

# 1

## Technik und Kontext

### Grundlagen Datennetze

Die einfachste Form der Datenübertragung stellt eine Punkt-zu-Punkt-Verbindung dar. Dabei sind zwei Rechner über ein Trägermedium (z. B. ein Kabel oder eine Funkfrequenz) miteinander verbunden. Die in digitaler Form (Bits) repräsentierten Botschaften werden durch Modems (zusammengesetztes Wort aus Modulator-Demodulator) in eine für die Übertragung geeignete Signalform umgewandelt. In Datennetzen wie dem Internet handelt es sich grundsätzlich immer um Zweiwegkommunikation. Jede Übertragung beinhaltet die drei Schritte, Verbindungsaufbau, Verbindungskontrolle und Verbindungsabbau. Bis vor kurzer Zeit gehörte das charakteristische Pfeifen der Modems beim Verbindungsaufbau zu den lieb gewonnenen (wenn auch manchmal störenden) Begleiterscheinungen der Datenkommunikation. Die Modems müssen sich miteinander synchronisieren, d. h. eine gemeinsame Trägerfrequenz, Signalform und Schrittgeschwindigkeit einhalten. Um den Verlust von Informationen durch Übertragungsfehler zu vermeiden, muss es einen Mechanismus zur Fehlerkorrektur geben.

Ein wichtiges Merkmal eines Trägermediums ist dessen Übertragungskapazität. Diese ist abhängig von der verwendeten Bandbreite, d. h. dem Frequenzbereich, in dem die Signale übertragen werden. Je größer die Bandbreite, desto größer ist die Zahl der Informationen, die pro Zeiteinheit übertragen werden können. Die Bandbreite wird in Hertz (Hz) bzw. kHz, MHz oder GHz angegeben. Die Übertragungsgeschwindigkeit wird in Kilobits pro Sekunde (kbps, Mbps etc.) angegeben, ebenso wie die Kanalkapazität. Durch verschiedene Formen der Kanalkodierung kann bei gleicher Bandbreite die Kanalkapazität vergrößert werden.

Wenn die Übertragung in beide Richtungen gleichzeitig erfolgen kann, handelt es sich um eine Duplex-Verbindung, wenn nur in einer Richtung übertragen werden kann, nennt man es eine Simplex-Verbindung, halb-duplex, wenn die Übertragungsrichtung wechseln kann. Erfolgt die Übertragung in beide Richtungen mit gleicher Übertragungsrate, so handelt es sich um eine symmetrische Verbindung, ansonsten um eine asymmetrische.

Die Regeln, nach denen diese Vorgänge zwischen Sender und Empfänger ablaufen, werden Protokolle genannt. Diese steuern die Datenkommunikation, die Verarbeitung der Botschaften in Signale und umgekehrt. Wir kennen Protokolle aus der ganz normalen menschlichen Kommunikation. Wenn sich Kommunikationspartner implizit an die gleichen Protokolle halten, wie z. B. zuzuhören, wenn der Partner spricht, oder nachzufragen, wenn man etwas nicht verstanden hat, dann funktioniert die Kommunikation zumindest auf dieser grundsätzlichen »technischen« Ebene (ob wir einander deshalb auch »verstehen«, ist eine andere Frage). Auf der Basis ähnlicher Prinzipien regeln Protokolle die technische Kommunikation.

## **Datennetze**

Wenn nun mehr als zwei Teilnehmer an ein Kommunikationssystem angeschlossen sind, wird aus der Datenstrecke ein Datennetz. In Datennetzen geschehen die gleichen Vorgänge wie die oben beschriebenen, es kommen jedoch noch einige hinzu. Da es mehrere Teilnehmer gibt, müssen diese adressierbar sein, d. h., es muss klar sein, wer mit wem »spricht«, und die Daten müssen den Weg zum Adressaten finden. Die Berechnung des besten Wegs, den Daten in einem Computernetz von einer Quelle zu einem Ziel über mehrere Zwischenstationen nehmen, nennt man Wegelenkung (engl. »routing«; in der Folge wird meist der englische Begriff verwendet, der sich auch in der deutschen Umgangssprache eingebürgert hat), und Maschinen, welche diese Aufgabe übernehmen, heißen Router. Da sich in einem Netz mehrere Kommunikationspartner ein Trägermedium teilen, aber nicht alle gleichzeitig senden und empfangen können, muss es Regeln für die gemeinsame Nutzung des Mediums geben, so genannte Vielfachzugriffsprotokolle.

Ein wichtiges Unterscheidungsmerkmal zwischen verschiedenen Netztypen ist die Art, wie die Leitungen genutzt werden. Das Telefonnetz ist ein Leitungsvermittlungsnetz. Für die Dauer einer Sitzung steht

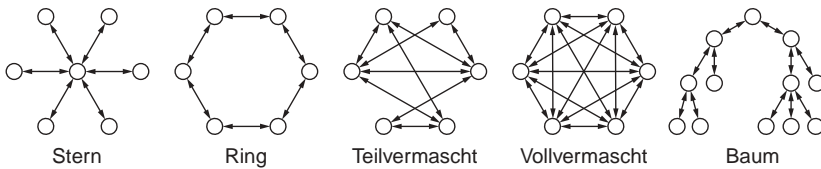
den Teilnehmern eine Leitung exklusiv zur Verfügung. Das Internet hingegen ist ein Paketvermittlungsnetz. Die zu übertragende Information in binärem Code wird in Blöcke unterteilt. Diese nennt man Pakete oder synonym dazu auch Datagramme. Neben dem zu übertragenden Inhalt enthält jedes Datagramm auch einen Header (Vorspann), in dem u. a. der Absender und die Adresse eingetragen sind.

Datagramme bewegen sich durchs Netz, indem sie gemeinsam mit anderen Datagrammen von einer Vermittlungsstelle zur nächsten weitergeleitet werden. Eine Verbindung besteht dabei immer nur von einer Vermittlungsstelle zur nächsten, jedoch nicht für die gesamte Übertragungsstrecke von der Quelle zum Ziel. Man spricht deshalb von Paketvermittlungsnetzen, die verbindungslose Protokolle benutzen. Die Pakete bewegen sich autonom durch das Netz und Pakete eines Absenders können unter Umständen auf unterschiedlichen Wegen zum Ziel kommen. Durch Paketvermittlung ist es möglich, dass z. B. auf einem transatlantischen Kabel Datagramme von Tausenden Nutzern (mehr oder weniger) gleichzeitig transportiert werden. Internetpioniere wie Vint Cerf betonen, dass Paketvermittlung eine wesentlich effizientere Nutzung eines Trägermediums darstellt. Cerf hat den leitungsvermittelten Verkehr einmal damit verglichen, dass man für eine Fahrt von New York nach L.A. für einen Wagen einen kompletten Fahrstreifen reserviert. Der Paradigmenwechsel vom leitungsvermittelten zum paketvermittelten Verkehr bildete in der Vergangenheit die wahrscheinlich singulär wichtigste Quelle des Missverständnisses zwischen den Telefongesellschaften und der Internetkultur. Allerdings sind die Grenzen heute weniger eindeutig, denn erstens benutzen inzwischen auch die Telekoms Paketvermittlung – und zwar hauptsächlich für ihre überregionalen Glasfaserstrecken –, während es zweitens im verbindungslosen Internet Protokolle gibt, die virtuelle Verbindungen auf der Anwendungsebene simulieren – so zum Beispiel bei Video-Conferencing oder Voice-over-IP (Internettelefonie).

## **Netzwerktopologien**

Ein wichtiges Unterscheidungsmerkmal zwischen Netzen ergibt sich aus dem Vorhandensein verschiedener Netzwerktopologien. Netze kann man abstrakt als Graphen darstellen, die aus Punkten und Linien bestehen. Die Punkte bezeichnet man als Knoten, die sowohl Vermittlungsstellen als auch Endgeräte sein können, die Linien stehen für Verbindungen, in der Fachsprache auch Ränder (engl. »edges«) genannt. Als

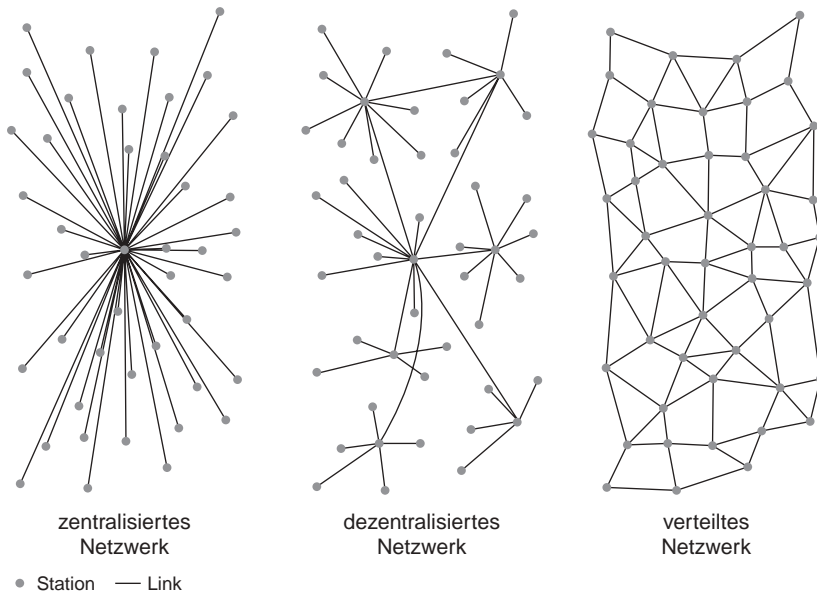
Netzwerktopologie wird die jeweils typische Anordnung von Knoten und Rändern bezeichnet. Verschiedene Topologien haben verschiedene Eigenschaften bezüglich der Strukturierung der Kommunikation und der Wegelenkung zur Folge. Die wichtigsten Typen sind das sternförmige Netz mit einem Knoten als Mittelpunkt, der mit den Außenstellen kommuniziert, ein ringförmiges Netz, eine Baumstruktur, sowie ein Maschennetz, bei dem jeder Knoten mit mehreren anderen Knoten verbunden ist. Ein Sonderfall ist die Funkzelle, wobei alle Teilnehmer dasselbe Medium verwenden.



**Abb. 1-1** Netzwerktopologien – Stern, Ring, Maschennetz, Baum

Alle diese Topologien haben ihre Vor- und Nachteile. So ist in einem sternförmigen Netz das Routing relativ einfach. Fällt aber der Zentralcomputer aus, bricht das ganze Netz zusammen. Telefonnetze haben einen sternförmigen Aufbau. Die Anschlüsse der Teilnehmer laufen in Vermittlungsstellen zusammen, so dass es relativ einfach ist, diese als Instrumente sozialer Kontrolle (z. B. durch Überwachung) einzusetzen. Im Auftrag der RAND Corporation beschäftigte sich Paul Baran Anfang der sechziger Jahre mit Netztopologien. Die Vorgabe lautete, dass Netze auch nach einem Nuklearschlag noch funktionieren sollten. Baran unterschied zwischen zentralen Netzen, dezentralen Netzen und Maschennetzen. Je mehr Verbindungen ein Knoten zu anderen Knoten hat, umso weniger macht es aus, wenn einer dieser Knoten oder sogar mehrere ausfallen. Diese Überlegungen führten Baran zu der Schlussfolgerung, dass ein Maschennetz die widerstandsfähigste Topologie hat (siehe Abb. 1-2).

Die Idee des Maschennetzes ist später in die Architektur des Internets eingegangen, es wäre aber falsch, deshalb zu behaupten, dass das Internet ein reines Maschennetz sei. Tatsächlich werden Mischungen aus den genannten Topologien verwendet. So kann z. B. ein lokales Funknetz über einen Knoten mit einem dezentralen Netz verbunden werden. Ein ringförmiges Hochgeschwindigkeitsnetz, das z. B. in Form eines Glasfasernetzes als Backbone eines Metropolitan Area Network dient, kann zahlreiche Öffnungspunkte hin zu kleineren lokalen Netzen haben, die



**Abb. 1-2** Netzwerkgrafik von Paul Baran

wiederum weiter in sich verschachtelt sein können. Je nach geografischer Ausdehnung unterscheidet man zwischen Local Area Networks (LANs), Metropolitan Area Networks (MANs) und Wide Area Networks (WANs). Die Free Networker haben dem augenzwinkernd eine weitere Variante hinzugefügt, das Community Area Network (CAN).

## Trägermedien

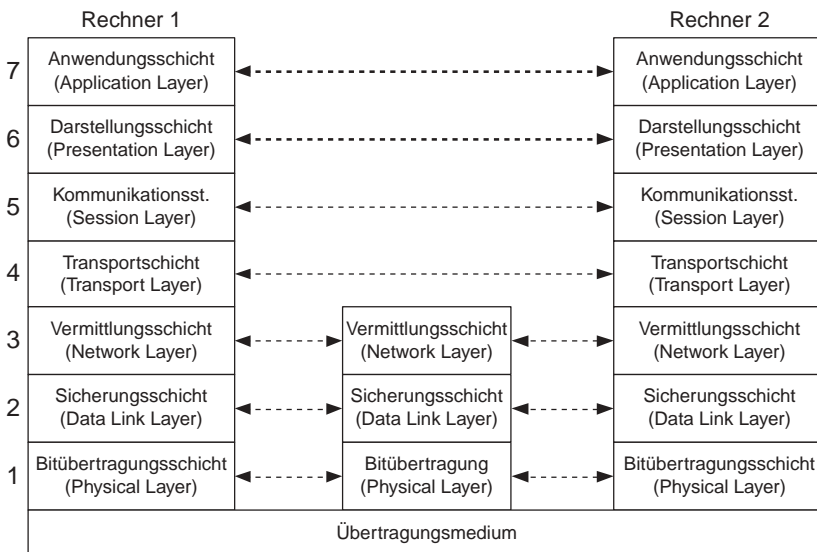
Grundsätzlich unterscheidet man zwischen leitungsgebundener und drahtloser Übertragung. Die Übertragung mittels Leitungen bezeichnet man auch als »geführte« Übertragung, die drahtlose als »ungeführt«. Die Daten werden in Form von elektromagnetischen Wellen übertragen. Der Modulator eines Senders hat die Aufgabe, die zu übertragenden Bits in entsprechende Signale zu übersetzen, die vom Demodulator des Empfängers detektiert werden können. Verschiedene Wellenformen und Pegelschwankungen werden benutzt, um ein detektierbares Signal herzustellen. Hier befindet man sich fest in den Händen der Physik, und die Eigenschaften des Übertragungsmediums, der verwendete Frequenzbereich und die benötigte Bandbreite des Signals spielen eine wichtige Rolle. Je größer die Bandbreite des Signals, umso höher ist theoretisch

die zu erzielende Datenrate. Die Entfernungen, die Signale überwinden können, hängen von der Dämpfung des verwendeten Mediums ab sowie von eventuell vorhandenen Störungen. Die am häufigsten verwendeten Kabeltypen sind die Zweidrahtleitung (engl. »twisted pair«), das Koaxialkabel und die Glasfaser. Letztere arbeitet in den höheren Frequenzbereichen, ermöglicht die schnellsten Datenraten und die Überbrückung großer Entfernungen. Koaxialkabel wird in der Regel für Kabelfernsehen eingesetzt und kann nebenbei auch noch Internetpakete übertragen. Twisted Pair wird hauptsächlich für lokale Netze eingesetzt.

