

Wer sucht, der findet (nicht immer)

Mit Internetzensur wird versucht, den Zugriff auf rechtswidrige oder unliebsame Inhalte im Internet zu verhindern



Daniel Zinn*,
Doktorand am
Department of
Computer Science
an der University
of California at
Davis (UC Davis).
dzinn@ucdavis.
edu

Nicht nur China oder der Iran zensurieren das Internet, sondern auch die USA, Deutschland und die Schweiz.

Das Verbreiten von Informationen hat sich durch das Internet drastisch verändert. Vor ein paar Jahren konnten Neuigkeiten nur via Printmedien, dem Radio oder Fernsehen publiziert werden. Eine Anzeige in einer weit verbreiteten Zeitung oder gar ein Werbespot im Fernsehen kostete (und kosten immer noch) eine erhebliche Menge Geld. Mit Hilfe des Internets ist es nun jedem möglich, Informationen schnell und kostengünstig an ein breites Publikum zu übermitteln.

Ein Artikel im eigenen Blog oder auf der persönlichen Homepage kann augenblicklich von überall auf der Welt gelesen werden. Nicht nur sind die Informationen sofort verfügbar, sondern bekannte Blogs erreichen auch viele Menschen. Das erfolgreiche deutsche Blog «Politically Incorrect» (pi-news.net) zum Beispiel zählt täglich 20 000–25 000 Leser. Die Monatsbilanz von 430 000 und 710 000 Lesern¹ gleicht der Leserzahl von 653 000 der Schweizer Zeitschrift «Das Magazin».

Auch wenn man nicht der Verfasser eines bekannten Weblogs ist, ist es trotzdem möglich, viele Menschen zu erreichen. Ganz ohne Stammler kann jeder einen Videoclip auf der Webseite Youtube veröffentlichen. Welche Videos besonders erfolgreich sind, ist schwer abzuschätzen: der meistbetrachtete Clip wurde über 90 Millionen mal abgerufen und zeigt das Musik-Video «Girl-Friend» von Avril Lavigne. Auch unter den Top-10 befindet sich ein Clip eines lachenden Babys, das 55 Millionen mal angeschaut wurde. Auch Videos mit politischem Inhalt sind vertreten: Der Clip «I Got a Crush ... On Obama» (Ich habe mich in Obama verknallt), in dem eine junge Frau verführerisch über ihre Liebe zu Barak Obama singt, wurde von über 9 Millionen Menschen gesehen. Dieser Clip machte Lee Ettinger

über Nacht zu einer Berühmtheit: Über 15-mal ist sie seitdem in Talkshows aufgetreten, und bekannte Nachrichtensendungen wie CNN und Foxnews haben sie interviewt. Zum Vergleich: Das erfolgreichste offizielle Video «A More Perfect Union», in welchem Barak Obama seine Kernpunkte in einer Rede präsentiert, wurde nur 4,5 Millionen mal geschaut.

Ein Löschen ist quasi unmöglich

Informationen aus dem Internet zu löschen ist quasi unmöglich. Inhalt, der auf einer Webseite veröffentlicht wurde, kann nur dessen Autor löschen. Natürlich unterliegen Schweizer Webseitenbetreiber der Schweizer Gesetzgebung; damit sind der freien Meinungsäußerung per Gesetz Grenzen gesetzt. Interessant ist, dass Autoren sich zwar vor dem jeweiligen *lokalen* Gesetz rechtfertigen müssen, ihre Webseiten aber *global* abrufbar sind. Inhalt, der zum Beispiel in China oder im Iran verboten oder sittenwidrig ist, kann so hier ganz legal online gestellt werden.

Verschiedene Landessprachen stellen natürlich gewisse Barrieren dar. Aufgrund der weiten Verbreitung des Englischen wird das allerdings relativiert. Im Internet sind weniger als 8% aller Seiten deutschsprachig, d.h. nur ein sehr kleiner Teil des Internets untersteht Schweizer, deutscher oder österreichischer Gesetzgebung. Im Gegensatz dazu sind circa 55% aller Seiten in Englisch verfasst². Da ein Grossteil der deutschsprachigen Bevölkerung auch englisch versteht, sind ihr die englischen Seiten auch zugänglich. Automatische Übersetzungswerkzeuge, wie sie z.B. Google zur Verfügung stellt, erlauben es sogar, im nichtdeutschsprachigen Internet zu suchen, wobei sowohl die Suchbegriffe als auch die Ergebnisseiten bequem ins Deutsche übersetzt werden.

