

## Hacker

A: qurşān aš-sifra. – E: hacker. – F: hacker.

R: chaker. – S: hacker. – C: heike 黑客

Mit dem Computer entsteht im Kapitalismus eine neuartige Formation von High-Tech-Akteuren, die sich in ironischer Untertreibung ihrer Virtuosität einfach nur »H« nennen (LEVY 2001, 23). – Sie eignen sich die neuen Produktivkräfte durch deren Weiterentwicklung und oppositionelle Umfunktionierung an und verknüpfen dabei Arbeit, Lebensweise, Ethik und Sport zu Gegenkulturen, die gegen die Bürokratien von Konzernen und Staat rebellieren. Die Regelverletzungen und Grenzüberschreitungen, die für den H konstitutiv sind, bewegen sich am Rande der Kriminalität und können u.U. auch diese Grenze überschreiten. Umgekehrt können private und öffentliche Sicherheitsagenturen H-Kompetenz rekrutieren.

*Hack* – so heißt u.a. auch »ein Lohnschreiberling, der auf seiner Schreibmaschine Textzeile auf Textzeile herunterhämert« (FREYERMUTH 1998, 30) – bedeutet ab den 1960er Jahren für Elektronikbastler und Programmierer an US-Universitäten eine Problemlösung mit drei Merkmalen: »*Einfachheit*: die Aktion muss einfach, aber wirkungsvoll sein. *Meisterschaft*: in ihr steckt raffiniertes technisches Wissen. *Unerlaubtheit*: die Aktion ›ist gegen die Regeln‹.« (TAYLOR 1999, 15; vgl. TURKLE 1984, 279f) Mit ihrer Verknüpfung von technischer Virtuosität und Regelverstoß (bis hin zur Sozialrebellion) trugen die H der 60er und 70er Jahre entscheidend zur Entwicklung neuer Programmiersprachen, des PC und des Internet bei (RAYMOND 1999, 231f; GRÖNDAHL 2000, 52f). In der Folge entstehen sich voneinander abgrenzende H-Kulturen, die in unterschiedlichen Feldern aktiv sind und an die Arbeitskultur der H-Pioniere anzuknüpfen suchen.

1. *Digitale Grenzüberschreitung*. – Mit überbetrieblicher Computervernetzung spitzt sich der Gegensatz zu, dass in die gleiche Technologie, mit der komplexes Herrschaftswissen höchster Geheimhaltungsstufe, aber auch besonders schutzwürdige medizinische Daten lokal konzentriert werden, die Möglichkeit eingebaut ist, dieses Wissen von beliebigen Punkten außerhalb des Betriebes zu inspizieren – und zu verändern. Hier bildet sich als »eine der neuen Individualitätsformen des Neoliberalismus« (HAUG 1999, 185) der H als digitaler Grenzgänger aus. Er verwandelt sich vom subalternen Unbefugten in den digitalen Doppelgänger eines ›legalen‹ Systemnutzers (indem er sich z.B. dessen Passwort beschafft). Der H kann sich durch seine Netzexplorationen Identitäten der Nutzer vieler unterschiedlicher Systeme besorgen, seine Macht zu anonymer Grenzüberschreitung

wächst. Roland ECKERT u.a. (1991) zeigen, wie sehr schon weltweite »Datenreisen«, bei denen Daten nur inspiziert werden, H faszinieren. Es gibt aber auch H, die erfolgreich nach dem Passwort des ›Superusers‹ bzw. ›Sysadmin‹ suchen (er verwaltet das System, hat Zugriff auf höchst sensitive Dateien, legt fest, wer auf diese zugreifen darf etc.). Sofern ein H sich technisch dazu qualifiziert hat, kann es ihm gelingen, den legalen Sysadmin aus dem System auszusperrern: »Es ist für jeden H der Höhepunkt, die totale Kontrolle über das andere Netz erreicht zu haben.« (169) Da sich der H vielleicht mehrere Passworte besorgt hat, wird der Sysadmin dessen Zugriffsmöglichkeiten womöglich nicht sofort eliminieren, legt es vielmehr darauf an, den digitalen Weg zur H-Person selbst zu ermitteln. Es gibt Zweikämpfe, die sich über Monate hinziehen, deren Darstellung (STOLL 1989) ein eigenes Literaturgenre begründet.

