth Mark (1981): »Modeling a Paranoid Mind«. In: Behavioral and Brain Sciences, 4, S. 515-560

Curry, Richard O. (Hrsg.) (1972): Conspiracy: The Fear of Subversion in American History. New York: Holt, Rhinehart and Winston.

Cyber Security Research and Development Act (November 27, 2002), http://www.house.gov/science/cyber/hr3394.pdf.

Dean, Jodi (2000): »Webs of Conspiracy«. In: Andrew Herman und Thomas Swiss (Hrsg.), The World Wide Web and Contemporary Cultural Theory. London: Routledge.

Denning, Dorothy E. (1990): »Concerning Hackers Who Break into Computer Systems«. Paper presented at the 13th National Computer Security Conference, Washington, DC, 1.-4. Oktober, http://www.cs.georgetown.edu/~denning/hakkers/Hackers-NCSC.txt.

Denning, Dorothy E. (1995): »Postscript to ›Concerning Hackers Who Break into Computer Systems‹«. 11. Juni, http://www.cs.georgetown.edu/~denning/hakkers/Hackers-Postscript.txt.

Denning, Dorothy E. (2000): »Hacktivism: An Emerging Threat to Diplomacy«. In: Foreign Service Journal, September, http://www.afsa.org/fsj/sept00/Denning.cfm

Denning, Dorothy E. (2003): »Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy«. In: John Aquilla und David Ronfeldt (Hrsg.), Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica: RAND National Defense Research Institute, S. 239-288.

Dominguez, Ricardo (2004): Activism/Activismo/Ativismo, e-misférica 1, no. 1, http://hemi.nyu.edu/journal/1_1/activism.html.

Dornseif, M. (2003): »Government Mandated Blocking of Foreign Web Content«. In: Jan von Knop (Hrsg.), Security, E-Learning, E-Services: Proceedings of the 17. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf: DFN, S. 617-648.

Dyson, Esther (1998): »The End of the Official Story«. In: Brill's Content Online, July/August, S. 50-51.

Eunjung Cha, Ariana (2005): »US Lab Simulates Terrorist Attacks«. In: Wall Street Europe, July 5, S. A3.

Fenster, Mark (1999): Conspiracy Theories: Secrecy and Power in American Culture. Minneapolis: University of Minnesota Press.

Fuller, Matthew (2003): Behind the Blip: Essays on the Culture of Software. New York: Autonomedia, 2003.

Gellman, B. (2002): »Cyber-Attacks by Al Qaeda Feared«. In: Washington Post, 27. Juni, S. A01.

Goody, Jack und Ian Watt (1968): »The Consequences of Literacy«. In: Jack Goody (Hrsg.), Literacy in Traditional Societies. Cambridge, UK: Cambridge University Press, S. 27-69.

Gordon Don E. (1981): Electronic Warfare: Element of Strategy and Multiplier of Combat Power. Oxford: Pergamon Press.

Grenier, Richard (1992): »On the Trail of America's Paranoid Class«. In: The National Interest, Spring, S. 84.

Groys, Boris (2000): Unter Verdacht: Eine Phänomenologie der Medien. München: Carl Hanser.

Gunkel, David (2001): Hacking Cyberspace. Boulder: Westview.

Hafner, Katie und Matthew Lyon (1998): Where Wizards Stay Up Late: The Origins of the Internet. New York: Touchstone.

Harmon, Amy (1997): »NASA Flew to Mars for Rocks? Sure«. In: New York Times, 20. Juli, S. 4E.

Havelock, Eric A. (1963): Preface to Plato. Cambridge, MA: Harvard University Press.

Havelock, Eric A. (1984): »The Orality of Socrates and the Literacy of Plato«. In: E. Kelly (Hrsg.), New Essays on Socrates. Washington, DC: University Press of America, S. 67-93.

Hofstadter, Richard (1965): The Paranoid Style in American Politics. New York: Knopf

Jameson, Fredric (1991): Postmodernism, or The Cultural Logic of Late Capitalism, London: Verso.

Johnson, George (1983): Architects of Fear. Los Angeles: Tarcher

Jordan, Tim und Paul Taylor (2004): Hacktivism and Cyberwars: Rebels with a Cause? New York: Routledge 2004.

Latour Bruno (1999): Pandora's Hope: Essays on the Reality of Science Studies. Cambridge, MA: Harvard University Press.

Lessig, Laurence (1999): Code, and Other Laws of Cyberspace. New York: Basic Books.