Selbst für den Autor einer Webseite ist es schwer, eigene Inhalte vom Internet zu löschen. Auch wenn man den Inhalt problemlos vom eigenen Server nehmen kann, bedeutet dies nicht zwangsläufig, dass die Daten nicht mehr verfügbar sind. Das Projekt «The Internet Wayback Machine» hat es sich zum Ziel gesetzt, Teile des Inter-

nets zu speichern und zu konservieren. Seit 1996 werden populäre Seiten des Internets archiviert. So sind zum Beispiel über 250 Versionen von der Titelseite auf zeitung.ch verfügbar. Obwohl die Wayback Machine eine gewaltig Datenmenge von über zwei Petabytes³ – mehr Informationen als in den Büchern aller Bibliotheken der Welt – archiviert hat, ist dies nur ein kleiner Teil des Internets und seiner Geschichte. Die Wayback Machine hat eine Kollektion von 85 Milliarden Seiten; die tatsächliche Grösse des Internets ist schwer abzuschätzen – es ist sogar schon schwer zu definieren, was man unter der Grösse versteht. Würde man einfach versuchen, alle Seiten im Internet zu zählen, wären es unendlich viele. Der Grund hierfür sind Seiten mit automatisch generiertem Inhalt: Jedesmal, wenn man in einem Web-Kalender auf «next» klickt und zum nächsten Monat gelangt, wird theoretisch eine neue Webseite generiert. Suchmaschinen wie Google versuchen, diejenigen Teile des Internets zu indizieren, die relevante Informationen besitzen. In einem aktuellen Artikel im offiziellen Google-Blog wird berichtet, dass Google eine Billion verschiedene Seiten indiziert hat. Zum schnellen Beantworten von Suchanfragen speichert Google die Daten all dieser Seiten auf eigenen Rechnern in ihren Datenzentren ab. So trägt auch Google dazu bei, dass Daten im Internet schwer zu löschen sind: Sollte eine Seite eines Google-Ergebnisses einmal nicht zu erreichen sein, kann man sich einfach die Google-Kopie anfordern, indem man auf den «Cached»-Link klickt. In gewisser Weise ist Google ein Kurzzeitgedächtnis des Internets: Eine gelöschte Seite ist für kurze Zeit noch über den Google-Cache verfügbar.

Verstecken statt löschen

Weil Informationen im Internet ungehindert Staatsgrenzen überwinden können, sich jedoch die staatliche Kontrolle nicht über die Grenzen hinaus erstreckt, wird im Internet oft nicht gelöscht, sondern nur versteckt. So versucht China zum Beispiel, fragwürdige Seiten unerreichbar zu machen. Im Allgemeinen bezeichnet man den Versuch von Staaten, den Datenaustausch über das Internet zu kontrollieren oder zu begrenzen, als Internetzensur. Wie bei gewöhnlicher Zensur wird versucht, die Verbreitung von Inhalten, die nicht dem jeweils herrschenden Recht genügen, zu verhindern oder einzudämmen.

Internetzensur ist weitverbreitet; das Ausmass der angewandten Restriktionen variiert allerdings erheblich (siehe Abbildung auf der nächsten Doppelseite). So zensiert China zum Beispiel die Online-Enzyklopädie Wikipedia in chinesischer Sprache und diverse Menschenrechtsseiten wie Amnesty International oder Hu-

man Rights in China (HRiC). Aber auch Staaten wie Deutschland oder gar die Schweiz zensieren das Internet.

Um die verschiedenen Methoden der Internetzensur besser zu verstehen, stellen wir kurz dar, was passiert, wenn man eine Webseite im Internet abrufen; jeder einzelne dieser Schritte kann durch bestimmte Zensurmassnahmen behindert werden.

