Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260

Herausgegeben von Stefan Schumacher und Jan W. Meine

Meine Verlag – Wissenschafts-, Sach- und Fachbuchverlag, Magdeburg

Eine Geschichte der Hackerkultur - Subkultur im Digitalen Zeitalter

Jens Holze

Aus Sicht der Bildungsforschung können Medien essentieller Katalysator für unser Selbst- und Weltbild sein. Der Beitrag argumentiert am Beispiel der Hackerkultur, dass konkrete Ausprägungen von Medienstrukturen dem Denken der Menschen und damit den Werten der Kultur entstammen, durch die sie erschaffen wurden. Im Kontext eines modernen Sicherheitsbegriffs scheinen die neuen sozialen Räume des Cyberspace auch zur Herausforderung für die gesamte Gesellschaft zu werden.

Zitationsvorschlag: Holze, Jens (2012). Eine Geschichte der Hackerkultur – Subkultur im Digitalen Zeitalter. Magdeburger Journal zur Sicherheitsforschung, Band 1, 2012, S. 179–188.

http://www.wissens-werk.de/index.php/mjs/article/viewFile/122/115

Einleitung

Unsere gegenwärtige Medienwelt befindet sich in einem revolutionären Wandel. Zumindest wird das überall mit Vehemenz diagnostiziert (Tapscott & Williams 2006), vor allem in den Medien selbst. Vieles stehe dabei auf dem Spiel: etablierte Geschäftsmodelle, die Art wie wir Informationen bekommen und filtern, unser Selbstverständnis, unsere Aus- und Weiterbildungsmöglichkeiten, unsere Jobs, unsere Sicherheit und damit unser Verständnis von Gesellschaft. Für viele scheint der Wandel plötzlich eingetreten zu sein und ist somit Symptom einer radikal beschleunigten Welt. Das Internet, so meint man, sei doch erst knapp 20 Jahre alt – gemeint ist natürlich eigentlich das WWW – und hat trotzdem schon weltumspannende Ereignisse auf wirtschaftlicher und politischer Ebene verursacht oder zumindest beeinflusst, vor denen sich niemand verschließen kann.

Doch wenn man die kulturellen Wurzeln insbesondere der Entstehung des Internet näher betrachtet, dann sind die Konflikte und Veränderungen, denen wir uns heute gegenübersehen nicht besonders überraschend und auch nicht plötzlich eingetreten. Kein modernes Medium, und es sei angemerkt, dass dieser Begriff die Möglichkeiten des Internet nur unzureichend beschreibt, entsteht losgelöst von einer Kultur und den vorherrschenden gesellschaftlichen Verhältnissen.

Ich betrachte die folgenden Phänomene vor dem Hintergrund einer neuen Theorie der Medienbildung (Jörissen & Marotzki 2009), die den veränderten Medienwelten Rechnung trägt und konstatiert, dass Medien nicht nur allgegenwärtig sind sondern auch zentralen Einfluss auf Bildung, im Sinne der Entwicklung eines individuellen Selbst- und Weltverhältnisses, nehmen. Sie beschreibt nicht den Aspekt des Kompetenzerwerbs, um mit den neuen Medientechnologien umgehen zu können, sondern komplexe Phänomene der Orientierung in der Welt, die Jörissen und Marotzki als „Bildung 1“ bezeichnen und die in medialen Strukturen stattfinden. Gemeint sind damit kulturell konstruierte Sichtweisen auf die Welt, die uns Handlungsmuster ermöglichen und die wir in früher Kindheit erlangen. Trifft das Individuum auf eine andere Konfiguration von Weltsicht (z.B. eine fremde Kultur) und stellt die eigene Weltsicht zur Disposition, besteht die Möglichkeit für Bildungsprozesse. In komplexerer Form kann das auch zur Modifizierung des eigenen Selbstbildes führen („Bildung 2“), wenn beispielsweise die eigenen kulturellen Wurzeln reflektiert und auf die eigene Identität bezogen werden. Medien allgemein und die Neuen Medien im Besonderen spannen nun Räume auf, in denen Bildungsprozesse möglich sind, was nicht bedeutet, dass sie zwangsläufig stattfinden müssen. Im sogenannten Cyberspace sind etablierte Formen der Kommunikation und andere realweltliche Strukturen zunächst nicht vorhanden, andere, medienspezifische Formen sind entstanden.