Die Individualitätsform des H als »Systemeindringling« reproduziert sich im transnationalen High-Tech-Kapitalismus auf immer höherer technischer Stufenleiter, da es zwischen H und Programmierern der Software-Industrie ein Fließgleichgewicht wechselseitigen Lernens gibt. Neue Programme füllen zwar manche alte Sicherheitslücken, enthalten aber auch neue – nicht zuletzt deswegen, weil es für die Industrie profitlicher ist, ein neues Produkt schnell, gegebenenfalls auch mit Sicherheitsmängeln zu verkaufen. Sind sie dann durch H-Aktionen zum öffentlichen Skandal geworden, werden die Programme zu ihrer Behebung zwar ausgeliefert, aber z.B. zeitverzögert in den Betrieben installiert (TAYLOR 1999, 66f). Folglich können auch weniger qualifizierte H große Erfolge erzielen, während qualifiziertere H kompliziertere Systemschwächen analysieren. Dazu sind nach Auffassung mancher Informatiker gerade H aufgrund ihres praktisch-experimentellen Herangehens besonders geeignet (76).

Manche H wechseln in die Sicherheitsabteilungen von Firmen über, werden Firmengründer oder ›Samurai‹-H mit einem spezifischen Berufsethos, die sich für Aufträge mieten lassen, die illegal, aber legitim sind (RAYMOND 1998, 396); auch kriminelle Organisationen suchen H anzuwerben. Die Individualitätsform des H, die sich durchs leidenschaftliche Explorieren fremder Systeme ausbildet, ist in ganz unterschiedliche politische Projekte einbindbar.

2. *Software-/Datenpiraterie*. – Vor dem Internet-Zeitalter entwickelte sich bereits eine ›Cracker‹- und ›Demo‹-Szene, deren Gruppen sich einen Sport daraus machen, möglichst als erste den Kopierschutz neu herausgekommener Computerspiele und Programme zu ›knacken‹ und ihnen »graphisch und

soundtechnisch anspruchsvolle ›Intros‹ voranzustellen (ECKERT u.a. 1991, 263), um sie dann kostenlos zu verteilen. Das Internet gibt dieser Szene neues Gewicht, denn es stehen Milliardenumsätze auf dem Spiel. Elektronischer Handel bedeutet, Produkte wie Musik, Bücher, Filme, Programme etc. zwecks digitaler Distribution in Digitalprodukte zu verwandeln. Deren Herstellung ist aufwendig – sie zu kopieren kostet fast nichts. Also werden sie und entsprechende Abspiegelgeräte zu Digitalwaren umgebaut (z.B. durch Verschlüsselung), die nur Käufer nutzen können. 180 Platten- und Technologiefirmen schlossen sich 1998 zur ›Secure Digital Music Initiative‹ (SDMI) zusammen, ihre Technologie wurde schon in der Entwurfsphase von Hackern geknackt. Manche Formen von besonders raffiniertem Kopierschutz (z.B. ›Dongles‹) können »auf der ganzen Welt vermutlich nur acht oder neun Hacker« (McCANDLESS 2001, 48) brechen. Arbeitsresultat und Tarnname des erfolgreichen H und seiner Gruppe verbreiten sich übers Internet.

Wiederherstellung allgemeiner Nutzbarkeit von Digitalwaren ist Ziel der H als ›Cracker‹. Aber H preschen auch dem Kapital voraus und etablieren eine neue Form massenhafter Distribution digitaler Produkte im Internet (z.B. ›Napster‹); sie bahnen damit u.U. neue Wege, die später profitlich gangbar sind und einzelne H dazu bringen, ihre Fähigkeiten zu kommerzialisieren. Die ›Cracker‹-Formation reproduziert sich aber immer wieder neu durch die – formationsspezifisch erfolgreiche – allgemeine Arbeit, vor allgemeiner Nutzung ›geschützte‹ Produkte allgemeiner Arbeit zu entfesseln oder noch ungefesselte Produkte zu nutzen, bevor ihnen die Fesseln der Warenform angelegt werden (OHM 2000, 731f).

Angesichts des Erfolgs der H interveniert der Staat. Der in den USA 1998 verabschiedete Digital Millennium Copyright Act (DMCA) stellt die Modifikation von »technologischen Maßnahmen, die den Zugang zu Copyright-geschützten Werken kontrollieren«, unter Strafe (bis zu 5 Jahre Gefängnis). Die Gesetzgebung in Europa zielt in die gleiche Richtung. – Es entstehen neue Widersprüche, da nicht nur H, sondern auch informatischer Erforschung bestimmter Verschlüsselungstechniken Repression droht.