Sucht man auf Google.com zum Beispiel nach «Wetter», generiert der Browser eine URL (uniform resource locator oder «einheitlicher Quellenanzeiger»), die etwa wie folgt aussieht:

`http://www.google.com/search?q=Wetter.`

Eine solche URL besteht aus dem Protokollnamen (hier *http*), einem Computernamen (*www.google.com*) und einem Pfadausdruck (*/search*) zusammen mit einer Anfrage-Zeichenkette (*?q=Wetter*). Zuerst zerlegt der Browser die URL in diese Komponenten. Als nächstes wird die Adresse des angefragten Google-Computers, des *Webserver*s, ermittelt. Hierzu wird eine Anfrage zu einem DNS-Server gestellt. DNS steht für «Do-

Internetzensur ist weitverbreitet; das Ausmass der angewandten Restriktionen variiert allerdings erheblich.

main Name System» und ist der Adressdienst des Internets. Mit Hilfe von DNS-Servern kann man eine IP-Adresse für Computernamen herausfinden. Eine IP-Adresse ist eine Nummer, die jeden Computer im Internet identifiziert, ähnlich einer Telefonnummer. So ist die IP-Adresse, die der DNS-Server für *www.google.com* mitteilt, *72.14.207.99*. Zu dieser IP-Adresse schickt der Browser jetzt die Suchanfrage. Wie dies geschieht, legt das Protokoll fest. Das Hypertext-

Kurz & bündig

Wie noch nie zuvor ist es heute möglich, Informationen zu verbreiten. Mit Hilfe der eigenen Web-Seite, des persönlichen Blogs oder eines Videos auf Youtube kann jeder mit Internetzugang beliebige Informationen veröffentlichen. Sobald die Daten auf dem jeweiligen Server hochgeladen wurden, sind sie augenblicklich für die ganze Welt erreichbar. Veröffentlichen ist einfach – das Löschen unerwünschter Informationen auf fremden Seiten hingegen quasi unmöglich. Dennoch kann der Informationsfluss im Internet zensiert werden: Es gilt: «gut versteckt ist fast gelöscht». Internetzensur verläuft oft nicht ohne Kollateralschäden: Zensiert man pornografische Werke in US-amerikanischen Schulen, verschwinden oft auch die Inhalte über Brustkrebs, Homosexualität und andere verwandte Themen. Doch versteckt ist nicht gelöscht, und meist gibt es zahlreiche Varianten, die Zensur zu umgehen.

Übertragungsprotokoll, kurz http, das hier verwendet wird, ist das Standardprotokoll für das Surfen im Web. Es spezifiziert unter anderem, dass die Daten unverschlüsselt übermittelt werden. In unserem Beispiel würde eine GET-Anfrage mit dem Text

Get /search?q=Wetter

Host: www.google.com

zum Web-Server übermittelt werden. Hierfür wird zunächst eine direkte Verbindung zum Rechner mit der Adresse *72.14.207.99* aufgebaut. Die Einzelheiten des Verbindungsaufbaus und wie

DNS-basiertes Filtern greift in das Nachschlagen der IP-Adresse ein, IP-Blockaden verhindern das Ansprechen des Webservers, Stichwort-basierte Zensur stört den Datenaustausch.

Daten hin- und hergeschickt werden, sind im TCP oder «Transmission Control Protocol» festgelegt. Beide Enden der Kommunikation – unser Browser und der Webserver auf dem Google-Rechner – verhalten sich, wie im TCP-Standard beschrieben⁴. Nachdem also der Browser die Anfrage versendet hat, antwortet der Google-Rechner mit einem langen Text, der dann vom Browser dargestellt wird.

Die Methoden der Internetzensur stören verschiedene Aspekte dieses Vorgangs: DNS-basiertes Filtern greift in das Nachschlagen der IP-Adresse ein, IP-Blockaden verhindern das Ansprechen des Webservers, und Stichwort-basierte Zensur stört den Datenaustausch.

Methoden der Internetzensur

DNS-basiertes Filtern

Eine weitverbreitete Technik der Internetzensur besteht darin, falsche IP-Adressen zu DNS-Anfragen zurückzugeben. Wenn man zum Beispiel *google.com* oder *www.allofmp3.com* in den Web-Browser eingibt und der DNS-Server mit einer falschen IP-Adresse antwortet, dann wird die Anfrage nicht zur MP3-Seite geschickt, sondern zur falschen Adresse. Ist an dieser Adresse kein Web-Server anzutreffen, macht es den Anschein, als wäre zum Beispiel *www.allofmp3.com* nicht erreichbar. Natürlich kann der Zensierende auch die Adresse einer eigenen Seite zurückgeben, um den Surfer darauf hinzuweisen, dass die angeforderte Seite rechtswidrige oder fragwürdige Inhalte enthält und deshalb nicht verfügbar ist.