Bei der drahtlosen Übertragung gibt es die verschiedensten Techniken, von den unteren Frequenzbereichen ab 30 kHz angefangen, die wir gewöhnlich als »Radio« bezeichnen, bis zu sehr hochfrequenten Signalen, die für Satellitenübertragungen genutzt werden. Auch hier gilt, dass mit größerer Bandbreite (d. h. bei höherer Frequenz) auch schnellere Datenraten erzielt werden können. Auch die Reichweite eines Signals ist von der verwendeten Frequenz abhängig. Niedere Frequenzen können auch bei geringer Signalstärke sehr weit reisen, Mauern und andere physische Hindernisse durchdringen, während hochfrequente Signale Sichtverbindungen benötigen. Der englische Begriff »line of sight« spiegelt diese Anforderung besser wider. Es muss zwischen Sender und Empfänger eine gerade Linie gezogen werden können, die auf kein physisches Hindernis trifft, damit Kommunikation erfolgen kann.

### **Schichtenmodelle der Netzkommunikation**

1982, als es absehbar wurde, dass die Kommunikation in Datennetzen nicht mehr aufzuhalten sein würde, setzten sich Vertreter der nationalen Monopolgesellschaften für Post, Telegrafie und Telefonie (im Folgenden PTTs oder Telcos genannt) zusammen, um gemeinsam mit Vertretern großer Technologiekonzerne und unter dem Dach der International Organization for Standardization (ISO) ein Referenzmodell für die Kommunikation in Datennetzen zu erarbeiten. Herausgekommen ist das OSI (Open Systems Interconnections)-Modell, das die Vorgänge in Datennetzen nach einem in hierarchischen Schichten aufgebauten Modell strukturiert.



**Abb. 1-3** OSI-Referenzmodell und logische Übertragungswege

Jede einzelne Schicht oder Ebene des Modells behandelt eine klar umrissene Zahl von Aufgaben. Die unterste von sieben Schichten ist die physikalische Schicht, deren Aufgabe es ist, die Bits als Signale abzubilden. Die darüber liegende Schicht ist die Sicherungsschicht, welche die Zuverlässigkeit der Übertragung sicherstellt. Diese wird unterteilt in eine untere Schicht namens Medium Access Control (MAC) und eine obere Schicht namens Logical Link Control. MAC wird immer dann benötigt, wenn sich mehrere Stationen ein Übertragungsmedium teilen. Würden alle Stationen gleichzeitig zu senden und zu empfangen versuchen, würde das zu Kollisionen und somit Datenverlusten führen. Deshalb muss es »Verkehrsregeln« (Vielfachzugriffsprotokolle) geben, die sicherstellen, dass zu einem Zeitpunkt immer nur ein Gerät sendet. In der Funknetztechnologie nach dem 802.11-Standard, die in diesem Buch eine zentrale Rolle spielt, wird auf der MAC-Schicht CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) verwendet.

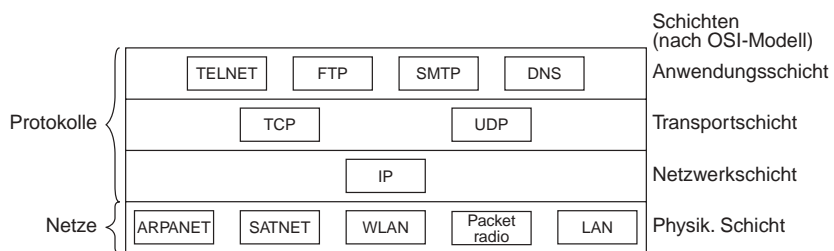
Weitere Schichten des OSI-Modells sind die Netzschicht, die Transportschicht, die Sitzungsschicht, die Präsentationsschicht und die Anwendungsschicht.

Das OSI-Schichtenmodell basiert auf dem Prinzip, dass für jede Schicht Protokolle existieren, welche die für die jeweilige Schicht definierten Dienste zur Verfügung stellen. Die Protokolle auf der jeweils

höheren Schicht können auf die Dienste der unteren Schicht zurückgreifen, ohne sich darum kümmern zu müssen, wie diese ihre Aufgaben erledigt. Der Vorteil dieses Referenzmodells ist es, dass es Entwicklern und Technikern einen Bezugsrahmen für die Vorgänge in Netzwerken bietet. Auch Geräte, die als Komponenten in Netzwerken dienen, werden entsprechend dem OSI-Modell behandelt. So werden z. B. Repeater, die der Verbindung von Netzwerksegmenten in LANs dienen, von ihrer Funktionalität her der OSI-Schicht 1 zugeordnet. Eine Bridge ist ein Gerät der OSI-Schicht 2 und dient der Verbindung von LANs mit verschiedenen physikalischen Eigenschaften. Router übernehmen u. a. Aufgaben auf OSI-Ebene 3.

### Internet – TCP/IP

Wenn wir vom Internet reden, so meinen wir eigentlich TCP/IP. Das Internet ist eigentlich kein einheitliches Netz, sondern eine Verbindung vieler Netze, die mittels TCP/IP miteinander kommunizieren können. Diese Abkürzung steht für die wichtigsten Protokolle, die bei der Kommunikation im Internet Verwendung finden – »Transmission Control Protocol« und »Internet Protocol«, zusammen also TCP/IP. Die Reihenfolge ist irreführend, denn eigentlich arbeitet IP auf der tieferen Schicht nach dem OSI-Modell, auf Layer 3. Vereinfachend gesprochen übernimmt IP die Aufgabe der Aufteilung der Informationen in Pakete/Data-gramme und versieht sie mit einem Header. TCP sorgt für die Flusskontrolle während der Übertragung und dafür, dass die Pakete am Ende wieder in der richtigen Reihenfolge zusammengesetzt werden.



**Abb. 1-4** TCP/IP

Die untersten Schichten – Layer 1 und 2 im OSI-Modell – sind bei TCP/IP kaum näher spezifiziert, was aus den Zielsetzungen des ARPANet-Forschungsprogramms erklärt werden kann, aus dem das Internet her-

vorgegangen ist. Den Militärs, die das ARPANet finanzierten, ging es darum, ein Protokoll zu haben, das die Kommunikation über verschiedene Typen von Netzwerken hinweg erlaubt. Auf diesen Schichten kann TCP/IP daher die verschiedensten Netzwerkprotokolle einsetzen, wie z. B. Ethernet (eine häufig für LANs verwendete Technologie), Funknetze (802.11, Packet Radio) oder das bei der Verwendung von Modems und Telefonleitungen eingesetzte X.25-Protokoll. Die Fähigkeit von TCP/IP, verschiedene Netze zu verbinden, indem ein gemeinsames Kommunikationsprotokoll verwendet wird, hat wesentlich zum Erfolg des Internets beigetragen.

Neben TCP/IP finden noch eine große Anzahl weiterer Protokolle Verwendung, die man zusammenfassend die Internet-Protokoll-Suite nennt. Auf der Anwendungsschicht sind das zum Beispiel FTP (File Transfer Protocol für die Übertragung von Dateien), E-Mail (SMTP) und HTTP (Hyper Text Transfer Protocol – WorldWideWeb). Die grafische Benutzeroberfläche des WWW hat sehr zur schnellen Verbreitung des Internets beigetragen. Viele Menschen verwechseln deshalb das WWW mit dem Internet. Für das Funktionieren des Netzes wichtiger sind aber die unteren Schichten, auf denen TCP/IP wirksam ist. TCP/IP ist immer im Spiel, auch wenn wir oft nur das WWW zu sehen bekommen.

#### Literatur

- [1] Andrew Tanenbaum, Computer Networks, Prentice Hall, 4. Aufl., 2002
- [2] Peterson, Davie: Computernetze. dpunkt.verlag, 2. Aufl., 2004
- [3] Hafner, Katie; Lyon, Matthew: ARPA Kadabra, dpunkt.verlag, 2. Aufl., 1999.
- [4] Lienemann, Gerd: TCP/IP-Grundlagen, 3. Aufl., Heise, 2003

## Kurze Geschichte des Datenfunks

Bereits in der Frühphase der Funktechnologie, vor der Nutzung des Radios als Unterhaltungsmedium, wurden »Daten« übertragen, wenn man den Morsecode, der ein Binärcode ist, als solche gelten lässt. Die drahtlose Technologie ermöglichte es bereits in den 1910er Jahren, kurze Nachrichten und Börsenkurse von Küstenstationen aus an Schiffe zu versenden, die für ihre Passagiere »drahtlose Zeitungen« zusammenstellten. Aber so richtig begann die Geschichte des Datenfunks im engeren Sinn erst Anfang der siebziger Jahre. Zumindest laut einigen Autoren (Tanenbaum, Perkins) stand die Entwicklung des Datenfunks in einer engen Verbindung sowohl zur Entwicklung des Internets als auch des Ethernets.

1971 wurden Funk- und Netzwerktechnologien im Rahmen des Forschungsprojekts ALOHANET unter der Leitung von Norman Abramson an der Universität von Hawaii erstmals zusammen eingesetzt. Die Universität von Hawaii war auf sieben verschiedene Standorte auf vier Inseln verteilt. ALOHANET ermöglichte es den Computern in den Außenstellen, mit dem Zentralcomputer in Oahu zu kommunizieren. Das Netz war sternförmig aufgebaut, die Außenstellen konnten miteinander nur über den Zentralcomputer Kontakt aufnehmen. Ungefähr zur selben Zeit arbeitete ein junger Student namens Bob Metcalfe an seinem Dokortitel. Im Rahmen seiner Studien begeisterte er sich für die Arbeit von Abramson, und zwar so sehr, dass er nach seinem Studienabschluss einen Sommer auf Hawaii verbrachte, bevor er im Forschungszentrum Xerox PARC (Palo Alto Research Center) zu arbeiten begann. Die Forscher dort hatten bereits an einer Erfindung zu arbeiten begonnen, die später als Personal Computer (PC) bekannt werden sollte. Doch die PCs im Xerox PARC waren voneinander isoliert. Aufbauend auf seinem Wissen über Abramsons Arbeit begann Metcalfe zusammen mit seinem Kollegen David Boggs an einem lokalen Netzwerk zu arbeiten (Local Area Network = LAN). Dieses Netzwerk wurde 1976 erstmals implementiert und auf den Namen Ethernet getauft. In der Frühzeit des Radiozeitalters hatte man geglaubt, dass elektromagnetische Wellen ein Medium in der Luft für ihre Ausbreitung benötigen, das »Äther« genannt wurde. Diese Ansicht wurde zwar schon 1887 bei Experimenten widerlegt, die zeigten, dass sich die Wellen auch in einem Vakuum ausbreiten können, doch die Vorstellung eines Äthers hält sich hartnäckig in der Alltagssprache.

1978 entwickelten die Firmen Xerox, DEC und Intel gemeinsam einen Ethernet-Standard mit Übertragungsraten von 10 Mbps.

Xerox kann den zweifelhaften Ruhm für sich in Anspruch nehmen, in seinen Labors bahnbrechende Entwicklungsarbeit geleistet, doch deren kommerzielle Ausschlichtung dann anderen überlassen zu haben. 1979 verließ Metcalfe Xerox, weil es sich für seine Erfindung über die Standardisierung hinaus wenig interessierte, und gründete die Firma 3Com. 1980 begann eine Arbeitsgruppe des IEEE mit der Entwicklung eines herstellerunabhängigen Standards für LANs, was 1983 in die Verabschiedung des Ethernet-Standards 802.3 mündete. Ungefähr zur selben Zeit begann 3Com Ethernet-Adapter zu verkaufen, mit denen IBM-PCs an ein lokales Netz angeschlossen werden konnten. Ethernet ist heute die verbreitetste Technologie für LANs und diente auch als Grundlage für die Entwicklung eines Standards für Wireless Local Area Networks (WLAN).

### **Internet und Packet Radio**

1968/69 hatten Forscher im Rahmen eines von der ARPA (Advanced Research Projects Agency) geförderten Projekts den Prototyp eines Computernetzwerks auf der Basis der paketvermittelten Kommunikation entwickelt. Im Herbst 1969 gelang es erstmals, vier Großrechner miteinander zu verbinden. Die ARPA erkannte das Potenzial dieser Technologie für die Bedürfnisse der Armee. Die Fahrzeuge der Armee in einer Kampfsituation haben die Anforderung, miteinander und mit der Kommandozentrale in Kontakt zu bleiben, obwohl sich ihre eigene Position ständig ändert und auf Grund der Geländetopologie Verbindungen vorübergehend ausfallen können. Paketvermittelte Kommunikation in einer mobilen, drahtlosen Umgebung erschien als geeignetste Lösung. Die ARPA initiierte 1972 Forschungsarbeiten zur Entwicklung eines Packet Radio Network (PRNet). Die Grundidee für das PRNet der ARPA wurde in verschiedenen Umgebungen implementiert, in terrestrischen Sendestationen und solchen aus der Luft, für Amateurfunk, Breitband, Schmalband und für Satelliten. Das Grundkonzept des PRNet sah vor, dass sich verschiedene Nutzer eine Frequenz in einem Sendernetz teilen. Theoretische Studien ergaben, dass es besser ist, einen breiten Kanal zu haben, der dynamisch geteilt wird, anstatt die Kommunikation in viele Kanäle aufzuteilen. Dieses dynamische Teilen eines Teils des Spektrums erforderte es, Spread-Spectrum-Technologie zu verwenden.