Liu, Catherine (1998): »Conspiracy (Theories)«. In: South Atlantic Quarterly, 97/2 (Spring), S. 80-99.

Loeb, Vernon (1998): »NSA Admits to Spying on Princess Diana,« Washington Post, 12. December, S. A13.

Mann, Michael (1986): The Sources of Social Power, Bd. 1: A History of Power from the Beginning to AD 1760. Cambridge, UK: Cambridge University Press.

Marin, Louis (1992): Lectures traversières. Paris: Albin Michel.

McCullagh, Declan (2003): »Cyberterror and Professional Paranoiacs,« CNETnews.com, 21. März, http://news.com.com/Cyberterror+and+professional+paranoiacs/2010-1071_3-993594.html

McLuhan, Marshall (1966): Understanding Media: The Extensions of Man. New York: Signet.

Melley, Timothy (2000): Empire of Conspiracy: The Culture of Paranoia in Post-War America. Ithaca: Cornell University Press.

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

Moscovici, Serge (1987): »The Conspiracy Mentality«. In: Carl F. Gramm und Serge Moscovici (Hrsg.), Changing Conceptions of Conspiracy. New York: Springer.

Ong, Walter J. (1971): Rhetoric, Romance and Technology. Ithaca: Cornell University Press.

Ong, Walter J. (1982): Orality and Literacy. London: Methuen.

Pias, Claus (2002): »Der Hacker«. In: Eva Horn und Stefan Kaufmann (Hrsg.), Grenzverletzer. Berlin: Kadmos, 248-270.

Pipes, Daniel (1997): Conspiracy: How the Paranoid Style Flourishes and Where It Comes From, New York: The Free Press

Popper, Karl (1963): Conjectures and Refutations: The Growth of Scientific Knowledge. London: Routledge.

Pratt, Ray (2001): Projecting Paranoia: Conspiratorial Visions in American Film. Lawrence: University Press of Kansas.

Rickels, Laurence (1998): »Cryptology«. In: Roberta Kevelson (Hrsg.), Hi-Fives: A Trip to Semiotics. New York: Peter Lang, S. 191-204.

Sandberg Jared und Thomas Hayden (2000): »Holes in the Net: What to Worry about Next«. In: Newsweek CXXXV, no. 8 , S. 47-49.

Shannon, Claude (1949): »Communication Theory of Secrecy Systems«. In: Bell Technical Journal, 28 (Oktober), S. 656-715.

Snow, C.P. (1961): Science and Government. Cambridge, MA: Harvard University Press.

Spiegel Online, 7 April 2001, http://www.spiegel.de.

Thomas, Douglas (2002): Hacker Culture. Minneapolis: University of Minnesota Press.

Treverton, Gregory F. (2003): Reshaping National Intelligence for an Age of Information. Cambridge University Press.

Vegh, Sandor (2002): »Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking«. In: First Monday, 7/10, http://www.firstmonday.org/issues/issue7_10/vegh/index.html.

Vegh, Sandor (2003): »Classifying Forms of Online Activism«. In: M. McCaughey und M. Ayers (Hrsg.), Cyberactivism. New York: Routledge, S. 71-95.

Walters, G.J. (2001): Human Rights in an Information Age. Toronto: University of Toronto Press.

Weber, Sam (2004): »Target of Opportunity: Networks, Netwar, and Narratives«. In: Grey Room, 15 (Frühjahr), S. 6-27.

Weber, Samuel M. (2005): Targets of Opportunity: On the Militarization of Thinking. New York: Fordham University Press.

Weizenbaum, Joseph (1966): »ELIZA: A Computer Program for the Study of Natural Language Communication between Man and Machine«. In: Communications of the ACM, 6/3 (March).

Weizenbaum, Joseph (1984): Computer Power and Human Reason: From Judgment to Calculation. London: Pelican.

Willmott, H.P. (1990): The Great Crusade: A New Complete History of the Second World War. New York: Free Press.

Wray, Stefan: »Aspects of Hacker Culture,« http://www.du.edu/~mbrittai/4200/socio_criminal.htm

Wray, Stefan: »Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics,« http://www.nyu.edu/projects/wray/wwwhack.html

Žižek, Slavoj (2002): »Is It Possible to Traverse the Fantasy in Cyberspace?«. In: Elizabeth Wright (Hrsg.), The Žižek Reader. Oxford, UK: Blackwell, S. 102-124.