Da *Internet Service Provider* (ISPs) wie z. B. Arcor ihren Nutzern vorgeben, welche DNS-Server sie benutzen sollen, können ISPs ohne technische Schwierigkeiten Nutzer-DNS-Anfragen zu

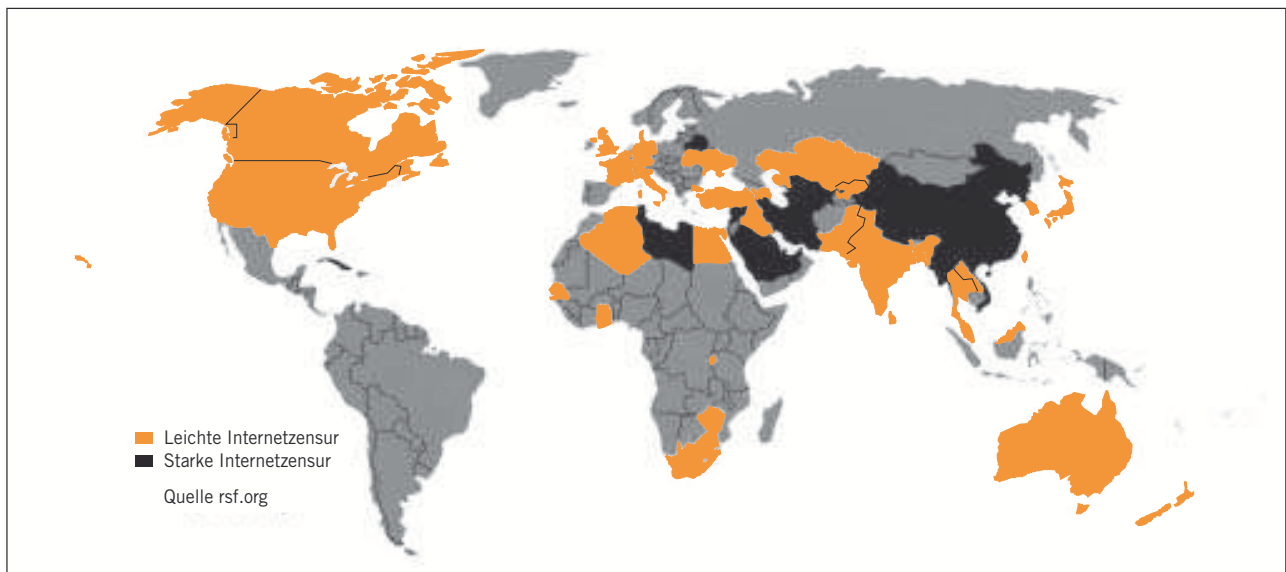
eigenen Servern leiten, die dann «zensierte» Adressen zurückliefern. So hat Dänemarks grösster Provider im Oktober 2005 seine DNS-Server modifiziert, um Kinderpornografieseiten zu sperren. Seit Mai 2006 benutzen die meisten dänischen Provider dieses modifizierte «IP-Adressbuch», so dass 98% aller dänischen Internetnutzer durch diesen Filter eingeschränkt sind⁵. Die Schweizer Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBİK) führt auch eine Liste von Seiten mit kinderpornografischen Inhalten. Schweizer Provider wurden angeschrieben mit der Empfehlung, diese Seiten freiwillig zu zensieren. Die meisten Provider kommen seit Anfang 2007 dieser Bitte nach und zensieren das Internet. DNS-Anfragen nach gesperrten Webseiten werden mit einer falschen Adresse beantwortet, welche auf die KOBİK-Stopp-Website weiterleitet⁶. Auch in Finnland, Schweden, Norwegen und den Niederlanden wird Kinderpornografie mittels modifizierter DNS-Server zensiert⁷. In Thailand wird diese Technik benutzt, um Seiten zu zensieren, die verschiedene illegale Aktivitäten repräsentieren. So sind Seiten über Glücksspiel, Drogenkonsum und Pornografie nicht erreichbar.