Spread Spectrum geht auf Forschungen der österreichischen Schauspielerin Hedy Lamarr und ihres Ehemannes George Antheuil zurück. Ausgangspunkt ihrer Idee war, eine Methode zu finden, wie es zu verhindern sei, dass die funkgesteuerten Torpedos der US-Navy durch deutsche Störsender vom Ziel abgebracht wurden. Ihre Idee war, das Steuersignal nicht auf einer festen Frequenz, sondern in einer Folge zufällig erscheinender verschiedener Frequenzen zu senden. Wenn der Empfänger die Abfolge der Sprünge von Frequenz zu Frequenz kennt, kann dieser das richtige Signal empfangen. Mithilfe von Forschern am MIT wurde die Idee weiterentwickelt und 1942 ein Patent angemeldet, doch das Verteidigungsministerium wollte vorerst nichts davon wissen. Erst viele Jahre später, 1962, wurde Spread Spectrum erstmals eingesetzt und bald zur Basis einer Reihe von Übertragungstechnologien. Spread Spectrum nutzt vorhandene Bandbreite effektiver, ist weniger anfällig für Störungen durch Interferenzen und abhörsicherer. Auf der Basis computergesteuerter Funkgeräte, die im Direct-Sequence-Spread-Spectrum-Verfahren senden und empfangen, entwickelte die ARPA bereits 1972 Netzwerke mit variablen Übertragungsraten zwischen 100 und 400 kbps. Zugleich laufende Forschungen über paketvermittelte Satellitenkommunikation führten zur Erkenntnis, dass diese verschiedenen Netze, ARPANet, PRNet und SatNet, miteinander verbunden sein sollten.

Eine berühmte Technik-Demonstration verband einen fahrenden Lastwagen in Kalifornien über das PRNet mit dem ARPANet, welches die Botschaften an die Ostküste sandte, von wo aus sie per Satellit an das University College in London verschickt wurden. Ein im Lastwagen in Kalifornien sitzender Forscher sollte über diese Verbindung über verschiedene Netzwerke hinweg einen Computer in London nutzen können. Das Experiment führte zu der Erkenntnis, dass die existierenden Protokolle des ARPANet nicht dafür geeignet waren, verschiedene Netze miteinander zu verbinden. Die Forschungen im Bereich der Protokolle wurden intensiviert, was zur Entwicklung des TCP/IP-Protokolls führte.

TCP/IP wurde mit der Absicht entwickelt, die Kommunikation »zwischen Netzwerken« (engl. »internetworks«) zu ermöglichen. Unabhängig vom physischen Medium und der Topologie des jeweiligen Netzwerks sollte TCP/IP den Datenaustausch zwischen den Netzwerken ermöglichen. Die ARPA beauftragte die Firma Bolt, Beranek and Newman (BBN) und die Universität von Kalifornien in Berkeley damit, TCP/IP in Unix zu integrieren. Dieser Schritt begünstigte das Durchsetzungsvermögen sowohl des Betriebssystems Unix als auch des Internetproto-

kolls. Amerikanische Universitäten hatten gerade damit begonnen, ihre Großrechner mit LANs zu verbinden, doch es fehlte ihnen an Netzwerksoftware. Nach der erfolgreichen Implementierung von TCP/IP in die Berkeley-Version des Unix-Betriebssystems (BSD – Berkeley System Distribution) begannen viele Universitäten, BSD zu verwenden und es zur Verbindung ihrer LANs einzusetzen. 1983 hatte sich TCP/IP als wichtigstes Protokoll im ARPANet durchgesetzt. Im schnell wachsenden Netz der Netze wurde immer häufiger vom Internetwork gesprochen, bis die Bezeichnung Internet schließlich im allgemeinen Sprachgebrauch hängen blieb. Da die Funknetztechnologie parallel mit der TCP/IP-Protokollfamilie entwickelt wurde, wird das PRNet auch als das erste Netzwerk mit »Internetbewusstsein« bezeichnet (Perkins, 2001).

Diese ersten Funknetze in den siebziger Jahren beruhten auf schwerer militärischer Hardware mit hohem Energiebedarf. Ein Folgeprogramm zur Entwicklung von Survivable Radio Networks (SURAN – überlebensfähige Funknetzwerke) konzentrierte sich auf Low Cost Packet Radio (LPR). Ein Mikroprozessor der (damals) modernsten Generation, ein Intel 8086, wurde zur Ansteuerung des Radios benutzt. Von da an entwickelte die militärische Forschung Konzepte weiter, die heute zu drahtlosem Internet im Schlachtfeld ausgereift sind. Ein wichtiger Beitrag aus dieser Richtung ist die Entwicklung dynamischer Routing-Protokolle. Die militärische Forschungsarbeit über mobile Ad-hoc-Netze [1] mündete in eine Forschungsgruppe im Rahmen der IETF mit der Bezeichnung Mobile Ad Hoc Networking Group – MANET [2].

### **Amateurfunker und Packet Radio**

Die wahren Helden des Datenfunks sind jedoch die Amateurfunker. Schon seit den sechziger Jahren gab es angeblich Experimente mit Datenfunk [3]. In den späten siebziger Jahren begannen erste Versuche der Hobbyfunker mit der Übertragung von Datenpaketen per Funk. 1978 führte der Montreal Amateur Radio Club Versuche mit Packet Radio auf Amateurfunk-Frequenzbändern durch. 1980 wurde der erste Terminal Node Controller (TNC) von Doug Lockhart in Vancouver entwickelt. Die Funktionsweise von TNCs ist mit der eines Telefonmodems vergleichbar, sie übersetzen die digitalen Informationen des Computers in eine Form, die von Funkgeräten moduliert werden kann. Tucson Amateur Packet Radio (TAPR) entwickelte 1982 den TNC-1 und 1984–85 den TNC-2. Die Amateurfunker begannen Packet Bulletin Board Sys-

tems zu entwickeln, Mailboxen, die über Funk miteinander kommunizieren. Die populären Hobbys Funk und Computer fanden so zueinander, und die Hobbyfunker schufen ab Mitte der achtziger Jahre ein weltweites Kommunikationsnetz per Funk und Satellit. In Deutschland schrieb Flori Radlherr aus München 1985 eine Software namens Digicom 64, die auf Commodore-64-Computern lief und diesen die Funkkommunikation ermöglichte, ohne einen teuren TNC anschaffen zu müssen. Die Amateurfunkverbände der USA und Kanadas sponserten in den achtziger Jahren die Computer Networking Conference, weil sie Interesse an einem Forum für die Entwicklung großräumiger Funknetze – Wireless Wide Area Networks – hatten, lange bevor die Industrie auf diese Möglichkeiten aufmerksam wurde.

### **Wavelan – 802.11**

1985 gab die Federal Communications Commission das ISM-Frequenzband zur allgemeinen Nutzung frei. ISM steht dabei für »Industrial, Scientific and Medical« (siehe nächsten Abschnitt). Die Öffnung des ISM-Bandes zur lizenzfreien Nutzung ermöglichte es der Industrie, funkbasierte LAN-Komponenten zu entwickeln. Da es aber noch keinen Standard gab, entwickelten die Hersteller proprietäre Systeme, die miteinander nicht kompatibel waren. Eine Arbeitsgruppe des IEEE begann Ende der achtziger Jahre mit der Entwicklung eines Standards, der diesen Mangel beheben sollte. 1997 wurde der erste FunkLAN-Standard 802.11 herausgegeben.

#### Literatur

- [1] Homepage Charles Perkins, <http://www.iprg.nokia.com/~charliep/>
- [2] MANET, [http://protean.itd.nrl.navy.mil/manet/manet\\_home.html](http://protean.itd.nrl.navy.mil/manet/manet_home.html)
- [3] Die Behauptung, dass es Amateurdatenfunk schon in den sechziger Jahren gab, wird im unten zitierten Artikel aufgestellt, konnte aber nirgends sonst verifiziert werden: »Why Packet Radio?«, <http://www.tapr.org/tapr/html/Fpktprm1.html>

## Einführung Technik WLAN – 802.11

Dieses Buch ist kein technisches Handbuch zum Aufbau von drahtlosen Netzen. Zu diesem Zweck gibt es eine wachsende Anzahl an spezialisierter Fachliteratur. Empfohlen sei z. B. »Building Wireless Community Networks« von Rob Flickenger (O'Reilly & Associates, Dezember 2001). Ein ausgezeichnetes Referenzbuch, das die zugrunde liegenden Standards erklärt, ist »Wireless LANs« von Jim Geier (Sams, 2001). Informationen auf dem letzten Stand finden sich auch auf zahlreichen Websites. In Mailinglisten und Online-Foren kann man praktische Hilfe und direkte Antworten auf direkte Fragen von Netz-Enthusiasten erhalten. Diese kurze Einführung richtet sich an interessierte Laien, in der Hoffnung, ein wenig begriffliche Klarheit und Übersicht zu schaffen.

Die unter verschiedenen Bezeichnungen wie Wavelan, WLAN, Wi-Fi oder Airport bekannte Funknetztechnologie beruht auf der Gruppe der 802.11-Standards des Institute of Electrical and Electronics Engineers (IEEE). Grundsätzlich gesprochen, kommen hier zwei Technologien zusammen, Radio und Computernetze. Hinsichtlich der Computernetztechnologie ist 802.11 eine Untergruppe der LAN/MAN-Standards, die mit der Zahlenfolge 802 [1] beginnen. Die Zahlen selbst haben keine Bedeutung, sondern resultieren daher, dass das IEEE die von ihm erarbeiteten Standards fortlaufend nummeriert. Mit der Entwicklung der 802.11-Standards wurde in den späten achtziger Jahren begonnen. Der erste WLAN-Standard 802.11 wurde schließlich im Juni 1997 verabschiedet und im November desselben Jahres veröffentlicht. Auf der Basis dieses Standards konnten Geräte für drahtlose Netze mit Datendurchsatzraten von 1 Mbps und 2 Mbps hergestellt werden. Funktechnisch waren zwei verschiedene Frequenzspreizverfahren vorgesehen, Frequency Hopping Spread Spectrum (FHSS) und Direct Sequence Spread Spectrum (DSSS).

Einzelne Hersteller hatten schon vor der Verabschiedung des Standards Geräte für Funknetze entwickelt und verkauft, doch da der Markt noch sehr klein war, waren sie teuer, und mangels eines Standards waren die Geräte verschiedener Hersteller nicht kompatibel zueinander.

1999 legte das IEEE zwei weitere Standards nach, 802.11a und 802.11b. Der heute am weitesten verbreitete Standard ist 802.11b, der eine Übertragungsrate von maximal 11 Mbps verspricht, die jedoch je nach Verbindungsqualität auf 5,5, 2 und 1 Mbit zurückgehen kann. Die

versprochene maximale Datendurchsatzrate von 11 Mbps ist jedoch eine Bruttoangabe, da ca. 40 Prozent der Kanalkapazität durch den Protokoll-Overhead belegt werden. Physische Einflüsse auf die Qualität der Funkverbindung führen zu einer zusätzlichen Verminderung des Datendurchsatzes. 802.11b arbeitet im 2,4-GHz-Frequenzbereich und verwendet das DSSS-Verfahren.

802.11a verspricht Übertragungsraten von bis zu 54 Mbps und sendet im Band zwischen 5,725 und 5,850 GHz. Auf Grund des Protokoll-Overheads werden jedoch nur 20 bis 30 Mbps erreicht. Im Juni 2003 wurde ein weiterer Standard verabschiedet, 802.11g, der ebenfalls bis zu 54 Mbps verspricht. Weitere Arbeitsgruppen der 802.11-Gruppe beschäftigen sich mit »Quality of Service« (garantierte Verbindungsqualität, die unter anderem Audio- und Videoanwendungen Auftrieb geben sollte), Interoperabilität zwischen Geräten verschiedener Hersteller und Sicherheit.

Der Ort, an dem 802.11 innerhalb eines Computersystems aktiv ist, ist die so genannte Funknetzkarte (engl. Radio Network Interface Card). Der Besitz und die erfolgreiche Installation einer solchen Karte sind also Voraussetzung, um an einem 802.11-Netz teilnehmen zu können. Da die Technologie schnell Akzeptanz und damit Verbreitung in großen Stückzahlen gefunden hat, gibt es inzwischen (Stand Juni 2003) bereits Funknetzkarten für unter 50 Euro. Es gibt Funknetzkarten für die verschiedensten Anschlussmöglichkeiten an Computer wie PCMCIA, PCI und USB. Weit verbreitet sind Funknetzkarten, die den gängigen Ethernet-Karten in Scheckkartengröße ähneln. Bei Laptops der neuesten Generation ist 802.11 häufig bereits in die Hardware integriert und vorinstalliert.

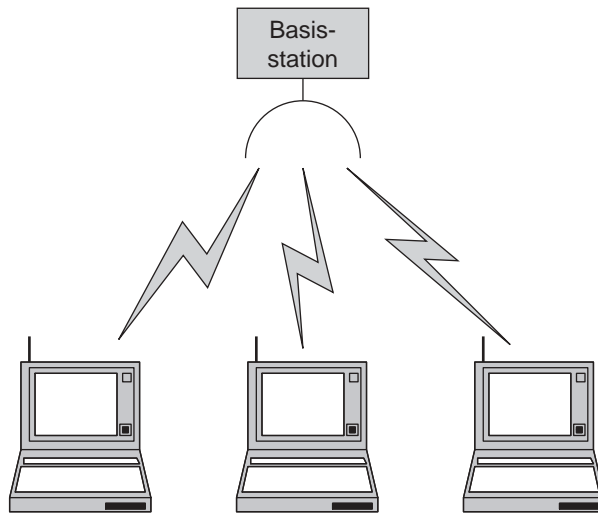
Um nicht fest integrierte Funknetzkarten zum Laufen zu bringen, müssen die entsprechenden Treiber installiert werden. Diese werden meist mit der Karte mitgeliefert oder können von der Website der Hersteller geladen werden. Zum Glück gibt es auch immer mehr herstellerunabhängige Open-Source-Treiber, so dass auch Linux-Freundinnen nicht zu kurz kommen. Die in den Funknetzkarten enthaltenen Radioteile sind softwaregesteuerte Sender/Empfänger (engl. »transceiver«). Diese können im Prinzip gehackt werden, wodurch z. B. die Sendestärke erhöht werden kann (womit jedoch keine Empfehlung ausgesprochen werden soll).