Dieser Beitrag soll einen kurzen historischen Einstieg in die Entwicklung der Hacker- und Netzkultur beginnend mit den 1950er Jahren bieten und im Anschluss daran die heute breit aufgestellte Subkultur der Hacker sowie daraus abgeleiteter Kulturgruppen beschreiben, die maßgeblich an der sogenannten digitalen Revolution und der Entwicklung des für uns heute ubiquitären Netzes beteiligt waren. Es soll argumentiert werden, dass technische und soziale Aspekte digitaler Medien eng verwoben sind und dem Wertesystem der Pioniere des Netzes entstammen. Insbesondere soll der Blick dabei auf Bildungsaspekte des Netzes gerichtet werden, denn

während das Netz einerseits seine Struktur aus der Gesellschaft bekommen hat, wirkt es durch seine neuen digitalen Bildungsräume auch wieder auf sie zurück.

Ursprünge des Hackertums

Wenn man Steven Levy (1984) und seinem Buch „Hackers - Heroes of a Computer Revolution" glauben darf, begann alles mit einen gewissen Peter Samson im Herbst 1958, frisch gebackener Student am Massachusetts Institute of Technology. Neben den üblichen Kursen interessierte er sich auch für den Tech-Model-Railroad-Club (TMRC), einen Club von Modellbaubegeistern am MIT, der in eigenen Räumen eine riesige Modelleisenbahnanlage aufgebaut hatte. Die Mitglieder des Clubs teilten sich grob in zwei Fraktionen auf. Da gab es zum einen die „Messer und Pinsel"-Abteilung, in der man sich für historische Loks und realistische Szenerie interessierte. Sie erbauten und pflegten alles, was an der Oberseite der Anlage zu sehen war, abonnierten Modellbauzeitschriften und veranstalteten Exkursionen zu historischen Zugfahrten. Die andere Fraktion beschäftigte sich eher mit der Unterseite der Modellanlage. Sie entwarfen ein komplexes System aus Signalen, Schaltungen und Stromkreisläufen, das die Anlage erst zum Laufen brachte. Wie besessen modifizierten und verbesserten die Mitglieder dieser Fraktion „das System" kontinuierlich, wobei es nicht selten komplett die Funktion einstellte. Bei diesen Leuten herrschte die Annahme vor, dass man das System in allen Einzelheiten durchschauen und verstehen müsse, um seine Funktion zu begreifen. Und sie bastelten durchaus auch einfach nur so herum, ohne damit ein konstruktives Ziel erreichen zu wollen. Wenn jemand ein bestimmtes Projekt – ohne Ziel aber mit wildem Enthusiasmus – verfolgte, nannte man das einen „hack". Daher wundert es kaum, dass auch sie es waren, die Mitglieder der Signals-and-Power-Gruppe, die sich auf dem gesamten Campus nach Möglichkeiten umsahen, um ihre Hände an ein technisches Novum genannt Computer legen zu können.

Das war in der Tat nicht so einfach, denn Computer waren teuer, groß und nicht ansatzweise mit dem zu vergleichen, was wir heute üblicherweise auf oder unter Schreibtischen finden können. Vielmehr waren Computer, wie der IBM 704 und 709 am MIT, im Grunde eine etwas komplexere Version eines „Systems", wie man es an der Modellbahnanlage fand und nur zu sehr spezifischen Aufgaben nutze. Darüber hinaus arbeitete man nicht direkt an der Maschine, sondern übergab seine in Lochkarten gemeißelten Programme den „Priestern", wie die Bediener der Maschinen auch genannt wurden. Diese ließen dann, so es ihnen genehm war, das Programm am Computer laufen und übergaben irgendwann später den Ausdruck mit den Ausgaben dem Programmautoren. Hatte man fehlerhafte Anweisungen benutzt, die zu einem falschen Ergebnis geführt oder gar das Programm schlicht hatten abstürzen lassen, ging der Kreislauf von vorn los. Das genügte den Hackern vom TMRC nicht, sie wollten direkt an die Maschine und sehen wie sie arbeitete, denn genau wie beim „System" erhofften Sie sich auf diese Weise tiefe Erkenntnisse über die Funktion des Apparates. Daraus entwickelte sich ein reger Austausch mit der „Priesterschaft" des Computers. So versuchten die Hacker beispielsweise in mühevoller Kleinarbeit dem Computer das Schachspielen beizubringen. Aber die Regeln im Computerlabor, insbesondere, dass niemand die Maschine anfassen oder daran herumfummeln konnte, und das ständige Warten auf die Ergebnisse frustrierte die Hacker über alle Maßen. Sie