3. *Viren-Produktion.* – Computerviren wurden von Jugendlichen in den USA schon Anfang der 80er Jahre entwickelt; 1986 verbreitet sich der erste Virus weltweit; ab 1987 bildet sich eine Szene von Virenprogrammierern (›Vx-Szene‹); Ende der 80er Jahre gibt es bereits Firmen, die Antiviren-Programme herstellen. Auch wenn die meisten Viren »nur in der

Szene« zirkulieren und »nur ein geringer Prozentsatz jemals die Rechner Unbeteiligter« infiziert (RÖTTIGERS 2001, 63), liegt in der Virenproduktion der Übergang vom Sport zur Kriminalität besonders nahe. Nach der Schätzung von Sarah GORDON gab es 1994 weltweit ca. 100 Personen, rund 20 aktive Gruppen, die ständig neue Viren schreiben. Der Wettbewerb in und zwischen den Gruppen ist zentrales Motiv der Virenprogrammierer, von denen aber einige – anonym – Viren ›freilassen‹. Diese Brutalität wird durch das Internet potenziert, da ein erfolgreich zirkulierender Virus bei Millionen von Nutzern Informationen unwiederbringlich zerstören kann.

Das Internet ist auch das Medium, aus dem ein technisch noch wenig qualifizierter H heutzutage komplette Virenbaukästen herunterladen kann; es fungiert damit als Multiplikator des gefährlichen Talents der kleinen Zahl von Virenprogrammierern. Dass jugendliche H, die selber Computer benutzen, sich zerstörerische Viren beschaffen und sie kursieren lassen, mag mit formationsspezifischen Momenten des Prozesses zusammenhängen, in dem H sich in die ›Subjektform« H hineinarbeiten. Aneignung technischer Handlungsfähigkeit geschieht oft als »Zerspielung« (WULFF 1987) von Wirklichkeit: einerseits erwerben werdende H durch PC- und Internet-Nutzung schon früh ein enormes technisches und auch kooperatives *know-how*, also auf Wirklichkeit bezogene Handlungsfähigkeiten, andererseits verändert die Welt der Computerspiele, so wie sie die Spieleindustrie als Wirklichkeitsersatz thematisch und dramaturgisch bauen lässt, die Wirklichkeitswahrnehmung. Auch das Einschleichen in fremde Rechnernetzwerke, der Kampf mit dem Sysadmin, das Zerstören von Daten, die er verwaltet, ist als eine Art Fortführung von Computer-Kampfspielen in der Art von ›Reality-TV‹ zu fassen. In der Kinder- und Jugendliteratur gibt es einen – nicht unbedingt illusionären – Vorgriff aufs Eingreifen junger H, der Jagd und Kampf gegen Destraktion koppelt: sieben 10-16 Jahre alte Cyberkids kooperieren per Internet über alle Kontinente hinweg gegen einen Virenverbreiter (Balan 1999). – Für die staatlichen Akteure, die H-Aktionen mit dem Strafrecht bekämpfen wollen, ergibt sich das Dilemma, dass viele H Kinder oder Jugendliche und insofern nicht strafmündig sind.

4. *Software-Entwicklung.* – H, die sich bewusst auch so nennen und damit an die Tradition der technologisch bahnbrechenden H der 1960er und 70er Jahre anknüpfen, schließen sich in einem Kernbereich des transnationalen High-Tech-Kapitalismus, der Entwicklung des Betriebssystems *Linux*, auf Basis unbezahlter Arbeit zu einem global vernetzten

Gesamtarbeiter zusammen, der mehr Personen umfasst als die größte Softwarefirma Microsoft. Für die perspektivische Überlegenheit dieser H-Kollektive vom Typ Linux werden vielerlei Gründe genannt (RAYMOND 1999). – Vorstellbar ist, dass diese Form nicht-kapitalistischer Softwareentwicklung sich weltweit durchsetzt, da Softwareentwicklung sich zu einer Form allgemeiner Arbeit entwickelt hat, die Formen der Selbstvergesellschaftung benötigt, die mit kapitalistischem – auch radikal modernisiertem – Produktionsregime unverträglich sind. Für die Linux-H ist nur die von ihnen gefundene neue Produktionsweise mit ihrem Produzentenstolz vereinbar, macht sie als Produzenten produktiv, da die Programme (und die Namen ihrer Autoren) im Internet veröffentlicht und kritischer Weiterentwicklung zugänglich werden. – Allerdings wird der transnational operierende High-Tech-Kapitalismus in seiner Existenz nicht bedroht, wenn Produktivkraftentwicklung in wichtigen Bereichen nicht-kapitalistisch stattfindet.