802.11 stellt Funktionen auf der Ebene der physikalischen Schicht und der MAC-Schicht nach dem OSI-Modell bereit. Jede Funknetzkarte hat eine eigene MAC-Adresse, die aus einer 96-Bit-Zahl besteht, die in Form von 12 Hexadezimalzahlen in 6 Zweiergruppen angegeben wird.

Die ersten 6 enthalten die Herstellerkennung, die letzten 6 die Seriennummer des Geräts. MAC-Adressen ermöglichen es 802.11-Geräten, sich gegenseitig zu erkennen und damit die Adressierbarkeit sicherzustellen. Mithilfe der MAC-Adressen kann die Verbindung zu Protokollen auf höheren Schichten des OSI-Modells hergestellt werden. MAC ermöglicht es z. B., dass einem Rechner von einem Host eine IP-Adresse zugewiesen wird. Die Vergabe von IP-Adressen ist Voraussetzung für die Benutzung von Internetanwendungen wie E-Mail und WWW. Da die Internetprotokolle mehr oder weniger blind gegenüber den Vorgängen auf der physikalischen und der MAC-Schicht sind, können Nutzer in 802.11-Netzen aktiv sein und merken (meist) keinen Unterschied zur Benutzung eines kabelgebundenen Netzes.

In einem drahtlosen Netz nach der Familie der 802.11-Standards gibt es zwei grundsätzlich verschiedene Betriebsmodi, das Basic Service Set (BSS) und das Independent Service Set. Das BSS ermöglicht die Kommunikation zwischen einem Access Point (AP) und Client-Rechnern. Dieser Modus wird häufig auch als Infrastrukturmodus bezeichnet. Der AP ist dabei der Boss im lokalen drahtlosen Netz, der den Datenverkehr mit den Client-Rechnern regelt. Letztere können nicht direkt, sondern nur über den AP miteinander kommunizieren. Der AP selbst kann wiederum mit anderen Netzen wie dem Internet verbunden sein und, je nach Konfiguration, für die Clients als Bridge (engl. »Brücke«) zum Internet dienen. Eine solche Konfiguration eines AP mit Internetzugang und einer Anzahl von Clients wird häufig auch als Hotspot bezeichnet. Kommerzielle APs gibt es in verschiedenen Preisklassen und Funktionsumfängen. Die billigsten sind inzwischen schon für unter 100 Euro zu haben und beinhalten meist nur die Funktion eines einfachen AP.

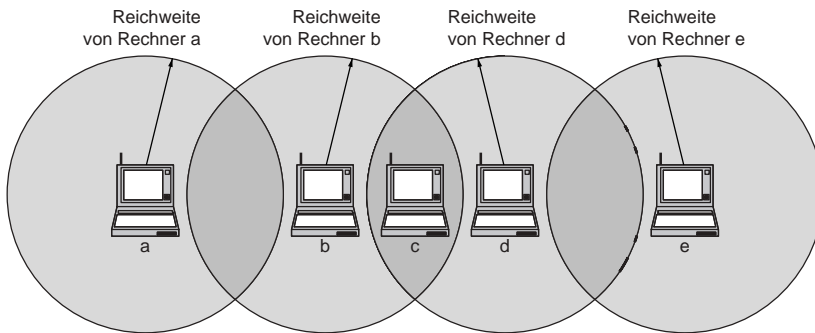
Eine erweiterte Form des Basic Service Set, das Extended Service Set, ermöglicht es mehreren APs innerhalb einer festen Installation miteinander zu kommunizieren, so dass sie gemeinsam ein größeres Gelände abdecken, innerhalb dessen sich Clients frei bewegen können, indem sie von einem AP zum nächsten übergeben werden. Selbst wenn sich nicht alle Rechner in einem solchen drahtlosen Rechnerverbund in Reichweite voneinander befinden, können Datenpakete zwischen diesen Rechnern ausgetauscht werden, indem zwischen Sender und Empfänger positionierte APs zur Überbrückung verwendet werden. Eine brauchbare Analogie ist die vom Seerosenteich: Die Pakete »springen« wie Frösche von Blatt zu Blatt. Man spricht daher auch von »Multi-Hop-Netzwerken«.



**Abb. 1-5** Access Point mit Verbindung zum Internet und mehreren drahtlos verbundenen Clients

Der IBSS-Modus ermöglicht die Bildung von Ad-hoc-Netzen (Netze aus dem Stegreif) – synonym auch Peer-to-Peer-Netze oder Computer-zu-Computer-Netze genannt. In diesem Fall gibt es keinen zentralen Rechner, der eine den anderen übergeordnete Rolle einnimmt. Jeder Rechner übernimmt für seine Nachbarn die Funktion der Vermittlung von Datenpaketen. Auf der Basis dieser Form der Vernetzung ist es möglich, spontan Netzwerke zu bilden. Eine Gruppe von Personen mit Laptops und Funknetzkarten kann z. B. in einem Konferenzsaal oder bei einer öffentlichen Veranstaltung ein solches Netz »ad hoc« aufbauen und Daten austauschen. Die Netzwerktopologie solcher Netze kommt der eines »Maschennetzes« (engl. »Mesh Network«) am nächsten, und viele Community-Netze experimentieren mit dieser faszinierenden Möglichkeit zur spontanen Bottom-up-Vernetzung (siehe Abb. 1-6).

Jedes 802.11-Netz benötigt die Angabe eines vom Systemadministrator festgelegten Netzwerknamens, ESSID (Extended Service Set ID) oder SSID (Service Set ID) genannt. Die ESSID kann eine beliebige Folge von Buchstaben sein. Auch die Teilnehmerinnen müssen die exakte ESSID (oder SSID) angeben und in geschlossenen Netzen dazu meist noch ein Passwort. WLANs im Infrastrukturmodus benutzen häufig auch die Möglichkeit der Filterung von MAC-Adressen. Damit kann man den Zugang auf jene Rechner beschränken, deren Besitzer sich zuvor mit dem



**Abb. 1-6** Peer-to-Peer-Netz zwischen Rechnern in einem WLAN-Netz unter Verwendung des IBSS-Modus. Auch wenn nicht alle Rechner in Reichweite voneinander sind, können sie trotzdem noch miteinander kommunizieren.

Netzwerkbetreiber bekannt gemacht und diesem die MAC-Adresse ihrer Netzwerkkarte mitgeteilt haben. Wirklich sicher ist diese Methode allerdings nicht, da MAC-Adressen gefälscht werden können.

Sicherheit in 802.11-Netzen ist überhaupt ein Problem. Eine weitere Sicherungsmethode neben der MAC-Adressenfilterung, die in den 802.11b-Spezifikationen vorgesehen ist, ist eine Verschlüsselungsmethode namens WEP (Wired Equivalency Privacy). WEP ist jedoch bekanntermaßen auf verschiedenen Wegen zu knacken. Ohne hier im Detail auf die Sicherheitsdiskussion einzugehen, sei denen, die sichere Kommunikation bevorzugen, angeraten, sich mit IPSec [3] und SSH [4] vertraut zu machen. Die Sicherheitsfrage ist zudem, wie alles, was mit Netzen zu tun hat, stark davon abhängig, was man mit einem Netzwerk vorhat. Bei Community-Netzen, die öffentlich nutzbare Funknetz-Hotspots anbieten, wird auf Späße wie WEP und MAC-Adressenfilterung von vorneherein verzichtet. Als Konfigurationsprofil wird häufig »any« verwendet und die SSID weithin publiziert, um es Clients so leicht wie möglich zu machen, Zugang zu bekommen. Es muss allerdings hinzugefügt werden, dass Community-Netze absichtlich frei und offen gehalten werden, und nicht, wie es bei privaten Hotspots so häufig der Fall ist, aus reiner Unwissenheit oder Faulheit. Und während der Zugang für Clients mit der Konvention des voreingestellten Konfigurationsprofils »any« so einfach wie möglich gemacht wird, werden die eigenen Rechner, Kommunikationen und Server mit starken Schutzmechanismen gesichert.

802.11b verwendet Frequenzen zwischen 2,4 und 2,485 Gigahertz. Dieser Frequenzbereich ist Teil des so genannten ISM-Bandes, was für

»Industrial, Scientific and Medical« steht. Die Benutzung dieser Frequenzen wurde 1985 in den Vereinigten Staaten erstmals zur Nutzung durch die Öffentlichkeit freigegeben, d. h., für die Benutzung ist keine Lizenz oder spezielle Erlaubnis nötig. Seither haben die meisten Länder nachgezogen (Deutschland im Jahr 1995) und das 2,4-GHz-Band ebenfalls für die öffentliche Nutzung freigegeben. Der deutsche Gesetzgeber legt allerdings Wert auf den feinen Unterschied, dass die Benutzung nicht »lizenzfrei« erfolgt, sondern dass die Erlaubnis zur Nutzung im Rahmen einer »Allgemeinzuteilung« erteilt wird. Um in diesem unregulierten und inzwischen stark überbevölkerten Teil des Spektrums Störungen durch Interferenzen zu vermeiden, wurden restriktive Vorschriften über die erlaubte maximale Abstrahlleistung erlassen. Diese beträgt in Europa 100 Milliwatt und 1 Watt in den USA. Durch die Verwendung von Antennen und eventuell auch Verstärkern kann die Abstrahlleistung erhöht werden. Doch Vorsicht, die Maximalwerte beziehen sich auf das Gesamtsystem, also das, was am Ende – Funknetzkarte plus Verstärker plus Antenne – herauskommt.

Ein offensichtlicher Nachteil des ISM-Bandes ist, dass es von den verschiedensten Geräten benutzt wird. Neben medizinisch-technischen Geräten können dies schnurlose Telefone, Fernsteuerungen für Garagentore und sogar Mikrowellenherde sein. WLANs haben keinerlei Priorität gegenüber diesen Geräten, und je nachdem, was sich in der Nachbarschaft abspielt, kann es zu Störungen kommen. Diese Gefahr wird allerdings dadurch etwas gemindert, dass 802.11b das Frequenzspreizverfahren DSSS benutzt. Anstatt auf einer schmalbandigen Frequenz zu senden, wird ein breiteres Frequenzband benutzt, innerhalb dessen zeitversetzt in verschiedenen Abschnitten des Bandes gesendet wird.

Das hat nun wiederum nichts damit zu tun, dass 802.11b in Europa 11 verschiedene, sich überlappende Kanäle verwendet. Da ein Kanal eine Bandbreite von 22 MHz benötigt, empfiehlt es sich, innerhalb eines bestimmten geografischen Gebiets die benutzten Kanäle aufeinander abzustimmen. Nur die Kanäle 1, 6 und 11 sind garantiert überlappungsfrei.

Antennen dienen zur Verbesserung von Empfangs- und Sendeleistung. Mit handelsüblichen Funknetzkarten lassen sich Entfernungen von 100 Metern, bei günstigen Bedingungen auch mehr, überbrücken. Mit den entsprechenden Antennen können jedoch Verbindungen über 20 km und mehr hergestellt werden. Der terrestrische Highscore liegt bei 70,5 km und dient der Verbindung zwischen Teneriffa und Gran Canaria. [2]



**Abb. 1-7** Richtantenne (Helix). Links Simon Worthington, Mute/YouAreHere, rechts James Stevens, Consume. [Foto: Chris Helgren]

Bei aller Verschiedenheit der existierenden Antennentypen gibt es einige grundlegende Charakteristika. Diese sind die Form der Ausbreitung (engl. »propagation pattern«) und die Verstärkung (engl. »gain«). Man unterscheidet grundsätzlich zwei Ausbreitungsmuster, die Rundstrahlantenne (omnidirektional) und die Richtantenne (unidirektional). Rundstrahlantennen senden kreisförmig in horizontaler Richtung. D. h., der Empfang ist dann am besten, wenn man sich auf derselben Höhe befindet, und am schlechtesten direkt unter der Antenne. Richtantennen ermöglichen, wie der Name schon sagt, die Ausrichtung der Wellen in einer bestimmten Richtung. Eine häufig verwendete Anordnung ist z. B. ein Access Point mit einer Rundstrahlantenne, auf die ein Client-Rechner seine Richtantenne richtet. Wegen der verwendeten hohen Frequenz wird zwischen den Antennen Sichtverbindung (engl. »line of sight«) benötigt, d. h., zwischen Punkt A und B sollten sich keine physischen Hindernisse wie Gebäude, hohe Hecken, Mauern oder dergleichen befinden. Auch Bäume können ein Hindernis darstellen. Da die Wellen die Luft durchdringen müssen, leidet die Verbindungsqualität auch unter

hoher Luftfeuchtigkeit, Regen und Schneefall. Die Qualität eines Signals wird als »Signal-to-noise ratio« (SNR) angegeben.



**Abb. 1–8** Alexei Blinow, Raylab, betrachtet kritisch eine Lötstelle.  
Foto: Chris Helgren

Für Bastler gibt eine ganze Palette an kreativen und billigen Möglichkeiten, Antennen zu bauen. So lässt sich z. B. die zylinderförmige Kartonverpackung einer bestimmten Sorte von Kartoffelchips in eine Richtantenne verwandeln. Auch Bier- und Konservendosen lassen sich in Antennen verwandeln, ebenso wie Milchtüten. Verbreitete Typen sind die Horn-, Helix-, Patch- und Yagi-Antennen. Antennenbau im Do-it-Yourself-Verfahren erfreut sich bei Gemeinschaftsnetzwerken großer Beliebtheit, und es gibt dazu eine ganze Anzahl von Leitfäden im Internet. Das Geheimnis des Antennenbaus ist die exakte Einhaltung der Maße und eine möglichst optimale mechanische Ausführung. Selbst kleine mechanische Fehler, die zunächst nicht auffallen, können sich später rächen, indem sie z. B. das Eindringen von Kondenswasser erlauben, wodurch Bauteile korrodieren. Zu beachten ist, dass bei der Berechnung der maximal erlaubten Abstrahlleistung die Summe aus verwendeter Leistung der Funknetzcard und Antennenverstärkung herangezogen wird. Insbesondere für Anfänger und für besonders ambitionierte Projekte wie Langstreckenverbindungen empfiehlt es sich, erfahrene Ama-

teurfunker als Helfer zu gewinnen. Beim Kauf der Funknetzkarte ist darauf zu achten, dass sie eine Anschlussmöglichkeit für eine Antenne hat.