spielten Streiche mit den überengagierten Priestern, deren Autorität ihnen kontinuierlich im Weg stand. Erst als ein neuer Computer, der TX-0, dem MIT übergeben wurde, bot sich endlich die Möglichkeit, direkt Hand anzulegen. Hier konnte man sein Programm über einen langen Flexowriter-Streifen direkt in den Rechner füttern und, weil man zu bestimmten Zeiten den Rechner allein reservieren konnte, sogar interaktiv Programme bearbeiten während man am Gerät war. Die TMRC-Hacker merkten schnell, dass nachts niemand Computerzeit in Anspruch nahm und versammelten sich fortan nächtens im Labor um den Tixo, wie der Rechner auch genannt wurde. In ihren Sessions, an denen ihnen oft mehr lag als am regulären Studium, entwickelten Sie Programme, mit denen die Arbeitsgeräusche des Rechners nach Musik klingen sollten, die römische in arabische Ziffern umrechneten und allerlei andere Dinge taten, für die man die teure und seltene Technik sonst nie nutzen würde.

Die Hackerethik und weitere Entwicklungen

Aus dieser engen Gemeinschaft von Hackern und den Problemen, die ihrem Interesse entgegenstanden, entwickelte sich die erste Ideologie, die in Levys Buch dokumentiert wurde. Die sogenannte Hackerethik verweist ganz deutlich auf die Herausforderungen und die Geisteshaltung der ersten Hacker. Sie wird auch heute noch von großen Teilen der Subkultur aufrecht erhalten, insbesondere von den sogenannten „White-Hats“ wie sich die ‚guten‘ Hacker selbst nennen. Es wird aber auch darauf Wert gelegt, dass es sich nicht im engeren Sinn um Regeln handelt sondern eher um Richtlinien mit geringerer Verbindlichkeit.

1. Der Zugang zu Computern und allem, was einem zeigen kann, wie diese Welt funktioniert, sollte unbegrenzt und vollständig sein.
2. Alle Informationen müssen frei sein.
3. Mißtraue Autoritäten - fördere Dezentralisierung
4. Beurteile einen Hacker nach dem, was er tut und nicht nach üblichen Kriterien wie Aussehen, Alter, Rasse, Geschlecht oder gesellschaftlicher Stellung.
5. Man kann mit einem Computer Kunst und Schönheit schaffen.
6. Computer können dein Leben zum Besseren verändern.

(Übersetzung ccc.de, nach Levy 1984)

Aus diesen ersten Versuchen und Experimenten entwickelte sich in den folgenden Jahrzehnten eine Strömung des Hackertums, die sich mit der fortschreitenden Verfügbarkeit von Computern und durch die beginnende Vernetzung verstärkt an diversen Universitäten und Forschungseinrichtungen verbreitete. Computer wurden kleiner und günstiger, waren aber weiterhin nicht für den Privathaushalt vorgesehen.

Erst 1974 war mit dem Altair der erste Heimcomputer verfügbar. Parallel dazu versammelten sich enthusiastische Ingenieure und Bastler im Bay Area Amateur Computer Users Group Homebrew Computer Club (kurz Homebrew Computer Club), um mit dem Altair oder selbstgebauten Rechnern herumzuspielen. In dieser Gruppe versuchte man nun den Gedanken des kreativen Umgangs mit Technik, der bei den MIT Hackern primär mit Software zu tun hatte, auf die Hardware zu übertragen. Einige Helden wie Steve Wozniak würden später die nächste Generation von Heimcomputern erschaffen und damit den PC in die Heime normaler Menschen tragen. Darauf folgten Pioniere wie Nolan Bushnell

mit Atari oder in den 1980ern Roberta und Ken Williams mit ihrer Firma Sierra On-Line, die einige der frühen erfolgreichen Computerspiele zunächst als Spielautomaten, später dann für PCs produzierten. Daraus wiederum entstand eine weitere Computeraffine Subkultur, die heute allgegenwärtig ist. All diese speziellen Gemeinschaften verband das Ziel, mit Technologie neue, bisher unbekannte Dinge zu tun. Viele der Ideen und der damaligen Ideologien sind in soziotechnische Systeme eingeflossen, deren Auswirkungen und Konsequenzen wir heute beobachten können.