Natürlich sind die zensierten Seiten nicht gelöscht; sie sind nur ein wenig versteckt. Benutzt man zum Beispiel nicht den vom Provider vorgeschlagenen DNS-Server, sondern einen «nichtzensierenden» Server, könnte man die vormals versteckten Seiten ohne Probleme erreichen. Das Anzeigen und Ändern des DNS-Servers ist ohne Probleme in den Netzwerkeinstellungen des eigenen Computers möglich.

IP-Blockaden

Eine etwas schwieriger zu umgehende Technik der Internetzensur ist die IP-basierte Zensur. Hier werden Datenpakete zu bestimmten IP-Adressen im Internet nicht weitergeleitet. Das Internet besteht neben den Rechnern, die Webseiten anbieten, auch aus vielen anderen Rechnern, die Datenpakete durch das Netz verschicken. Diese Rechner, auch *Router* genannt, leiten Datenpakete, basierend auf der IP-Adresse, vom sendenden Computer bis zum Empfänger weiter. Von meinem Laptop, mit dem ich gerade diesen Artikel schreibe, zur Seite *www.spiegel.de* sind zum Beispiel 23 verschiedene Router, die jedes einzelne meiner Datenpakete zu *spiegel.de* empfangen und weiterleiten⁸. Jeder Besitzer eines Routers kann veranlassen, dass Pakete für bestimmte IP-Adressen nicht weitergeleitet, sondern einfach weggeworfen werden, und kann somit den Datenaustausch im Internet stören.

IP-Blockaden sind neben DNS-basierten Methoden die meistbenutzte Technik der Internet-



zensur. Da Internet-Nutzer keine Kontrolle über den Weg der versandten Datenpakete haben, ist IP-basierte Zensur schwieriger zu umgehen als eine DNS-Blockade. Eine der wenigen Möglichkeiten ist das Benutzen von Proxy-Servern. Dies sind Rechner im Internet, die stellvertretend für deren Nutzer Seiten im Internet abrufen. Wenn zum Beispiel mein ISP alle IP-Pakete zu *wikipedia.org*⁹ verwirft anstatt sie weiterzuleiten, dann kann ich über einen Proxy-Server die Seite trotzdem anwählen. Nachdem ich einen solchen Server konfiguriert habe, würde mein Webbrowser nicht *wikipedia.org* kontaktieren, sondern den Proxy-Server. Da der Proxy-Server nicht blockiert ist, können meine Datenpakete diesen ungehindert erreichen. Basierend auf meiner Anfrage *Get/index.html Host: wikipedia.org* kontaktiert nun der Proxy-Server selbst den Rechner von Wikipedia – er leitet quasi meine Anfrage weiter. Da «mein» ISP keine Kontrolle über die Router zwischen dem Proxy-Server und *wikipedia.org* hat, kann der Proxy-Server ungehindert mit Wikipedia kommunizieren (sofern keine «bösen» Router dazwischen sind). Sobald der Proxy-Server nun die Wiki-Seite erhalten hat, wird er diese zu mir weiterleiten. Folglich kann ich den Inhalt von einer IP-blockierten Seite betrachten, obwohl der direkte Weg zum Ziel für mich gesperrt ist. Da es technisch sehr einfach ist, einen Proxy-Server zu betreiben, ist es nahezu unmöglich, eine Liste aller Proxy-Server zu erstellen, um den Datenverkehr zu diesen gezielt zu blockieren. Das Benutzen von Proxy-Servern ist eine weit verbreitete Technik, um IP-basierte Blockaden zu umgehen.

Stichwortbasierte Zensur

Ein Nachteil der bisher vorgestellten Methoden zum Verstecken von Informationen im Inter-

net ist, dass man als Zensor festlegen muss, welche Seiten man zensieren will. Das Erstellen und Pflegen einer Liste von geblockten Seiten in Form einer IP-Adress- oder DNS-Namensliste bringt somit einen hohen Verwaltungsaufwand mit sich. Darüber hinaus ist es möglich, eine neue, dem Zensor unbekanntes Seite zu erstellen und darüber «fragwürdiges» Material zu verbreiten. Solange die neue Seite noch nicht auf der «Schwarzen Liste» erscheint, ist es jedem Surfer möglich, die Inhalte abzurufen.