## Nachteile und Schwächen

Einige der Probleme mit 802.11 sind

- »multipath propagation«: Ein Signal wird von Wänden oder anderen physischen Hindernissen reflektiert und kommt zeitversetzt mehrfach beim Empfänger an (kann aber auch zur Verbesserung der Verbindungsqualität benutzt werden).
- Luftfeuchtigkeit oder Regen, welche die SNR soweit abschwächen, dass es zu Paketverlusten kommt.
- Störungen, die von anderen WLANs verursacht werden.
- Störungen, die von Signalen anderer Geräte im ISM-Spektrum verursacht werden.
- Verfügbarkeit von elektrischem Strom: Nicht überall, wo man ein drahtloses Netz aufbauen möchte, steht Strom zur Verfügung. Aber auch die drahtlosen Clients, wie z. B. Laptops, brauchen Strom. Die Funknetzkarten sind echte Stromfresser, und eine Laptop-Batterie kann u. U. schon nach der Hälfte ihrer normalen Laufzeit leer sein.
- Sicherheit: Der Hinweis soll genügen, dass die standardmäßig vorhandenen Sicherheitsfunktionen wie MAC-Adressenfilterung und WEP ungenügend sind; alles weitere ist vom Anforderungsprofil eines Netzes abhängig. [5]

## Zusammenfassung

Die 802.11-Technologie bietet eine Reihe von Vorteilen. Sie beruht auf international akzeptierten, weit verbreiteten und herstellerunabhängigen Standards. Deshalb ist Interoperabilität zwischen Produkten verschiedener Hersteller gegeben. Die verwendeten Frequenzen sind Teil des ISM-Bandes und können in den meisten Staaten der Welt lizenzfrei, d. h. im Rahmen einer Allgemeinzuteilung genutzt werden. Die Technologie ermöglicht es, eigene Kommunikations-Infrastrukturen aufzubauen und die »letzte Meile« (Verbindung vom Haushalt zu Provider oder Telefonschaltzentrale) zu überspringen. Community-Netze auf 802.11-Basis machen die letzte Meile zur ersten Meile – die Nutzerinnen stehen im Vordergrund und nicht die Telefonfirmen und kommerziellen Provider. 802.11-Netze können dazu dienen, Konnektivität im öffentlichen Raum herzustellen oder semi-private Netze aufzubauen. Innerhalb dieser selbst-

organisierten Netze fallen außer den Investitionskosten und der Arbeit zum Erhalt der Systeme keine zusätzlichen Kosten (z. B. Leitungsgebühren) an. Breitbandige Kommunikation zwischen lokalen Gemeinschaften in selbstverwalteten Netzen wird möglich, Zugangskosten werden vermindert und andere Zugangsbarrieren abgebaut. Die Technologie eignet sich auch besonders für temporäre, öffentlich nutzbare Infrastrukturen bei verschiedensten Ereignissen oder Veranstaltungen. Breitbandinternet kann in ländliche Gebiete gebracht werden, wo es ansonsten schwierig oder unmöglich wäre, Zugänge mit hoher Datenrate zu erhalten. Dasselbe gilt für Entwicklungsländer mit veralteten oder nicht vorhandenen Kommunikationsinfrastrukturen. Anwendungen wie Voice-over-IP (Internettelefonie) ersetzen traditionellen leitungsgebundenen Verkehr. Freie Netze sichern den Erhalt freier Kommunikationsmöglichkeiten und freier Medien.

#### Literatur

- [1] LAN/MAN Standards, <http://www.ieee802.org/>
- [2] WLAN Kanarische Inseln, Weitenrekord, <http://www.canariaswireless.net/>
- [3] IPsec – Standard, der den Aufbau von sicheren IP-Verbindungen (z. B. VPN-Verbindungen) ermöglicht. Er wird verwendet zur Verschlüsselung als Schutz gegen unbefugtes Mitlesen, zur Authentisierung der Nachricht (Beweis der Unverfälschtheit einer Nachricht – Paketintegrität), zur Authentisierung des Absenders (unzweifelhafte Zuordnung eines Senders/Empfängers) und zur Verwaltung von kryptographischen Schlüsseln.
- [4] SSH – Secure Shell, ein kryptographisches Protokoll und darauf basierende Programme für die sichere Datenübertragung. Es baut ähnlich wie Telnet eine Verbindung mit einem anderen Rechner auf, ermöglicht zuverlässige gegenseitige Authentifizierung der Partner sowie Integrität und Vertraulichkeit der ausgetauschten Daten in unsicheren Netzen.
- [5] Auch ungeschützte Verbindungen im Internet sind unsicher; die Tatsache, dass Funktechnologie eingesetzt wird, macht die drahtlosen Netze nicht automatisch unsicherer. Eine etwas ausführlichere Behandlung der Sicherheitsthematik findet sich im Kapitel East End Net/Free2air.

## Gesetze und Vorschriften, die WLAN betreffen

Funknetze sind nicht nur von Gesetzen und Vorschriften zur Regulierung elektronischer Kommunikationsnetze betroffen, sondern auch von jenen für die Frequenznutzung des elektromagnetischen Spektrums. Auf weltweiter Ebene wird die Frequenznutzung von der International Telecommunications Union (ITU) koordiniert, die regelmäßig alle zwei Jahre die World Radio Conferences organisiert. Auf europäischer Ebene erfolgte die Koordination der Funkpolitik bisher überwiegend im Rahmen der Conférence Européenne des Postes et Télécommunications (CEPT), einem 1959 gegründeten Gremium der nationalen Monopolbehörden. Spektrumsfragen werden innerhalb der CEPT im European Radiocommunications Committee (ERC) besprochen. Zusätzlich hat die EU vor relativ kurzer Zeit eine eigene »Spectrum Policy Task Force« gegründet, die politische Leitlinien und Ziele definieren sollte.

Mit der »Frequenzentscheidung« [1] der EU wurde die Einrichtung eines Funkfrequenzausschusses beschlossen, der in Kooperation mit ITU und CEPT die europäischen Frequenzuteilungen koordinieren soll. Diese wurden bisher als »Empfehlungen« (man nennt es Empfehlungen, da sich Regierungen nicht gerne Vorschriften machen lassen, aber eigentlich sind diese schon ziemlich verbindlich) von ITU, WRC und CEPT/ERC formuliert. Auf nationalstaatlicher Ebene ist in Deutschland das Bundesministerium für Wirtschaft und Arbeit (BMWi) für linguistische Unappetitlichkeiten wie die Frequenzbereichszuweisungsplanverordnung zuständig. Damit wird festgelegt, welcher Teil des Spektrums von welchen Funkdiensten genutzt werden darf. Für die konkrete Festlegung der Regeln für die einzelnen Slots ist die Regulierungsbehörde (RegTP – [www.regtp.de](http://www.regtp.de)) zuständig. Ihr obliegt auch die Regulierung der Telekommunikation in der BRD.

Das regulatorische Klima für WLANs lässt sich derzeit als günstig beschreiben. Mit dem Aktionsplan eEurope 2005 haben sich die Mitgliedstaaten der EU ehrgeizige Ziele für die Entwicklung der Kommunikation in elektronischen Netzen gesetzt. Der Nutzung breitbandiger Kommunikationstechnologien wird eine große Bedeutung für die wirtschaftliche Innovation beigemessen. WLAN, das in EU-Papieren meist R-LAN (von Radio-LAN) genannt wird, wurde als alternative Breitbandtechnologie – neben Kabelmodem und DSL – identifiziert. Um der Umsetzung der Ziele des Aktionsplans eEurope 2005 näher zu kommen,

wurde ein gemeinsamer Rechtsrahmen für elektronische Netze und Dienste beschlossen. Dieser besteht aus einer Rahmenrichtlinie [2] und mehreren Einzelrichtlinien, darunter die Richtlinie über die Genehmigung elektronischer Netze. Diese »Genehmigungsrichtlinie« [3] empfiehlt, dass für die »Genehmigung der Bereitstellung elektronischer Kommunikationsnetze und -dienste das am wenigsten schwerfällige Genehmigungsverfahren verwandt werden sollte« und dass diese folglich »nur von einer Allgemeingenehmigung abhängig gemacht werden« solle. Das bedeutet, dass für die meisten Anbieter elektronischer Kommunikationsnetze und -dienste die Verpflichtung zur Einholung einer Lizenz abgeschafft wurde.

Den Mitgliedstaaten wurde bis zum 24.07.2003 Zeit gegeben, das Richtlinienpaket in nationale Gesetzgebung umzusetzen. Am 25.07.2003 traten die neuen Bestimmungen in Kraft. Deutschland hatte es zu diesem Zeitpunkt versäumt, das Telekommunikationsgesetz zu novellieren. Die Genehmigungsrichtlinie brachte dennoch eine Verbesserung mit unmittelbarer Wirkung, da die Regierung schadenersatzpflichtig ist, falls Bürgern durch ihr Versäumnis bei der Richtlinienumsetzung Nachteile entstehen.

Im März 2003 folgte eine Empfehlung der EU-Kommission [4], die sich direkt auf WLANs bezieht. Mit Bezugnahme auf die Genehmigungsrichtlinie empfiehlt die Kommission, die Nutzung öffentlicher WLANs nur von einer Allgemeinzuteilung abhängig zu machen. Weiter heißt es dort:

»Funk-LAN-Systeme dürfen entweder das Frequenzband von 2400,0–2483,5 MHz (nachfolgend »2,4-GHz-Band« genannt) oder die Frequenzbänder von 5150–5350 MHz oder von 5470–5725 MHz (nachfolgend »5-GHz-Bänder« genannt) ganz oder teilweise nutzen.« Das Wort »teilweise« bezieht sich auf den oberen Bereich des 5-GHz-Bandes, der in einigen Ländern für Radar benutzt wird.

Die Nutzung des 2,4-GHz-Bandes [5] und der 5-GHz-Bänder [6] durch WLANs im Rahmen einer Allgemeinzuteilung war von der Regulierungsbehörde ohnehin bereits bewilligt worden. Für WLAN-Betreiber stellt die neue Regelung jedoch insofern eine Verbesserung dar, als damit die Gefahr gebannt wurde, unter die Lizenzpflicht nach Paragraph 6 des TKG zu fallen. Grundstücksübergreifende Funknetze, für deren Benutzung Geld verlangt wurde, wären in der Vergangenheit lizenzpflichtig gewesen. Es war nicht unbedingt klar, ob das auch auf freie offene Bürgernetze zugefallen hätte. Durch ihren nichtgewerblichen Charakter

waren sie möglicherweise sowieso von dieser Bestimmung ausgenommen. Nun ist diese Unsicherheit aber beseitigt und es heißt »freies Funken«.

Weiterhin gültig ist die Bestimmung, dass grundstücksübergreifende Funknetze angemeldet werden müssen. Das entspricht jedoch nicht dem Einholen einer Genehmigung. Dabei geht es hauptsächlich um die Vermeidung bzw. Beseitigung von Störungen, indem die Existenz der Anlagen und Namen und Kontaktinformationen der Betreiber bekannt sind. Außerdem müssen die »in Verkehr gebrachten Geräte« die Spezifikationen des europäischen Standards ETS 300 328 [7] einhalten und den technischen Zulassungsvorschriften (CE-Zeichen) entsprechen.

Zusammenfassend lässt sich also sagen, dass dem Betrieb einzelner Hotspots und auch größerer drahtloser Netze keine gesetzlichen Hindernisse und Auflagen im Weg stehen, insbesondere wenn diese Netze nicht gewerblich betrieben werden. Diese Aussage bezieht sich jedoch nur auf die physisch-materielle Ebene der drahtlosen Netze. Auf der inhaltlichen Ebene, d. h., wenn Anwendungen ins Spiel kommen, droht immer noch eine Menge Ungemach. Freie Netze sind nicht automatisch von Copyright, Patentrecht, Markenschutz, Jugendschutz usw. ausgenommen. Ein gewisser Freiraum, z. B. hinsichtlich File-Sharing von Musikdateien, kann wahrscheinlich gewahrt bleiben, sofern sich die Kommunikation auf eine geschlossene Nutzergruppe in einem freien drahtlosen Netz beschränkt. Auch sollte man davon ausgehen können, dass die Telekommunikationsüberwachungsverordnung [8] nicht greift, wenn Netze als verteilte Ressource von lauter unabhängigen Knoteninhabern betrieben werden. Getestet wurden solche Annahmen allerdings noch nicht und es ist zu hoffen, dass diese Rechtsauslegung Bestand hat.