Aus der beginnenden Vernetzung von Computern bildeten sich ebenfalls neue Gruppierungen. So entstand etwa die erste virtuelle Community The WELL (für Whole Earth ‚Lectronic Link) aus einer generellen Geisteshaltung der Gegenbewegung, die zuvor schon Grundlage für den von Mitgründer Steward Brand ab 1968 herausgegebenen Whole Earth Catalog gewesen war (Rheingold 1994) Diese spezielle Gemeinschaft, die lange Zeit als Prototyp für Online-Communities galt, entstammt also durchaus einer speziellen Subkultur und war insofern ideologisch vorgeprägt. Es gibt viele Parallelen zwischen der Hippiebewegung in Amerika und der Hackerbewegung, deren Wechselwirkung zu technologischen Revolutionen im Silicon Valley und später weltweit beigetragen hat.[1]

Die ersten Schritte ins das Netz kamen also zu großen Teilen aus Subkulturen und so blieb auch das Netz selbst ein Hort für Randgruppen und Subkulturen, die sich hier eigene Räume schaffen konnten. Erst mit der Öffnung des Netzes für die Öffentlichkeit und dem Beginn der kommerziellen Nutzung bekam die generelle Öffentlichkeit überhaupt Interesse am Internet und speziell am World Wide Web. Es dauerte knapp 20 Jahre, bis das Web ein tatsächliches Massenphänomen werden konnte. Doch die Ideale der ersten Netznutzer, der Hackerbewegung, der amerikanischen Gegenkultur und der Hippiebewegung sind in der DNA des Netzes von Beginn an vorhanden gewesen, weshalb das Netz, so wie es heute existiert, durch seinen technischen Aufbau Bedingungen vorgibt, die durchaus große Auswirkungen haben und die zum Teil mit etablierten Vorstellungen der realen Welt brechen. So macht sich das Netz im Grunde nichts aus Nationen und Grenzen, beachtet folglich nur schwer Unterschiede in Gesetzgebung und überwindet kulturelle Barrieren. Auch die Aversion gegen Autorität ist in den Strukturen des Netzes und zum Teil seiner Administration verblieben, es bedarf besonderer Anstrengung, sie im Netz zu simulieren. Diese Aspekte nachträglich wieder zu implementieren ist schwierig und funktioniert nicht immer, gleichzeitig ist es instinktiv der erste Schritt von Menschen in einer unbekannten Umgebung, bekannte Strukturen übernehmen zu wollen. Daraus entstehen Spannungen, die heute allgegenwärtig geworden sind.

Die Hackerbewegung und Gegenkultur fand jedoch nicht nur in Amerika statt, weshalb 1981 in Deutschland der Chaos Computer Club (CCC) als Organisation von Hackern gegründet wurde.

Hacking, das wird schon durch die historische Rekonstruktion deutlich, impliziert immer auch eine potentielle Auseinandersetzung mit Autoritäten. Die frühen Hacker aus dem akademischen Rahmen waren vom Erkenntnisdrang getrieben und Aspekte wie Sicherheit, private Daten, Datenschutz

1 (vgl. dazu die BBC Podcast Reihe über Social Networking http://www.bbc.co.uk/podcasts/series/shsn) und die Dissertation „New edge : technology and spirituality in the San Francisco Bay Area“ https://openaccess.leidenuniv.nl/handle/1887/17671)