Stichwortbasierte Zensur, wie sie im Backbone des chinesischen Internets betrieben wird, zensiert nicht nur basierend auf DNS-Namen oder IP-Adressen, sondern auch auf Grund des tatsächlichen Inhaltes. Wenn die GET-Anfrage des Browsers oder die Antwortseite des Webserver ein zu zensierendes Wort enthält, wird der weitere Datenaustausch zwischen Browser und Webserver verhindert. Wie bei der IP-basierten

IP-Blockaden sind neben DNS-basierten Methoden die meistbenutzte Technik der Internetzensur und schwieriger zu umgehen als eine DNS-Blockade.

Zensur geschieht das Blockieren durch Router im Internet. Diese lesen die Pakete zwischen Browsern und Webservern mit. Sollte ein Datenaustausch ein verbotenes Wort enthalten, stört der Router im Internet die TCP-Verbindung zwischen Browser und Webserver. Hierzu versendet der Router TCP-Reset-Pakete mit gefälschter Absenderadresse: Dem Browser wird ein Reset-Paket geschickt, das so aussieht, als würde es vom

Server stammen – mit der Konsequenz, dass der Browser die Verbindung beendet und anstelle der Webseite eine Fehlermeldung darstellt. Zusätzlich vermerkt der Router die Sender- und Empfänger-Adresse in einer Schwarzen Liste, um dann für eineinhalb Minuten weitere Kommunikation zwischen diesem Browser und Server durch herkömmliche IP-Adressen-Zensur zu verhindern¹⁰. Mit Hilfe dieser Methode wird das Browsen von Webseiten zielgerichtet zensiert. Da die zensierenden Rechner unter der Kontrolle der ISPs sind, kann man die Zensur – ähnlich wie IP-Blockaden – nicht durch einfache Konfiguration umgehen. Auch die Benutzung von Proxy-Servern hilft hier nicht, weil dann einfach die Verbindung zum Proxy-Server gestört wird. Allerdings gibt es auch hier einen Ausweg: Da die Router den Inhalt der Kommunikation mitlesen, ist es ausreichend, auf ein verschlüsseltes Protokoll zurückzugreifen. Bei Webseiten, die via *https*¹¹ anstatt *http* angeboten werden, werden die ausgetauschten Daten verschlüsselt verschickt; die Router können deshalb keine Entscheidung treffen, ob eine Verbindung geblockt werden soll oder nicht. Da viele wichtige Dienste (wie zum Beispiel Internet-Banking oder auch Online-Shops) für die Übermittlung sensibler

Werden Suchmaschinenbetreiber vor die Wahl gestellt, entweder die Suchergebnisse zu zensieren oder komplett geblockt zu werden, dann wählen sie lieber die erste Variante.

Daten das *https*-Protokoll benutzen, ist es unwahrscheinlich, dass verschlüsselte Nachrichten generell geblockt werden. Proxy-Server, die über *https* zu erreichen sind und normale *http*-Seiten zur Verfügung stellen, können deshalb genutzt werden, um versteckte *zensierte* Inhalte wieder zu finden.

Zwei Schweizer Künstler stellen mit ihrem Projekt *picadae.net* eine Alternative zu einem *https*-Proxy vor: Anstatt den Inhalt zum Nutzer via *https*-Protokoll zu verschlüsseln, macht der *picadae*-Server ein Foto der angeforderten Webseite und verschickt die Seite als Bilddatei. Wie bei der Benutzung eines *https*-Proxies ist es auch hier den Routern nicht möglich «mitzulesen», da das Erkennen von Text in den Bildern zu viel Rechenaufwand erfordern würde.