#### Literatur

- [1] Entscheidung Nr. 676/2002/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen Rechtsrahmen für die Funkfrequenzpolitik in der Europäischen Gemeinschaft
- [2] Richtlinie 2002/21/EG des Europäischen Parlaments und des Rates vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), [http://europa.eu.int/information\\_society/topics/telecoms/regulatory/new\\_rf/documents/l\\_10820020424de00330050.pdf](http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/l_10820020424de00330050.pdf)
- [3] Genehmigungsrichtlinie, [http://europa.eu.int/information\\_society/topics/telecoms/regulatory/new\\_rf/documents/l\\_10820020424de00210032.pdf](http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/l_10820020424de00210032.pdf)

- [4] 32003H0203, Empfehlung der Kommission vom 20. März 2003 zur harmonisierten Gewährung des öffentlichen Funk-LAN-Zugangs zu öffentlichen elektronischen Kommunikationsnetzen und -diensten in der Gemeinschaft (Text von Bedeutung für den EWR), Amtsblatt Nr. L 078 vom 25.3.2003 S. 0012–0013, [http://europa.eu.int/smartapi/cgi/sga\\_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=de&numdoc=32003H0203&model=guichett](http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=de&numdoc=32003H0203&model=guichett))
- [5] WLAN 2,4 GHz, »Allgemeinzuteilung von Frequenzen für die Benutzung durch die Allgemeinheit für Funkanlagen für die breitbandige Datenübertragung im Frequenzbereich 2400–2483,5 MHz (RLAN-Funkanlagen)«, Amtsbl. 22/1999, Vfg 154
- [6] WLAN 5 GHz, »Allgemeinzuteilung von Frequenzen in den Bereichen 5150 MHz–5350 MHz und 5470 MHz–5725 MHz für die Nutzung durch die Allgemeinheit in lokalen Netzwerken; Wireless Local Area Networks (WLAN-Funkanwendungen)«, Amtsbl. 22/2002, Vfg 35
- [7] ETS 300 328 Radio Equipment and Systems (RES); Wideband transmission systems; technical characteristics and test conditions for data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques, Suchmaschine für ETSI Standards, <http://webapp.etsi.org/WorkProgram/SimpleSearch/QueryForm.asp>
- [8] Telekommunikations-Überwachungsverordnung (TKÜV), <http://www.bmwi.de/Navigation/Wirtschaft/telekommunikationundpost,did=6018.html>

#### Weitere Informationen

- BMWI-Website, Rechtsgrundlagen Telekommunikation, [http://www.bmwi.de/Navigation/Wirtschaft/Telekommunikation\\_20und\\_20Post/telekommunikationspolitik/rechtsgrundlagen.html](http://www.bmwi.de/Navigation/Wirtschaft/Telekommunikation_20und_20Post/telekommunikationspolitik/rechtsgrundlagen.html)
- Regulierungsbehörde, <http://www.regtp.de>

## Kommunikationsmodell Netzfreiheit

Das OSI-Referenzmodell und die TCP/IP-Protokollstapel sind in Schichten aufgebaute Modelle der Netzkommunikation. Darüber brütend, wie sich denn nun eigentlich die Freiheit in freien Netzen definiert, kam ich zu dem Ergebnis, dass es naheliegend ist, auch hierbei eine Art Schichtenmodell zu verwenden. Es gibt eine Reihe von Freiheitsbegriffen – philosophische, natur- und staatsrechtliche. Diese sind jedoch wenig aussagekräftig bezüglich der Freiheit, die in Netzen zu finden ist. Denn es geht nicht darum, einen allumfassenden, absoluten Freiheitsbegriff zu verwenden. Die Freiheiten, um die es in diesem Buch geht, sind konkreter und praktischer Natur und lassen sich mit den Ebenen der Netzkommunikation in Beziehung setzen. So landete ich bei einem »Kommunikationsmodell Netzfreiheit«. Dieses ist in vier Schichten aufgebaut:

- Physisch-materielle Netzfreiheit
- Zugangsfreiheit
- Kommunikationsfreiheit
- Medienfreiheit

Auf der physisch-materiellen Ebene geht es darum, die Möglichkeit zu haben, Netzwerke aufzubauen und miteinander zu verbinden. Auf der Ebene der Zugangsfreiheit geht es um das Recht oder den Grad der Möglichkeit, diese Netze zu nutzen. Kommunikationsfreiheit ist die Freiheit, mit wem immer man will in Einzel- oder Gruppengesprächen zu kommunizieren. Medienfreiheit ist die Freiheit, die Netze für Massenkommunikation zu nutzen.

Diese Ebenen stehen miteinander in wechselseitigen Beziehungen, diese nicht ganz so hierarchisch wie im OSI-Modell sind. Schließlich handelt es sich im einen Fall um Technik, im anderen um ein soziales Interaktionsmodell. Man kann das Modell auch in die Ebene kippen und als überlappende Mengen darstellen.

Diese verschiedenen Freiheiten lassen sich abhängig von einer Reihe von Faktoren in verschiedenen Freiheitsgraden realisieren. Jede Schicht wird von internen und externen Faktoren beeinflusst, die miteinander in Wechselwirkung stehen und den Grad der Freiheit determinieren.

Interne Faktoren auf der physisch-materiellen Netzwerkschicht z. B. sind die Technologie und ihre Eigenschaften, der Preis, die Organisationsform, Besitzverhältnisse und vorhandene Ressourcen. Externe Fakto-

ren sind u. a. die Gesetzgebung und andere regulatorische Rahmenbedingungen, das Vorhandensein verbindungswilliger Netzwerkpeers, die Verbreitung und Akzeptanz der Technologie in der Gesellschaft und das allgemeine sozio-politische Klima, das sich aus Einflüssen wie z. B. Wettbewerb, Wirtschaftszyklen, Krisen und anderer Rahmenbedingungen zusammensetzt.

Es ist zu betonen, dass im Prinzip jede Netzwerktechnologie »befreit«, also zur Grundlage eines freien Netzes werden kann. Je nach den Rahmenbedingungen und Anforderungen können die verschiedensten Netzwerktechnologien verwendet werden, ob Telefon- oder Kabelnetz, Ethernet, Ethernet über Wechselstrom, Glasfaser, GSM und UMTS. WLAN ist ein Sonderfall und jetzt gerade besonders populär. Die Technologie hat bestimmte Eigenschaften, die es opportun machen, sie derzeit zu verwenden. Für technisch versierte Leute sind alle Netze »frei«, man denke z. B. an Phreaker (Telefon-Hacker). Doch das Hauptaugenmerk in diesem Buch ist nicht auf die Ausbeutung technischer Schlupflöcher, sondern auf Netzwerke gerichtet, die im Rahmen der Gesetze mit legitimen Mitteln aufgebaut werden und bewusst frei und offen zugänglich gemacht werden. Die Dynamik der gesellschaftlichen und technischen Entwicklung eröffnet diesbezüglich die verschiedensten Optionen.

So sind z. B. Technologien im Laufe ihrer Lebensspanne, von der Entwicklung über die Verbreitungsphase bis hin zur Sättigungsphase, immer gerade mehr oder weniger »frei«, und diese Freiheit realisiert sich auf den verschiedenen Ebenen des Kommunikationsmodells. Sehr junge Technologien, für die sich noch kein weithin etablierter gesellschaftlicher Nutzen gefunden hat, aber auch alte Technologien, die aus der Sicht der bestimmenden wirtschaftlichen Interessen bereits wieder überholt sind, können freien Netzwerken strategische Vorteile bieten.

Ein gutes Beispiel für den ersten Fall ist SMS. Die Textmessages, die einen gewaltigen Boom erlebt haben, waren anfangs frei im Sinne von gratis, eine Beigabe zur Ware Mobiltelefon. Inzwischen hat sich das Blatt gewandelt und »txting« kostet. Wenn UMTS dann endlich eingeführt ist, wird möglicherweise GSM für die Wirtschaft nicht mehr so interessant sein und es können Community-GSM-Netze aufgebaut werden. Radio ist ein gutes Beispiel für den zweiten Fall. Bis vor nicht allzu langer Zeit war es strikter Kontrolle unterworfen. Mit dem Wechsel auf digitale Übertragungsmethoden werden Frequenzen frei. Damit verbessern sich die Chancen für freie Radios, also z. B. lokale Radios, Nischen- und Minderheitenprogramme, nichtkommerzielle, von Gemeinschaften getra-

gene Radios. »Radio ist aber kein Netzwerk«, werden manche sagen, weil die Kommunikation nur in eine Richtung geht. Ich denke, Radio gehört dennoch hierher, da freie Radios von basisdemokratischen, sozialen Netzwerken betrieben werden. Und die Geschichte freier Radios enthält wichtige Lehrbeispiele für freie Netze.

Das Internet wurde bis vor nicht allzu langer Zeit als ein freies Netz bezeichnet. Auf einer gewissen Ebene ist es das auch nach wie vor. Die Forscher, die das Internet entwickelt haben, preisen dessen offene Netzwerkarchitektur. TCP/IP verkörpert »eine entscheidende zugrunde liegende technische Idee, nämlich jene einer offenen Netzwerkarchitektur. In einer offenen Netzwerkarchitektur können Netzwerke verschiedene Gestaltungs- und Funktionsweisen haben und jedes hat womöglich auch seine eigene Nutzerschnittstelle. [...] Es gibt ganz allgemein gesprochen keinerlei Beschränkungen bezüglich der Art von Netzwerk, das angeschlossen werden kann. [...] Ein Schlüsselkonzept für das Internet ist, dass es nicht für eine bestimmte Entwicklung gedacht wurde, sondern als eine allgemeine Infrastruktur, auf deren Grundlage Anwendungen entwickelt werden konnten.« [1]

Wie die Entwickler des Internets betonen, von denen obiges Zitat stammt, sind es die Eigenschaften der Internetprotokolle, die das Internet zu einem (zumindest teilweise) freien Netz machen. Neben deren technischen Eigenschaften, wie z. B. besonders »verbindungsfreundlich« zu sein, ist ein wichtiger Umstand, dass die Protokolle frei zugänglich sind. Sie sind im Netz zu finden, jeder kann sie herunterladen und einsehen. Sie sind unabhängig von Herstellern und Rechnerplattformen. Wer die technischen Fähigkeiten besitzt, kann auf der Basis von TCP/IP neue Anwendungen entwickeln. Auf der Anwendungsschicht können mit einem hohen Flexibilitätsgrad neue »Medien« konstruiert werden. Diese rein virtuellen, völlig softwarebasierten Medientypen greifen auf die Dienste von TCP/IP zurück. Sie benötigen keine eigene, dedizierte physische Netzwerkschicht, sondern können auf den vorhandenen Infrastrukturen laufen.

Verschiedenste kollaborative Medien wie z. B. Wikis, Weblogs, Peer-to-Peer-Netze für File-Sharing oder z. B. auch Freenet, ein besonders schwer zu überwachendes Peer-to-Peer-Netz für Inhalte aller Art [2], sind in den letzten Jahren entstanden. Aber auch ältere Anwendungen wie E-Mail, Usenet und IRC lassen sich schwer kontrollieren. Das Internet eignet sich besonders für die Ausübung der Kommunikations- und Medienfreiheit. Staatliche Einflüsse wie Zensur und Überwachung und

von den Copyright-Industrien ausgeübter Druck versuchen, diese Freiheiten einzuschränken.

Auf der physisch-materiellen Ebene und der Zugangsebene würde ich das Internet allerdings kaum als frei bezeichnen. Zugangsschranken, finanzielle Schranken und eine Flut an Gesetzen haben die Freiheit auf diesen Ebenen bereits ziemlich vermiest. Dass wir heute von freien Netzen überhaupt sprechen können, verdankt sich jedoch den grundlegenden Eigenschaften des Internets. Freie Netze sind also kein Gegenentwurf zum Internet (auch wenn das bei vereinzelt Projekten so aussehen mag), sondern eine logische Fortsetzung der Ideen, auf denen das Internet ursprünglich aufgebaut war. Freie Netze setzen da an, wo das Internet am unfreiesten geworden ist, an der physisch-materiellen Ebene und der Zugangsebene. Indem nichtkommerzielle Netze aufgebaut werden, die im Besitz ihrer Nutzerinnen sind, stehen wieder offene Netze mit geringeren Zugangsbarrieren und nach selbst gemachten Regeln zur Verfügung.

#### Literatur

- [1] A Brief History of The Internet, Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff,  
*<http://www.isoc.org/internet/history/brief.shtml>*
- [2] Freenet, *<http://www.freenet.org>*

## Vom Boom zur Pleite: Die New Economy im Rückspiegel

Die Vereinigten Staaten und Großbritannien erfreuten sich von den frühen neunziger Jahren bis zu deren Ende eines kontinuierlichen Wirtschaftswachstums. Wesentlich schneller, als die Wirtschaft wuchs, stiegen die Börsenkurse vieler Unternehmen. Das Millenniumsieber erfasste auch viele andere Märkte in hoch entwickelten Industriestaaten rund um die Welt. Diese Entwicklung wurde mit der Privatisierung des Internets, dessen Öffnung für Firmen und Individuen und dem Entstehen neuer Industrien in Zusammenhang gebracht – daher sprach man von einer Internet- oder Dotcom-Bubble. Doch wie viel hatte diese sich immer mehr ausdehnende Spekulations-Blase, die irgendwann einfach platzen musste, tatsächlich mit dem Internet zu tun? Das Internet wurde zu einer Chiffre, die für alles stand, was mit Information, Kommunikation, Neuen Medien zu tun hatte. Das Fieber erfasste jedoch auch andere Börsenwerte, und auch der Dow Jones, auf dem viele alte Industrien gelistet sind, kletterte auf nie zuvor erreichte Höchstwerte. Nach dem Crash litten besonders die Internet- und Technologiewerte (während, unterstützt durch weltpolitische Ereignisse, die Gefahr einer längeren, allgemeinen Rezession noch nicht gebannt ist, aber das steht auf einem anderen Blatt). Das Internet wurde wiederum verantwortlich gemacht, als auf den Boom die Pleite folgte. Viele Investitionen wurden nicht zu Ende geführt, der Neue Markt verschwand in Deutschland gleich wieder ganz von der Bildfläche, und in der noch fortwährenden Phase der »Marktkorrektur« mangelt es im gesellschaftlichen Mainstream an Vertrauen in die eben noch so bejubelten neuen Netzwelten und alles, was mit diesen assoziiert wird.

Doch der Millenniums-Boom hatte nicht nur mit dem Internet zu tun. Dieses war bestenfalls einer von mehreren Katalysatoren für eine Entwicklung, die eine wesentlich längere Vorgeschichte hat. Ein wichtiger Faktor ist, was ich das neoliberale Projekt nennen möchte, das spätestens mit Reagan und Thatcher begann und einen fundamentalen Umbau der Gesellschaft zum Ziel hatte. Staatliche Monopolbetriebe wurden privatisiert, die Rechte der Arbeitnehmer abgebaut und, insbesondere in England, die Macht der Gewerkschaften zerschlagen – und das ganz wörtlich, als Thatcher den Streik der Kohlekumpel niederknüppeln ließ. Der neoliberale Angriff richtete sich nicht nur gegen die lautstarken und sichtbaren Organe der Linken, sondern gegen die Möglichkeit der

Arbeitnehmer grundsätzlich, sich zu organisieren und als Kollektiv zu handeln. Die erzwungene Entsolidarisierung der Gesellschaft wird durch Thatchers berühmtes Diktum »there is no such thing as a society« unterstrichen. Indem sie die Existenz einer »Gesellschaft« verleugnet, wird auch dem Gemeinschaftsinteresse eine Absage erteilt. Sozialdarwinismus und die Maximierung des Profitstrebens wurden als die einzigen gültigen Motive anerkannt. Dies wurde begleitet von sozialkonservativen Vorstellungen von der Familie als der einzigen legitimen Form des sozialen Zusammenhalts. Zumindest innerhalb der Familie ist der permanente Wirtschaftskrieg teilweise suspendiert. Solche extremen Anschauungen führten zu Auswüchsen wie z. B., dass alleinerziehende Mütter, die von der Sozialhilfe leben, plötzlich zu Feinden der Gesellschaft erklärt wurden. Solche Tendenzen fanden in den Vereinigten Staaten und in Großbritannien ihren schärfsten Ausdruck, doch auch in Deutschland unter Kohl und in den meisten westlichen Ländern wurde wirtschaftspolitisch eine ähnliche Linie gefahren. Diese Linie wurde unter Clinton, Blair und Schröder mit leichter Nuancenverschiebung unter Begriffen wie »The Third Way« und »Neue Mitte« bis heute beibehalten.