etc. existierten im digitalen Kontext noch nicht. Schon in den 1970ern war beispielsweise Phone Phreaking - also das Hacken des Telefonnetzes - in Amerika verbreitet. Dafür wurden einfache Schaltungen konstruiert (die sogenannten blue boxes), die die Steuerungstöne für Schaltanlagen der Telefonkonzerne replizieren konnten. Mit den richtigen Frequenzen konnte man sich so gratis Telefongespräche erschleichen. Die erste gemeinsame gewinnbringende Unternehmung von Steve Jobs und Steve Wozniak, die später Apple gründen sollten, war das Bauen und Verkaufen von selbstentwickelten „blue boxes", die sie aus Material im Wert von 40 Dollar herstellten und dann für 150 Dollar von Tür zu Tür verkauften (Isaacson 2011, S. 29). Das Blue-Boxing wurde ein verbreitetes Hobby, es entstand eine relativ große Szene der „phone phreaks", die auch andersfarbige Boxen, wie beispielsweise die „red box" zum kostenlosen Telefonieren an Telefonzellen, entwickelte. Bis heute ist das Telefonnetz (inklusive Diensten wie Voicemail, Mobilfunk etc.) ein bedeutendes Feld für Hackeraktivität weltweit. Erst dadurch wurden Hackeraktivitäten auch zu kriminellen Akten im großen Stil (Sterling 1993). Während einige Phreaker und Hacker lediglich durch die technische Herausforderung motiviert waren, verfolgten andere ausschließlich ihren persönlichen Vorteil. Darin besteht die moralische Dichotomie der Hacker, während ‚guten' White-Hats Sicherheitslücken aufdecken um Systeme dadurch sicherer zu machen, suchen ‚böse' Hacker Sicherheitslecks, um sie kriminell auszunutzen, sich Daten oder Dienste zu erschleichen und womöglich gegen Geld zu veräußern. Beides widerspricht zunächst nicht der Hackerethik, die in ihrer ursprünglichen Form keine moralische Komponente hat.

Der CCC wurde 1989 mit einem Fall von Cyberspionage in Verbindung gebracht, bei dem Hacker im Auftrag des KGB in US-amerikanische Computersysteme eindrangen und Daten entwendeten. Erst aufgrund dieser Ereignisse ergänzte man die Hackerethik durch zwei weitere Punkte, die im Grunde das Mission Statement des CCC sind:

1. Mülle nicht in den Daten anderer Leute.
2. Öffentliche Daten nützen, private Daten schützen

(siehe www.ccc.de/hackerethics)

Der Begriff des Hackers aus den 1960er wandelte sich in der öffentlichen Wahrnehmung, heute gilt er als Sammelbegriff für Computerkriminelle und trotz Bemühungen der Szene sich von diesem Anhang frei zu machen und alternative Begriffe zu finden, hat sich dieses Verständnis lediglich verfestigt.

Die Hackerkultur entwickelte sich kontinuierlich weiter, bis Anfang der 1980er Jahre eine Art Spaltung stattfand. Computerhardware war verbreitet und relativ günstig verfügbar, aber die Softwarehersteller gingen dazu über ihre Programme insbesondere auch Betriebssysteme, mit immer restriktiveren Auflagen in Form von Lizenzen zu veröffentlichen. Obwohl man viel Geld für die Software zahlte, stand es einem nicht frei, sie nach eigenem Ermessen zu verwenden. So veröffentlichten die Anbieter Programme auch nicht mehr im Quelltext, den fähige Programmierer zuvor nutzen konnten um ein Programm zu verbessern, zu überarbeiten oder im Falle von Fehlern selbstständig zu reparieren. Diese Möglichkeiten wollten sich die Firmen selbst vorbehalten, sicherlich auch, weil mit dem Support noch zusätzlich Geld zu verdienen war, aber auch, um die Herstellung von Klonen und Kopien ihrer Soft-

ware zu erschweren. Für Richard Stallman, zu dieser Zeit laut Levy der letzte wahre Hacker am MIT, widersprach diese Praxis den Idealen der Hackerethik (Levy 1984). Er war überzeugt, dass jedermann in der Lage sein sollte zu verstehen, wie Computer funktionieren. Dies sei nicht möglich, wenn man nicht herausfinden könne, wie die Software funktioniert, wenn man nicht Einblick in den Quelltext nehmen könne. Aus diesem Gedanken heraus gründete Stallman die Free Software Foundation und begann freie Software zu schreiben, mit dem Ziel alle Werkzeuge frei anzubieten, die ein Programmierer brauchte, um neue Software zu schreiben. Dazu gehörten unter anderem ein Editor, Compiler für Programmiersprachen und natürlich ein Betriebssystem. Besonders schwierig war all das, weil Stallman beabsichtige, ein Unix-kompatibles System zu bauen, dass aber völlig unabhängig vom kommerziellen Unix sein sollte. Insbesondere konnte Stallman, auch nach jahrelanger Arbeit mit vielen Helfern, keinen funktionierenden Betriebssystemkernel entwickeln. Erst Anfang der 1990er Jahre veröffentlichte auf der anderen Seite der Welt Linus Torvalds eine erste Version seines Linux-Kernels, den er mit den GNU-Tools von Stallman zu programmieren begonnen hatte, auf einem FTP-Server und forderte andere auf, sich an dem Projekt zu beteiligen.