5. »Hactivismus«. – Der Begriff entsteht durch Zusammenziehung der Worte »Hacken« und (politischer) »Aktivismus«, ist also Nutzung technischer Fähigkeiten der H für politische Projekte. Eines der Ziele ist es, das Medium Internet gegen Privatisierungs- und sonstige Abschottungsstrategien als öffentlichen Raum zu nutzen, also die Versammlungs- und Demonstrationsfreiheit, wie sie vor Heraufkunft des Internet für öffentliche Räume erkämpft worden ist, aufs Internet als elektronischen öffentlichen Raum zu übertragen, indem man strukturelle Analogien zu *sit-ins* und Blockaden konstruiert. Hier ist neben politischen Vernetzungsfähigkeiten eben auch netzwerktechnische Kompetenz vonnöten. Die Begeisterung für politische Projekte zieht, so Stefan WRAY (1998), zusehends technisch orientierte H in ihren Bann. So organisierte eine Gruppe, das *Electronic Disturbance Theatre* (EDT), zur Unterstützung des Freiheitskampfs der Zapatistas virtuelle Sit-Ins gegen Websites der mexikanischen Regierung: wer sich daran beteiligt, wählt mittels eines Programms alle paar Sekunden den Zielsever an und hinterlässt dort eine kritische Botschaft. Tun dies genügend Surfer gleichzeitig, so ist er von der Außenwelt nicht mehr adressierbar. Eine von EDT inspirierte Gruppe in Großbritannien sind die Electro-Hippies. Sie lehnen klandestine Aktionen ab und arbeiten an einer Weiterentwicklung von Protestformen, bei denen es nicht darauf ankommt, möglichst schnell den Zielsever lahmzulegen, sondern möglichst viele zu spontaner Beteiligung zu aktivieren. – Inwieweit überhaupt die Störung von Kommunikationsflüssen im Internet politisch sinnvoll ist, da sich ja auch die Gegenseite

dieser Waffe bedienen kann, wird zwischen Hacktivist\*innen kontrovers diskutiert.

Im Gegensatz zum Hacktivismus ist es Ziel des Cyberterrorismus (Dorothy DENNING 2001), durch Netzwerkattaken Katastrophen herbeizuführen und Menschen zu töten. Am Konzept eines Cyberkriegs, der eben dies vermag, arbeitet seit 10 Jahren das US-Militär; eine Reihe weiterer Staaten arbeitet mittlerweile an diesem Modell der Kriegsführung.

6. *H-Ethik(en)*. – Prozesse der Selbstvergesellschaftung, der Umleitung aggressiver Arbeitsenergien junger H auf zivilgesellschaftlich vertretbare Projekte, werden durch H-Verbände wie dem Chaos Computer Club (CCC) angestoßen. Die H-Kongresse des CCC etwa enthalten immer »Sessions«, in denen H, die in der H-Welt angesehen sind, an »Script-Kiddies« appellieren, »richtige H« zu werden, – z.B. nicht die Institutionen Andersdenkender mit Viren zu attackieren. (In diese Richtung zielt auch einschlägige Jugendliteratur, etwa Bruce BALANS Reihe *Cyber.KDZ*). – Der CCC wurde Anfang der 1980er Jahre gegründet und fungiert heute als Dachverband, in dem sich viele H in Deutschland zusammengeschlossen haben. Er hat eine von H weithin anerkannte Ethik erarbeitet, deren erster Imperativ lautet: »Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.« – Diese Ethik ist unter den gegebenen gesellschaftlichen Verhältnissen zugleich ein Manifest, kapitalistisch-staatliche Geheimhaltung zu durchbrechen.