Der wirtschaftliche Neoliberalismus führte in den achtziger Jahren zu einer deutlichen Aufwertung der Börse und des Finanzsektors gegenüber den produzierenden Industrien (und deren Arbeitnehmern). Der Handel mit Währungen und derivativen Finanzinstrumenten gewann eine neue Qualität. Die Vervielfachung der Umsätze auf diesen Märkten wurde möglich durch die Einführung des elektronischen Wertpapierhandels und die Vernetzung der Finanzplätze und wichtigsten Global Player. Die Global Cities entstanden, mit ihren spezifischen Infrastrukturen und Demographien. In der Vergangenheit war das Börsengeschäft in der City of London mit Gentlemen mit Bowler-Hüten und Nadelstreifenanzügen assoziiert worden. In den achtziger Jahren hielt ein neuer, jüngerer und aggressiverer Typus Einzug. Unter dem Motto »Greed is good« (Gier ist gut) produzierten Thatcher-Boys einen Börsenboom in den achtziger Jahren, der mit dem Crash von 1987 zwar eine Delle erhielt, aber bald wieder Fahrt aufnahm. Mit dem Fall des Eisernen Vorhangs sahen sich die Anhänger des neoliberalen Projekts in ihren Bestrebungen bestärkt. Der Kapitalismus habe gewonnen, weil er die der Natur des Menschen am besten entsprechende Wirtschaftsordnung sei, meinten sie. Ein weiteres berühmtes Thatcher-Zitat schien sich damit bewahrheitet zu haben: »There is no alternative«, es gäbe keine Alternative zum Neoliberalismus.

Anfang der neunziger Jahre befanden sich die USA, trotz eines gerade gewonnenen Golfkriegs, in einer Wirtschaftskrise. Der Schlachtruf, »it is the economy, stupid«, verhalf Bill Clinton 1992 zum Wahlsieg. Die Regierung Clinton/Gore erklärte in ihren ersten Regierungsjahren die Metapher »Datenautobahn« zum Hoffnungsträger für eine Wiederbelebung des Wirtschaftswachstums. 1993 ging das Weiße Haus online. Im selben Jahr begann das selbsterklärte Leitmedium der »digitalen Revolution«, das Magazin Wired, die Maximen zu formulieren. Wired wurde in San Francisco herausgegeben, das bis dahin nicht viel mehr gewesen war als ein Künstlerdorf am Nordrand des wirtschaftlich wesentlich bedeutsameren Silicon Valley. Das Internet, so die Wired-Botschaft, würde einen tief greifenden Wandel auf allen Ebenen der Gesellschaft auslösen. Wer diesen Wandel verstehe und frühzeitig sein Fähnchen nach dem Wind richte, werde gewinnen, die anderen, die alten Dinosaurier-Industrien, würden verlieren und vom Erdboden verschwinden. Dank seiner inhärenten Eigenschaften würde das Internet zum Abbau von Hierarchien führen und zum Umbau in eine dezentralisierte, partizipative und damit immanent demokratischere Gesellschaft beitragen. Diese befürwortenswerten Veränderungen würde das Internet aber nur dann in die Wege leiten können, wenn es von staatlichen Eingriffen möglichst verschont bliebe und die Exploration der Möglichkeiten des Mediums der Privatwirtschaft anvertraut werden würde – eigentlich ironisch, wenn man bedenkt, dass die Entwicklung des Internets aus staatlichen Mitteln gefördert worden war und der Backbone zum damaligen Zeitpunkt immer noch von staatlichen Institutionen finanziert, betrieben und verwaltet wurde.

Wired versah seine Mischung aus Wirtschaftsliberalismus und technik-deterministischen Ideen über sozialen Fortschritt mit einer weiteren Zutat, einem kulturellen Liberalismus, der von den Anschauungen und Werten der diversen Subkulturen in SF und der Bay Area gespeist wurde. Das Magazin verschmolz eine extrem wirtschaftsfreundliche libertäre Ideologie mit politisch und kulturell progressiv klingenden Diskursen. Technologie, zuvor eine Angelegenheit für Nerds und Geeks, wurde plötzlich hip, jugendkulturell, subversiv, trendy. Es wurde aber auch hip und trendy, mit diesen Technologien unternehmerisch aktiv zu werden. Die Werte von Subkulturen, die sich zuvor apolitisch oder explizit anti-kommerziell gegeben hatten, standen plötzlich nicht mehr im Widerspruch zu einer neuen Business-Kultur. [1] Der Internet-Entrepreneur erschien als neuer Held auf der Wired-Plattform. Jung, unkonventionell

gekleidet, egalitär denkend, voller Enthusiasmus für den Aufbau von Unternehmen, die zugleich Profit abwerfen und die Welt verbessern würden.

Diese Saat schien aufzugehen, als Netscape 1995 an die Börse ging und starke Nachfrage den Aktienwert des Unternehmens auf zwei Milliarden Dollar hoch trieb. Das, obwohl Netscape sein wichtigstes Produkt, den Web-Browser, verschenkte und bei relativ geringen Umsätzen Verluste schrieb. Netscapes Börsengang wird als der Wendepunkt in der kommerziellen Internetgeschichte verstanden. Von da an schienen traditionelle Bewertungskriterien für Internetunternehmen außer Kraft gesetzt. Angesichts unendlicher Wachstumschancen und zu erwartender zukünftiger Profite waren die gegenwärtigen Einnahmen und Ausgaben eine redundante Information. Der Begriff New Economy begann sich einzubürgern und damit die Implikation, dass für Internetfirmen andere Regeln gelten. Die Informations- und Kommunikationstechnologien würden einen wirtschaftlichen Paradigmenwechsel auslösen. Anstatt zyklischer Auf- und Abschwünge würde es in der New Economy nur fortgesetztes Wachstum geben. Die inhärente Logik der Technologie und deren Auswirkungen auf die Produktivität würden die wirtschaftlichen Gesetze der Schwerkraft außer Kraft setzen. [2]

Trotz bestens funktionierender Propaganda entging es Beobachtern nicht, dass das neue Medium kein Geschäftsmodell hatte – niemand wusste, wie man damit tatsächlich Geld verdienen konnte, abgesehen von Hardwareherstellern und Telefonfirmen (die wohl gar nicht wussten, wie sie zu ihrem Glück kamen). Der Internet-Mythos verkaufte sich auf der Basis von Eigenschaften, die noch aus seiner akademischen Unschuldphase stammten, als Werbung im Netz verboten war und Geschenkökonomie vorherrschte. Genau dieselben Eigenschaften machten es jedoch schwierig, aus der »freien« Kultur des Netzes eine Geldmaschine zu machen. Kein Wunder, denn schließlich war die Netzwerkarchitektur des Internets nicht auf Geldverdienen ausgelegt.

Gegen Ende 1996 warnte Alan Greenspan, Chef der US-Bundesbank, vor dem »irrationalen Überschwang« (engl. »irrational exuberance«) der Anleger. Prolongiertes Wachstum seit 1980 hatte den Börsenindex Dow Jones auf über 6000 Punkte steigen lassen. Die zugrunde liegenden Wirtschaftsdaten, die »fundamentals«, korrespondierten jedoch nicht mit diesem Wachstum. Greenspan sah deshalb bereits 1996 die Gefahr einer spekulativen Blase, deren Platzen die gesamte Wirtschaft schwer schädigen könnte. Doch der eigentliche Boom hatte da noch kaum begonnen.

Die etablierten Großunternehmen hatten das Internet noch kaum für sich entdeckt. In Deutschland hatten nur wenige der »alten Medien« überhaupt eine Internetpräsenz. Skepsis gegenüber dem Internet war weit verbreitet und Kulturkonservative prophezeiten, dass diese Mode bald wieder vom Erdball verschwinden würde. Stattdessen stieg der High-Tech-Index NASDAQ zwischen Oktober 1998 und März 2000 um 256 Prozent auf 5048,62 Punkte [3], seinen wahrscheinlich für lange Zeit vorläufigen Höhepunkt, denn im Juli 2003 krebste der NASDAQ in der Region von 1700.

Robert Shillers Buch »Irrational Exuberance« leistet eine Analyse des Wachstums der Aktienmärkte in den neunziger Jahren. Es erschien im März 2000, genau zu dem Zeitpunkt, als der NASDAQ abzustürzen begann. Shiller wurden prophetische Gaben zugesprochen und das Buch wurde ein Bestseller. Dabei macht er nichts anderes, als die Marktentwicklung in eine historische Perspektive zu rücken. Die Geschichte zeigt, dass alles, was steigt, irgendwann wieder fällt. In der Steigphase jedoch ist es häufig der Fall, dass von einer »Neuen Ära« gesprochen wird. Das Wachstum wird mit einer Rhetorik ähnlich der von der New Economy zu rationalisieren versucht. Im Juli 1997 veröffentlichte Wired eine Titelseitegeschichte unter der Überschrift »The Long Boom«. Darin wurde eine Fortsetzung des Booms für weitere 25 Jahre versprochen. Der Artikel wird heute unter »peinlichste je veröffentlichte Story« verbucht.

Es wäre jedoch völlig verfehlt, Wired alleine für den Hype um die New Economy verantwortlich zu machen. Das Medium hatte seine eigentliche Glanzphase in den frühen Jahren, bevor der Boom begann, und neben heute peinlichen Storys über lange Booms und Push-Medien veröffentlichte es eine große Anzahl hervorragend recherchierter, langer Artikel über Netzthemen. Hätten sie den Mund nicht so voll genommen, könnten einem die ehemaligen Wired-Herausgeber beinahe Leid tun, wurde Wired doch mit dem Verkauf an das Firmenkonglomerat Condé Nast eines der ersten Opfer der Gegenoffensive der »alten Medien«.

Wireds Führungsrolle wurde von einem neuen Typ an New-Economy-Medien abgelöst, die sich wohlweislich jeglicher Prophezeiungen enthielten und nur mehr von Geld und Erfolgchancen handelten. Wie Shiller analysiert, kam es zu einem sprunghaften Anstieg an Berichten über die Börse in Presse und Fernsehen. Diese Welle positiver PR veranlasste einen neuen Typus Investor, sich am großen Börsenspiel zu beteiligen. Aktienhandel über das Internet gab normalen Bürgern die Möglichkeit, zu geringen Gebühren mit Wertpapieren zu handeln. Amerika

wurde eine Nation von Day Traders. Anstatt auf langfristige Zinserträge zu setzen, begannen Bürger ihr Ersparnis auf den NASDAQ zu wetten. Pensionsreformen schürten diese Entwicklung. 1999 wurde zum offiziellen Boomjahr und der konzertierte Hype führte zu bizarren Bewertungen von Firmen. Der Internetspielwarenhändler eToys wurde kurz nach seinem Börsengang 1999 mit acht Milliarden Dollar bewertet, zwei Milliarden mehr als die »Ziegel und Mörtel«-Spielzeugkette Toys »R« Us. Der wenige Jahre zuvor relativ unbedeutende Provider AOL konnte den Mediengiganten Time Warner in einem als Fusion getarnten Vorgang übernehmen. Es ist kaum nötig hinzuzufügen, dass beider Höhenflug nicht lange währte. eToys ist Pleite gegangen, während AOLTW noch immer nach Synergien zwischen alten und (nicht mehr ganz so) neuen Medien sucht.

Als auf den hyperventilierenden Jahrtausendwenderummel die Katerstimmung folgte, taten manche geradezu so, als sei es ein Versagen der Technologie, dass ihre Hoffnungen auf schnellen Reichtum nicht eingetroffen waren. Hatte man eben noch die ethischen Werte und Konzepte, die mit dem Internet assoziiert wurden, in auf Werbesprüche reduzierten Fassungen brav nachgeplappert (Empowerment, blah, blah), so wurden genau diese Werte nun als »Illusionen« verdammt. Das Erstaunlichste an all dem ist, dass das Internet selbst während dieser ganzen Boom-und-Pleite-Phase relativ unbeeinträchtigt vor sich hin tuckerte. Es konnte den Ansturm neuer User verdauen, während sich unter der Oberfläche des WWW tektonische Verschiebungen anbahnten. Die Zahl der Internetnutzer und der Host-Rechner wuchs auch nach 2000 noch mit beachtlichen Raten. Die Investoren hatten das Vertrauen verloren, die Schönredner sprachen von einer »notwendigen Marktkorrektur«, doch das Internet wurde für die Nutzerinnen deshalb nicht weniger populär und die Ansätze der Netzkultur(en) [4] waren mit dem Scheitern der New Economy nicht automatisch ebenfalls gescheitert.

### **Die Entstehung einer neuen alten Netzkultur**

Denn nicht alle hatten sich von den Luftschlossern der New Economy blenden lassen. Parallel zur Kommerzialisierung des Internets und abseits vom Blitzlichtgewitter der Medien hatten neue, zunächst lose miteinander verwobene Bewegungen Momentum gewonnen. Diese speisten sich aus den Einflüssen der neuen sozialen Bewegungen der sechziger und siebziger Jahre ebenso wie aus den Werten der frühen Internetkultur.