Daraus entwickelte sich das erste freie Betriebssystem „GNU/Linux“, welches mittlerweile in verschiedenen Paketen kostenlos oder kommerziell vertrieben wird. Nach diesem Vorbild sind noch viele andere Softwareprojekte entstanden, heute gibt es eine massive Bewegung von freier Software, die auch Open-Source-Software genannt wird. (Raymond 1999c) Die Infrastruktur des Internet basiert zum größten Teil auf Open-Source Programmen wie dem Webserver Apache, der wiederum meist auf einem Linux Betriebssystem läuft. Viele andere Programme wie Bürosoftware, Webbrowser, Email-Software oder Grafikbearbeitung gibt es ebenfalls als freie Software, was meist auch bedeutet, dass sie im Internet kostenlos heruntergeladen werden kann. Möglich ist dies, weil Programmierer in ihrer Freizeit daran arbeiten und jeder, der Interesse hat und programmieren kann, sich den Quellcode besorgen und selbst die Software verändern kann. Kosten entstehen dafür meist keine und falls doch (z.B. wenn ein Programmierer Vollzeit an einem Projekt arbeiten will) gibt es Möglichkeiten dies über Werbung, Spenden oder Sponsoring zu finanzieren. Die Funktion der Hacker wird in diesem Zusammenhang auch schlicht als effektive Form der Softwareentwicklung verstanden und ist damit ein weniger ideologisches Konstrukt, was im kommerziellen Bereich leichter durchsetzbar ist (Torvalds et al., 2001).

Was lässt sich vor dem ausgeführten Hintergrund der Hacker- und Netzkultur nun über ein modernes Verständnis von Sicherheit sagen? Zunächst eine kurze Herleitung: Im Verständnis von Thomas Hobbes und seiner Staatstheorie aus dem 17. Jahrhundert, schließen alle Menschen untereinander einen Vertrag, mit dem sie freiwillig ihre individuelle Freiheit einschränken und dem Staat (bei Hobbes noch einem Souverän) das Machtmonopol übertragen, damit dieser sie gegen gewaltsame Angriffe von innen und außen schützt. Sicherheit bedeutete hier Sicherheit für Leib und Leben, die Möglichkeit sich nicht vor anderen Menschen fürchten zu müssen und dadurch zu Leistungen, die das schlichte Überleben übersteigen, überhaupt fähig zu sein. Ohne den Staat herrsche, laut Hobbes, der „Krieg aller gegen alle“ (Hobbes 1986).

Diese grundlegende Sicherheit ist auch heute noch ein Teil der Aufgabe des Staates, aber mittlerweile gehört dazu einiges mehr. Neben dem Recht auf Leben, definiert z.B. das deutsche Grundgesetz noch andere unveräußerliche Menschenrechte und zudem sehen wir es als Aufgabe des Staates an, seinen Bürgern eine gewisse Qualität von Leben, also eine gewisse materielle Absicherung, soziale Teilhabe und anderes mehr zu ermöglichen. Unser Verständnis von Sicherheit ist also kulturell verankert.

Doch aus modernitätstheoretischer Sicht haben wir mit neuen Unsicherheiten zu kämpfen, die sich generell aus der wachsenden Freiheit ergeben. Dazu gehört beispielsweise die Auflösung von Raum und Zeit. Technologie hat dazu beigetragen, dass Menschen Strecken zwischen verschiedenen Orten schneller und schneller zurücklegen konnten, dafür wurde die Zeit standardisiert und ihre Bedeutung von der Natur (Tag und Nacht, Jahreszeiten) entkoppelt (Giddens 1996, Sennett 2000).

Mittels elektronischer Medien hat sich dieser Prozess abermals beschleunigt, Informationen sind raum- und zeitlos verfügbar, die lang etablierten naturalistischen Strukturen der vormodernen Gesellschaft sind zur Ordnung unserer Existenz also nicht länger verfügbar. Das führte zu gesamtgesellschaftlichen Revolutionen wie der Industrialisierung, durch die tradierte Handlungsmuster wie beispielsweise Geschlechterrollen oder die traditionelle Konstruktion von Familie zur Disposition gestellt wurden und nicht länger verpflichtend waren. Während früher der Beruf der Eltern und ihre soziale Stellung die Möglichkeiten der Kinder diktierten (und Partnerschaften als geschäftliche Vereinbarung gehandhabt wurden), obliegen diese grundlegenden Weichenstellungen heute in vielen Kulturen nur der eigenen Entscheidung. Wir haben viele Optionen aber immer weniger Wegweiser.