Zensur durch Suchmaschinen

Da der Zugriff auf das Internet heutzutage vorwiegend über Suchmaschinen geschieht, kann man das Internet zensieren, ganz ohne Webseiten zu verstecken: Man zensiert einfach das Ergebnis

zu Suchanfragen und verhindert so, dass Webseiten gefunden werden. Natürlich erfordert dies die Zusammenarbeit von Regierung und jeweiligem Suchmaschinenbetreiber, aber wenn Suchmaschinenbetreiber vor die Wahl gestellt werden, entweder die Ergebnisse zu zensieren oder komplett geblockt zu werden, dann wählen sie wie Microsoft, Yahoo und Google lieber die erste Variante. So ergeben Suchanfragen nach der religiösen Bewegung «Falun Gong» komplett verschiedene Resultate auf *google.com* und *google.cn*: Die Wikipedia-Seite und die offizielle Seite der Bewegung werden auf *google.com* als Top-Resultate gezeigt, während die beiden Seiten auf der chinesischen Variante von Google nicht einmal erwähnt werden. Auch in Deutschland zensiert Google die Ergebnisse: Eine Anfrage nach «youporn» liefert nur auf der US-amerikanischen Seite einen Verweis zu *youporn.com*, nicht aber auf der deutschen Variante. Stattdessen ist ganz unten die Nachricht zu lesen: «Aus Rechtsgründen hat Google 2 Ergebnis(se) von dieser Seite entfernt».

Umfang und Auswirkungen der Zensur

Was wird zensiert? Grob eingeteilt können drei Kategorien unterschieden werden:

- Politische und sozial «heikle» Themen (wie Kinderpornografie);
- Informationen über (bewaffnete) Konflikte und militante Bewegungen;
- Seiten, die Internetdienste wie E-Mail, Webseiten-Hosting, Internet-Suche oder auch Werkzeuge zur Umgehung von Zensur anbieten.

China und der Iran zensieren all diese Bereiche in grossem Umfang. Staaten wie Deutschland, Frankreich, Schweden, Norwegen, Kanada, die USA oder Australien zensieren sozial fragwürdige Inhalte – zum Beispiel in Verbindung mit Pornografie (siehe die Abbildung auf der letzten Doppelseite). Genauere Informationen darüber stellt die OpenNet-Initiative auf *www.opennet.net* bereit.

Unabhängig davon, ob Zensur dieser Themen gerechtfertigt ist oder nicht, ist Internetzensur problematisch. Wird zum Beispiel die IP-Adresse einer zu zensierenden Seite gesperrt, kann es sein, dass aus Versehen viele andere Seiten nicht mehr erreichbar sind. Der Grund hierfür ist, dass oft mehrere Seiten auf dem gleichem Rechner angeboten werden und deren Namen somit einer einzigen IP-Adresse zugeordnet sind. Nach einer Studie von Edelman an der Harvard Law School¹² teilten sich 83% aller aktiven Domain-Namen die IP-Adresse mit einer anderen Seite. Zusätzlich wird eine IP-Adresse nicht nur von wenigen Webseiten benutzt, sondern wenn geteilt wird, dann gleich mit vielen anderen Seiten: Mehr als zwei

Drittel aller aktiven .com-, .net- und .org-Seiten teilen sich eine IP-Adresse mit mehr als 50 anderen Seiten.

So wurden, als Arcor *privatamateure.com* mittels IP-Blockade zensierte, unbeabsichtigterweise auch noch mehr als drei Millionen andere Seiten zusätzlich geblockt. Die amerikanische Pornografie-Seite wird nämlich von einem US-Dienstleister namens GoDaddy.com gehostet. Dieser Anbieter, ähnlich wie *1und1.de*, verwaltet noch viele andere Seiten. Unter den geblockten Seiten waren die Bollywood-Fanseite Barathstars, eine Seite über den Linux-Kernel-Debugger Linice, sowie die WLAN-Initiative Fon-City – alles Seiten, die in keinster Weise Pornografie vertreiben¹³.

Auch die auf Stichwörtern basierende Blockade, wie sie in China praktiziert wird, bringt Kollateralschäden mit sich. Generell wird eine Verbindung gestört, sobald ein indiziertes Wort entdeckt wurde. Der Kontext, in dem das Wort verwendet wird, wird nicht in Betracht gezogen; dies ist auf Grund der hohen Datenraten an den Routern technisch nicht möglich. So blockiert das chinesische Backbone zum Beispiel Webseiten, welche das deutsche Bundesland *Nordrhein-Westfalen* in chinesischen Schriftzeichen enthalten. Natürlich liegt es der chinesischen Regierung fern, Informationen über Nordrhein-Westfalen zu zensieren, jedoch klingt «falen» in Westfalen ähnlich dem «Falun» in Falun Gong. Da das Schriftzeichen für «falen» oft verwendet wurde, um die Stichwort-Zensur von Falun zu umgehen, wird dies nun auch geblockt – und damit alle Seiten über das deutsche Bundesland.