Anstatt einer Warenökonomie wurde eine Geschenkökonomie des freien Austauschs geistigen Eigentums gepflegt. Die Hacker-Szene (der Begriff »Hacker« wird in diesem Buch meist in seinem ursprünglichen, positiven Sinn verwendet, bevor die Medien daraus ein Schimpfwort machten) und die »Multitudes«, die vielgestaltige, uneinheitliche Front der Globalisierungskritiker, bildeten die aktivsten Elemente dieser Bewegung. Vernetzung primär als sozialen, kulturellen und politischen Vorgang begreifend, formierten und organisierten sich kleine translokale Gemeinschaften mittels des Internets. Die freien Medien der Gegen- und Subkulturen, die freien Radios, Fanzines, Community-Medien, migrierten ins Netz. Mailinglisten, Chat-Kanäle, Webforen und zunehmend auch Peer-to-Peer-Software ermöglichten die Kommunikation in Gruppen und verstärkten damit das Potenzial zuvor marginalisierter Schichten. Klein- und Kleinstmedien, die unterhalb des Radars der Massenmedien und des gesellschaftlichen Mainstreams agieren, wurden davon begünstigt. Diese Ausübung der Medienfreiheit als Individuen und in Gruppen wurde jedoch nur möglich, weil Hacker dafür freie Software schrieben und damit die Werkzeuge für die neue Freiheit und Vielfalt bereitstellten. Freie Software ist nicht nur gratis, sondern auch geschützt durch eine Lizenz (bzw. mittlerweile eine Anzahl verwandter Lizenzen), die garantiert, dass die Software nicht privatisiert werden kann. Dadurch haben auch Inhalte und Kommunikationsplattformen, die auf freier Software beruhen, eine verbesserte Chance auf Langlebigkeit und Schutz vor Privatisierung. Das Modell der freien Software wurde darüber hinaus als Vorbild für andere Bereiche genommen und auf Genres wie Musik und Texte übertragen. Eine Copyleft-Bewegung entstand, die es sich zum Ziel setzte, möglichst viele kulturelle Artefakte als Gemeinschaftsgut von jeglichen Zugangsschranken zu befreien.

Die Internet-Bubble war geplatzt. Der Versuch, das Internet in einen elektronischen Versandwarenkatalog zu verwandeln, war fehlgeschlagen. Von ungebrochener Popularität erwies sich das natürliche Bedürfnis der zwischenmenschlichen Kommunikation. Nicht nur gesellschaftliche Avantgarde-Gruppen wie Hacker und Globalisierungskritiker, sondern breite Bevölkerungsschichten begannen sich an der Geschenkökonomie im Internet zu beteiligen. Anstatt Geld für Waren und Dienstleistungen zu bezahlen, ziehen es die meisten Nutzerinnen und Nutzer vor, sich in E-Mails auszutauschen, ihre Musiksammlungen anderen anzubieten, die eigene Homepage zu pflegen, nützliche Linklisten und Dokumentationen zusammenzustellen. Mit dem zunächst langsamen, aber stetigen Aufstieg

einer neuen/alten Netzkultur rückten wieder Werte wie Kooperation und Gemeinschaftssinn in den Mittelpunkt. Zweifel und Kritik am neoliberalen Projekt wuchsen. Baronin Thatchers Versicherung zum Trotz, dass es »keine Gesellschaft gibt«, brachte eine wachsende Zahl von Menschen durch ihre Handlungen das Gegenteil zum Ausdruck. Kooperatives Verhalten ist ebenso Teil der menschlichen Natur wie der Wettbewerb. Mit jeder E-Mail in einer Diskussionsgruppe und mit jeder getauschten Musikdatei wird dieser Punkt implizit unterstrichen.

Doch einige Probleme blieben trotz der Fortschritte, die die freie Software, die alternativen Netzmedien und Netzgemeinschaften gemacht hatten, bestehen. Um sich wirklich intensiv an dieser Geschenk- oder Tauschökonomie im Netz beteiligen zu können, ist es nötig, einen Internetzugang mit hohen Übertragungsgeschwindigkeiten zu haben, denn sonst ist das alles einfach zu zeitaufwändig, vor allem, wenn audiovisuelle Medien im Spiel sind. Darüber hinaus ist es essenziell, dass man einen Zugang hat, bei dem nicht jede Zeiteinheit abgerechnet wird, die man im Internet verbringt. Eine Geschenkökonomie mit einer tickenden Uhr im Nacken, welche die an die Telekom zu bezahlenden Telefongebühren anzeigt, kann nicht funktionieren. Ebenfalls hinderlich ist, wenn nach übertragenem Datenvolumen abgerechnet wird. Vielnutzer, die nicht nur Daten aus dem Netz saugen, sondern auch selbst viele Informationen anbieten, leiden besonders unter einer solchen Volumenabrechnung. Die Boom-und-Pleitephase hat jedoch eine Providerlandschaft hinterlassen, die überwiegend nach solchen kommunikationsfeindlichen Kriterien funktioniert.

In der Zeit des euphorischen Höhenflugs von Internetaktien und Telekommunikationsunternehmen wurde auf einen dramatischen Anstieg des Bedarfs an Bandbreite für Internetkommunikation spekuliert. Konvergenztechnologien wie z. B. interaktives Fernsehen im Internet, Voice-over-IP, Videokonferenzen und andere breitbandige Anwendungen würden, so glaubte man, bald neue Geschäftsmodelle ermöglichen. Es kam aber nicht so weit. Als die Aktienkurse zu purzeln begannen, wurden viele Projekte eingestellt, und einige der wichtigsten Player im Bereich überregionalen breitbandigen Datenverkehrs mussten Konkurs anmelden. In den gerade erst verlegten Glasfaserkabeln wurde nie das Licht eingeschaltet, sie blieben und bleiben »dark fibre« (da die Datenübertragung in Glasfaserkabeln über Lichtimpulse erfolgt, bezeichnet man mit diesem Begriff nicht aktivierte Glasfaserverbindungen).

Für die Endanwenderinnen hatte das zur Folge, dass sich die gerade noch versprochenen Freuden der breitbandigen Internetanwendungen zu Hause nicht oder nur sehr verzögert realisieren würden. Obwohl Dollar-Milliarden wortwörtlich in der Erde vergraben worden waren, »surft« die Mehrheit der privaten Nutzer immer noch mit mickrigen Modemgeschwindigkeiten. Als Breitbandtechnologien für Haushalte begannen sich in den letzten Jahren vor allem ADSL und Internet via TV-Kabel durchzusetzen. ADSL (Asynchronous Digital Subscriber Line) benutzt konventionelle Kupfertelefonkabel als Trägermedium, verwendet aber ein anderes Modulationsverfahren, mit dem höhere Übertragungsraten als mit normalen Modems erzielt werden können. Die dicken Koaxialkabel, die für Kabel-TV verwendet werden, erlauben neben der Übertragung eines Fernsehsignals auch die parallele Zurverfügungstellung eines breitbandigen Internetzugangs. Der Charakter dieser Technologien führte dazu, dass sich ein wirklicher Wettbewerb auf dem Gebiet der »letzten Meile«, der Anbindung des einzelnen Haushalts an den Backbone der Telekommunikationsnetze, nie entwickeln konnte. Die ehemaligen Staatsbetriebe wie Deutsche Telekom, British und France Télécom dominieren nach wie vor die Märkte – bei ADSL sind europaweit durchschnittlich 80 % der Kunden bei den ehemaligen Monopolen. Im Bereich Internet via TV-Kabel gibt es aus historischen Gründen meist nur ein regionales Unternehmen und somit keine echte Konkurrenz.

Der Mangel an echter Konkurrenz führt dazu, dass die Firmen damit durchkommen, Breitbandinternet anzubieten, das erstens kein wirkliches Breitband ist und zweitens immer noch einen ziemlich hohen Preis kostet. Die großen Telekommunikationsunternehmen und einige wenige Massenmarkt-Provider kontrollieren die Zugangswege zum Internet. Sie bestimmen die ökonomischen und technischen Parameter der Angebotsstrukturen. Die Freiheit, die das Internet einst versprach, ist von einer Reihe weiterer Faktoren bedroht.

### **Angriffe auf die Netzfreiheit**

Staatliche und private Institutionen versuchen, das Internet unter Kontrolle zu bekommen. Überwachung, Unterwanderung der Privatsphäre, Zensur- und Kontrollmechanismen haben Einzug gehalten. Auch die Institutionen, die mit dem Internet entstanden und mitgewachsen sind, blieben von den Auswirkungen der Kommerzialisierung nicht verschont. Das schnelle Wachstum und der kommerzielle Druck in der Phase des

Booms haben diese Institutionen verändert. Die Art, wie das Internet regiert wird, hat sich grundlegend gewandelt.

Die Entwicklung der technischen Internetstandards erfolgt unter dem Dach der Internet Engineering Task Force (IETF). Die an der Entwicklung des Internets beteiligten Informatiker treffen sich bei Konferenzen und Workshops, bei denen technische Fragen diskutiert werden. Lange Zeit genügte der IETF ein Modus der Entscheidungsfindung, der sich in der Phrase vom »groben Konsens und funktionierendem Code« zusammenfassen lässt. Ein neues Protokoll konnte nur angenommen werden, wenn es eine funktionierende Implementation gab. Die IETF bezeichnet sich auch heute noch als »offene, internationale Gemeinschaft von Netzwerkentwicklern, Betreibern, Verkäufern und Forschern, denen die Evolution der Internetarchitektur und ein reibungsloses Funktionieren des Internets ein Anliegen ist«. Doch anstatt einiger Dutzend Akademiker kommen heute Tausende zu IETF-Konferenzen. Viele der Delegierten arbeiten für internationale Konzerne mit beträchtlicher Marktmacht. Das ehemals so effiziente Entscheidungsfindungsverfahren der IETF kracht nun an allen Ecken und Enden. [5]

Wichtige Ressource für das Funktionieren des Internets sind die IP-Nummern und das Domain-Name-System. Die Administration der IP-Nummern und des Domain-Name-Systems erfolgte ursprünglich durch die Internet Assigned Numbers Authority (IANA). Jahrzehntlang wurde diese Mini-Behörde von Jon Postel am Stanford Research Institute geleitet, der übereinstimmend in den meisten Internet-Historien als eine Art Netz-Heiliger beschrieben wird. Als die US-Regierung beschloss, das Internet zu privatisieren, verfügte sie, dass eine neue Behörde zu gründen sei, die Internet Corporation for Assigned Names and Numbers (ICANN). Diese nimmt nun die Funktionen der IANA wahr, die formal unter ihrem Dach weiter besteht. Die ICANN ist zwar von internationaler Bedeutung, steht jedoch unter direktem Einfluss der US-Regierung. Die Organisation war von Anfang an von demokratiepolitischen Defiziten geplagt. Der Einfluss von Regierungs- und Konzernvertretern ist in den wenigen Jahren ihres Bestehens deutlich gewachsen, während Internetnutzerinnen nur einen marginalen (wenn überhaupt) Einfluss auf Entscheidungen haben.

Die Freiheit im Netz ist jenen Industriezweigen ein Dorn im Auge, die einen Großteil ihrer Einnahmen mit der Verwertung urheberrechtlich geschützter Werke machen – die Musik-, Film-, Spiele- und Softwareindustrien. Mit Gesetzen wie dem Digital Millennium Copyright Act

(USA 1998) und von diesem »inspirierten« Urheberrechtsgesetzen in Europa wird versucht, dem Tauschen von Musik und Videos in File-Sharing-Systemen Einhalt zu gebieten. Vor allem in den USA wurde begonnen, an NutzerInnen Exempel zu statuieren. Provider werden zur Herausgabe von Nutzerdaten gezwungen, damit diese vor Gericht gezerzt werden können. Unter Euphemismen wie »trusted computing« und »Digital Rights Management« wird versucht, eine neue Kontrollarchitektur in PC-Systeme zu integrieren, um das unerlaubte Kopieren auf technischer Ebene zu verhindern.

Werbeindustrie und Marketing haben ein starkes Interesse an Nutzerdaten. Mit Methoden wie Data-Warehousing, -Mining und Profiling werden Informationen über das Kommunikationsverhalten von NutzerInnen im Netz gesammelt und ausgewertet. [6]

Nationalstaaten haben ebenfalls einen gewaltigen Appetit auf Nutzerinformationen. Die Existenz des internationalen Überwachungssystems Echelon wurde lange Zeit von US-Geheimdiensten weder bestätigt noch dementiert. Eine Untersuchung des EU-Parlaments hat inzwischen jegliche Zweifel an der Existenz des Systems beseitigt. Die EU selbst hat eine Richtlinie beschlossen, die das Speichern von Verbindungsdaten erlaubt. Kommunikationsprovider können demnach angehalten werden, Informationen über das Nutzungsverhalten der Kunden vorsorglich aufzubewahren und bei Bedarf an Strafverfolgungsbehörden weiterzuleiten. In Deutschland schreibt die Telekommunikationsüberwachungsverordnung vor, dass Provider eine Abhörschnittstelle einrichten, so dass Polizei und Geheimdienste Zugang zu Log-Files von Web- und Mailservern bekommen. Diese Überwachungsmöglichkeit soll auf Kosten der Provider, d. h. letztlich auf Kosten der Nutzer eingerichtet werden.

Wer heute das Internet nutzt, muss davon ausgehen, aus den verschiedensten Gründen belauscht und bespitzelt zu werden. Hierarchische und autoritäre Strukturen sind im Begriff, das Netz immer stärker in den Griff zu bekommen. Die Freiheit im Internet ist bereits jetzt massiv eingeschränkt.

An diesem Punkt erscheinen die freien Netze auf der Bildfläche. Just in dem Augenblick, als die Kurve der New Economy im April 2000 zum Sturzflug überging, begannen Ideen und Initiativen zum Aufbau freier Netze in den Vordergrund zu rücken. Es ist nahe liegend, hier einen Zusammenhang zu sehen. Das Platzen der Börsenblase erzeugte ein Vakuum, das nach neuen Taten verlangte. Wie nach einem Gewitter-

sturm war die Luft gereinigt und der Druck und die Hysterie verflogen, die gerade noch alles zu lähmen gedroht hatten.

#### Literatur

- [1] Richard Barbrook, Andy Cameron, Die kalifornische Ideologie, in »Netzkritik«, Lovink/Schultz (Hrsg.), Edition ID-Archiv, Berlin 1997
- [2] Regula Bochsel, Adam Wishart, Leaving Reality Behind, Fourth Estate, London 2002
- [3] Robert Shiller, Irrational Exuberance, Princeton University Press 2000
- [4] Inke Arns, Netzkulturen, EVA, Wissen 3000, Hamburg 2002
- [5] Helmers, Hoffman & Hofmann, »Internet ... The Final Frontier: Eine Ethnographie«, Schlussbericht des Projekts »Interaktionsraum Internet. Netzkultur und Netzwerkorganisation«, Berlin 1998
- [6] Christiane Schulzki-Haddouti (Hrsg.), Vom Ende der Anonymität, Heise Verlag, 2. Aufl., 2001