Es ist dieser Verlust von Sicherheit, der die gesellschaftliche Herausforderung in der Moderne darstellt. Der technologische Fortschritt ist maßgeblich mit ihr verknüpft, befördert er doch das Wegfallen des Traditionellen, das Vermischen verschiedener vormals getrennter Kulturen und fordert oder schafft gar neue Strukturen. Bei jeder neuen Technologie entstehen daher erneute Grabenkämpfe zwischen Befürwortern, die die neuen Möglichkeiten begrüßen und Gegnern, die aufs Neue den Untergang prophezeien. Das gesamte 20. Jahrhundert ist geprägt durch diese wiederkehrenden Auseinandersetzungen. Auch dass insbesondere die Jugend neuen Technologien gegenüber aufgeschlossen ist und sie meist bereitwillig für ihre Weltkonstruktion integriert ist ein deutliches Muster. Das Hackertum ist eine Subkultur, die die digitale Welt als etwas Erstrebenswertes betrachtet und davon ausgehend sie selbst gestaltet hat. Dabei wurden vorhandene Wertvorstellungen in soziotechnologische Strukturen implementiert. In einer Welt, die zutiefst von Menschen vorrangig über Medien erfahren wird, wurden damit dem digitalen Zeitalter erste Impulse verliehen. Gleichzeitig hat die Hackerkultur aber aus ihrem Forscherdrang heraus auch die Problemfelder kultiviert, denen wir heute gegenüberstehen. Datenschutz, Datensicherheit, Cyberkriminalität, Cyberterrorismus, all diese Konzepte entstammen ebenfalls der Hackerbewegung und wurden erst durch ihre Aktivitäten - positiv wie negativ - gesellschaftlich relevant und damit auf die Tagesordnungen etablierter Institutionen gesetzt. Heute sehen wir, wie daraus resultierende Gegensätze zum Problem werden. Die Hackerkultur selbst mag

weiter als Subkultur gelten, auch wenn sie an Bedeutung gewonnen und dem Mainstream näher gerückt ist. Sie hat durch mediale Artefakte mitgeholfen eine digitale Welt zu kreieren (ein Fork der realen Welt, wenn man so will), die erst einige Zeit parallel existierte und nun langsam mit den Problemen einer unvermeidlichen Integration konfrontiert wird. Daraus entsteht zunächst eine erhöhte Unsicherheit im Sinne der Modernitätstheorien, weil etablierte Strukturen herausgefordert werden und sich neue herausbilden. Konzepte wie Privatheit aber auch Transparenz in politischen und gesellschaftlichen Prozessen und damit verbundene gesellschaftliche Werte werden derzeit neu verhandelt. Mit einem Verständnis von Bildung im Sinne einer „Herstellung von Bestimmtheit und Ermöglichung von Unbestimmtheit" (Marotzki 1990) ist es daher für die Erhaltung der Sicherheit zunächst notwendig genau zu verstehen und bewerten zu können, worin die mögliche Unsicherheit besteht. Möglicherweise befindet sich auch das Konzept der Sicherheit als eine Wertvorstellung in einem Prozess der Neugestaltung.

Ausblick

Ausgehend von der historischen Rekonstruktion der Hackerkultur und den Überlegungen zu Sicherheit und Unsicherheit in der Moderne wird klar, dass die generelle Herausforderung auch für sicherheitspolitische Ziele zunächst im Verstehen der neuen Phänomene und ihrer Strukturen liegt. Dabei ist zu berücksichtigen, dass bestimmte Wertvorstellungen dem Netz zugrunde liegen und durch eine noch näher zu bestimmende Netzkultur weitergetragen werden. Womöglich handelt es sich in Teilen um klassische Generationskonflikte, die hier zum Tragen kommen. Aus bildungstheoretischer Sicht scheint es wichtig festzustellen, dass auch die sogenannten „virtuellen Räume" Teil der realen Welt sind. Sie sind aus dem Denken und Handeln von Menschen entstanden und sie beeinflussen das Denken und Handeln von Menschen. Insofern sind auch ihre Auswirkungen real, sie finden nicht in einer Parallelwelt statt.