Fazit

Das Internet hat es ermöglicht, Informationen schnell und unkompliziert zu verbreiten: Eigene Webseiten, Blogs oder aber auch Dienste wie Youtube machen es möglich. Solche Informationen zu löschen oder zu kontrollieren ist als Indi-

Auch die auf Stichwörtern basierende Blockade bringt Kollateralschäden mit sich. Generell wird eine Verbindung gestört, sobald ein indiziertes Wort entdeckt wurde.

viduum schwer möglich. Selbst als Staat ist es unmöglich, Informationen zu löschen, die auf Rechnern angeboten werden, welche nicht der eigenen Rechtsprechung unterliegen. Viele Staaten bedienen sich deshalb des Mittels der Internetzensur, um rechtswidrige Daten zu verstecken oder den Zugriff auf diese zu erschweren. Wie in anderen Bereichen der Zensur ist das Ausmass der Internetzensur sehr vom jeweiligen Staat und dem vorherrschenden Rechtssystem abhängig. Internetzensur an sich ist oftmals mit einfachen Mitteln zu umgehen – die Zensurmassnahmen genügen aber in den meisten Fällen, die Staatsbürger darauf hinzuweisen, dass sie sich strafbar machen könnten. Dies resultiert oft in einer «freiwilligen Selbstzensur». Im Internet reicht es also oft aus, fragwürdige Inhalte ein wenig zu verstecken anstatt sie zu löschen. ■

Fussnoten

* Daniel Zinn untersucht mit anderen Forschern aus Davis und der Universität von New Mexico die Internetzensur in China (conceptdoppler.org). Die Resultate dieser Untersuchung (Liste geblockter Wörter sowie Liste der blockierenden chinesischen Provider) wurden in der Konferenz für Computer- und Kommunikations-Sicherheit 2007 veröffentlicht. Zurzeit absolviert er ein Praktikum bei Google, Inc. in Mountain View.

¹ Statistik auf <http://pi-news.net/chc_2/stats/index.php?cat=access_statistics> (letztmals kontrolliert: 8.8.2008).

² Daten von <<http://www.netz-tipp.de/sprachen.html>>.

³ 1 PB = 1 000 TB = 1 000 000 GB.

⁴ RFC 793 Transmission Control Protocol, <www.ietf.org/rfc/rfc0793.txt> (letztmals kontrolliert: 8.8.2008).

⁵ KRABBE KLAUS (2005-10-18). «TDC aktiverer filter mod børneporno», Computerworld. Retrieved on 2006-07-19.

⁶ Rechenschaftsbericht der KOBIC 2006, <http://www.cybercrime.ch/report/Rechenschaftsbericht_2006_d.pdf>.

⁷ Wikipedia: Stichwort «Internet censorship».

⁸ Der «Weg» zu einer bestimmten URL kann mit den Tools «Traceroute» (tracert.exe unter Windows, traceroute oder tcptraceroute unter Unix/Linux, Mac) ermittelt werden.

⁹ Wikipedia.org wurde des Öfteren in China geblockt. Quelle Wikipedia, <http://en.wikipedia.org/wiki/List_of_websites_blocked_in_the_People%27s_Republic_of_China>.

¹⁰ ConceptDoppler: a weather tracker for internet censorship, Conference Proceedings of the 14th ACM Conference on Computer and Communications security <<http://portal.acm.org/citation.cfm?doid=1315245.1315290>>.

¹¹ Das «s» steht für secure oder sicher.

¹² <http://cyber.law.harvard.edu/archived_content/people/edelman/ip-sharing/>.

¹³ Quelle: <<http://www.spiegel.de/netzwelt/web/0,1518,506143,00.html>>.

Alle URLs letztmals kontrolliert am 8.8.2008.