Zentrales Thema der Kongresse des CCC ist es, technische Schwachstellen von Computernetzwerken aufzudecken, was nur durch praktisch-experimentelles Vorgehen möglich ist, und die Entdeckungen der Öffentlichkeit zu präsentieren. Aufgedeckt werden dadurch auch mögliche Einbruchstellen von Computerkriminalität, die solche Schwachstellen nutzt und immer mit der Verschwiegenheit der betroffenen Betriebe und Behörden rechnen kann. Insofern ist die Aufdeckungsarbeit des CCC und der unter seinem Dach organisierte H gesellschaftlich unentbehrlich. – Die Terrorattacke des 11. September 2001 schuf den Anlass für Einführung neuer Formen elektronischer Bürgerüberwachung. Hier ergibt sich ein neues zivilgesellschaftlich wichtiges Aufgabenfeld für den CCC und die in ihm sich sammelnden H.

BIBLIOGRAPHIE: B.BALAN, *Cyber.KDZ 1*, Hamburg 1999; ders., *Cyber.KDZ 2*, Hamburg 2000; ders., *Cyber.KDZ 3*, Hamburg 2001; D.DENNING, »Cyberwarriors. Activists and Terrorists Turn to Cyberspace«, in: *Harvard International Review*, 23. Jg., 2001, H. 2, 70-5; R.ECKERT u.a., *Auf digitalen Pfaden. Die Kulturen von Hackern, Programmierern, Crackern und Spielern*, Opladen 1991; G.S. FREYERMUTH, *Cyberland. Eine Führung durch den High-*

*Tech-Underground*, Hamburg 1998; S.GORDON, »The Generic Virus Writer«, in: *Proceedings of the International Virus Bulletin Conference*, Jersey, Channel Islands 1994, 121-138; B.GRÖNDAHL, *Hacker*, Hamburg 2000; ders., »The Script Kiddies Are Not Alright«, in: Medosch/Röttgers 2001, 143-52; W.F.HAUG, *Politisch richtig oder Richtig politisch. Linke Politik im transnationalen High-Tech-Kapitalismus*, Hamburg 1999; S.LEVY, *Hackers. Heroes of the Computer Revolution* (1984), New York 2001; D.McCANDLESS, »Warez World«, in: Medosch/Röttgers 2001, 35-51; CCC (Chaos Computer Club), *Die Hackerethik* (o.O. u. J.); A.MEDOSCH u. J.RÖTTGERS (Hg.), *Netzpiraten. Die Kultur des elektronischen Verbrechens*, Hannover 2001; C.OHM, »Hacker – das Ethos der neuen Kämpfe im Internet-Zeitalter«, in: *Argument* 238, 42. Jg., 2000, 720-40; E.S.RAYMOND, *The New Hacker's Dictionary*, 3. A., Cambridge 1998; ders., *The Cathedral & the Bazaar. Musings on Linux and Open Source by an Accidental Revolutionary*, Peking-Cambridge 1999; J.RÖTTGERS, »Sie lieben uns.txt.vbs«, in: Medosch/Röttgers 2001, 53-72; P.A.TAYLOR, *Crime in the Digital Sublime*, London 1999; *Telepolis, Elektronische Zeitschrift*, www.heise.de/tp; S.TURKLE, *Die Wunschmaschine. Vom Entstehen der Computerkultur*, Reinbek 1984; C.STOLL, *Kuckucksei – Die Jagd auf die deutschen Hacker, die das Pentagon knackten*, Frankfurt/M 1989; S.WRAY, »Die Umwandlung des Widerstands der Maschinenstürmer in einen virtuellen Widerstand – Die Herstellung eines World Wide Web des elektronischen zivilen Ungehorsams«, in: *Telepolis*, 5. Mai 1998; E.WULFF, »Zementierung oder Zerspielung. Zur Dialektik von ideologischer Subjektion und Delinquenz«, in: W.F.Haug, H.Pfefferer-Wolf (Hg.), *Fremde Nähe. Festschrift für Erich Wulff*, Hamburg-Berlin/W 1987, 171-212.

CHRISTOF OHM

⇒ allgemeine Arbeit, Aneignung, Destruktivkräfte, Entwicklung, Gegenmacht, Gegenöffentlichkeit, Gesamtarbeiter, hochtechnologische Produktionsweise, immaterielle Arbeit, Individualitätsform, Internet, Macht, Neoliberalismus, Privateigentum, Produktivkräfte/Produktionsverhältnisse, Selbstbestimmung, Sicherheit, Spiel, Subjekt, subversiv, Technikentwicklung/technische Revolutionen, Zapatismus