Noch sind Begriffe wie Cyberkriminalität oder Cyberkrieg schnell bei der Hand, um Phänomene zu beschreiben, die möglicherweise nur aufgrund ihrer Unbekanntheit bedrohlich wirken. Es ist falsch, diesen Phänomenen keine Aufmerksamkeit zu widmen, es ist aber ebenso problematisch, sie mit alten Kategorien erfassen zu wollen, ohne kritisch zu hinterfragen, ob diese zutreffend sind. Auch wenn Werte neu verstanden und ihr Schutz neu organisiert werden muss, ist Vorsicht geboten. Betrachten wir die populären Dienste im WWW, die sozialen Netzwerke, Suchmaschinen und Dienstleister mit weltweiter Präsenz, dann stellen wir fest, dass noch immer viele von ihnen in oder in der Nähe des Silicon Valley zu finden sind und damit in direkter Tradition der beschriebenen Hacker- und Gegenkultur stehen. Ähnliches gilt für diverse prominente Vordenker des digitalen Zeitalters. Die Strukturen der dort entwickelten digitalen Welt tragen Grundideen und Bruchstücke eines konkreten Weltverständnisses in sich, die damit weitergegeben werden können. Einige davon lassen sich relativ einfach in vorhandene kulturelle Kontexte integrieren. Dazu zählt beispielsweise die Idee Wikipedia, welche in Deutschland sehr starke Unterstützung gefunden hat. Andere, wie der Datenschutz, der in Deutschland anders verstanden wird als beispielsweise in den USA, fordern sie heraus. Die Erhaltung der Sicherheit darf dabei nicht leichtfertig mit dem Bewahren etablierter Strukturen und Institutionen gleichgesetzt werden. Gleichsam bildet der Cyberspace eben keine unabhängige,

von der restlichen Welt getrennt funktionierende Virtualität sondern gehört immer mehr zur gängigen Realität. Das Besondere am Netz wird alltäglich werden, so wie zuvor die Druckerpresse oder Elektrizität und mit diesem Wissen müssen wir uns fragen, wie unsere Welt morgen aussehen soll.

Autoreninfo

Jens Holze ist wissenschaftlicher Mitarbeiter am Institut für Erziehungswissenschaft der Otto-von-Guericke Universität Magdeburg. Er beschäftigt sich innerhalb des noch jungen Forschungszweiges der Medienbildung in Bereichen wie Internet Studies oder Digital Game Studies mit den Auswirkungen digitaler Medien auf Bildung und Gesellschaft.

Literaturverzeichnis

Giddens, Anthony. Konsequenzen Der Moderne. 7 ed. Suhrkamp Verlag, 1996.

Hobbes, Thomas. Leviathan. Reclam, 1986.

Isaacson, Walter. Steve Jobs. Simon & Schuster, 2011.

Jörissen, Benjamin und Winfried Marotzki. Medienbildung - Eine Einführung. Stuttgart: UTB, 2009.

Levy, Steven. Hackers: Heroes of the Computer Revolution. 1st ed. Anchor Press/ Doubleday, 1984.

Marotzki, Winfried. Entwurf einer strukturalen Bildungstheorie. Weinheim: Deutscher Studien Verlag, 1990.

Raymond, E. "The Cathedral and the Bazaar." Knowledge, Technology & Policy 12, Nr. 3 (1999): 23–49. (a)

Raymond, E.S. "A Brief History of Hackerdom." DiBona, Ockman & Stone, Open Sources, unter: www. tuxedo. org/~ esr/ writings/cathedral-bazaar/hacker-history/ (erste Version 1992), 1999. (b)

Raymond, E.S. The Revenge of the Hackers. In: Open Sources: Voices from the Open Source Revolution. Sebastopol, CA.: O'Reilly & Associates (1999): 207-19. (c)

Rheingold, Howard. Virtuelle Gemeinschaft. Soziale Beziehungen im Zeitalter des Computers. Addison-Wesley, 1994.

Sennett, Richard. Der Flexible Mensch. btb Verlag, 2000.

Sterling, Bruce. The Hacker Crackdown: Law and Disorder on the Electronic Frontier. Bantam, 1993.

Tapscott, Don und Anthony D. Williams. Wikinomics : How Mass Collaboration Changes Everything. New York: Portfolio, 2006.

Torvalds, Linus, Pekka Himanen und Manuel Castells. The Hacker Ethic. New edition ed. Vintage, 2001.