Filterung und Zensur im Internet

Möglichkeiten, Wirkungsweise und wie man sie umgehen kann
Seminararbeit

Manuel Mausz
manuel-tu@mausz.at

ABSTRACT
Diese Seminararbeit untersucht die verschiedenen Möglichkeiten, die der heutige Stand der Technik bietet, um Zugriff auf ausgewählte Bereiche des Internet einzuschränken. Insbesondere wird die technische Wirkungsweise von einfachen bis hin zu komplexen Maßnahmen, im Speziellen die Wirkungsweise der so genannten "Great Firewall of China", untersucht und die daraus resultierenden Möglichkeiten, diese zu umgehen, aufgezeigt. Obgleich die von der "Great Firewall of China" gesendeten TCP-RST-Pakete durch den Einsatz einer Paket-Firewall oder aber auch durch gezielte Verschleierung "verbotener Inhalte", umgangen werden kann, unternimmt die Volksrepublik China große Anstrengungen das Internet innerhalb des Landes zu zensieren und findet dabei unter anderem auch indirekte Unterstützung seitens großer, westlicher Suchmaschinenbetreiber.

Categories and Subject Descriptors
H.3.3 [**Information Storage and Retrieval**]: Information Search and Retrieval Information—*filtering*; C.2.0 [**Computer-Communuication Networks**]: General—*Security and protection (e.g., firewalls)*

General Terms
Security

Keywords
Seminararbeit, Internet Filterung, Firewall, Zensur, umgehen, China, Great Firewall of China

1. EINLEITUNG
Das Internet ist heutzutage ein wichtiger Bestandteil unseres Lebens geworden. Wir verwenden es in unserer täglichen Arbeit, in unserer Freizeit und immer mehr auch um uns über aktuelle Tagesgeschehnisse zu informieren. Griffen wir früher noch zur Tageszeitung, informieren sich heutzutage vor allem junge Menschen nicht nur über die Websites der Zeitungen, sondern auch über Foren oder so genannte Blogs.

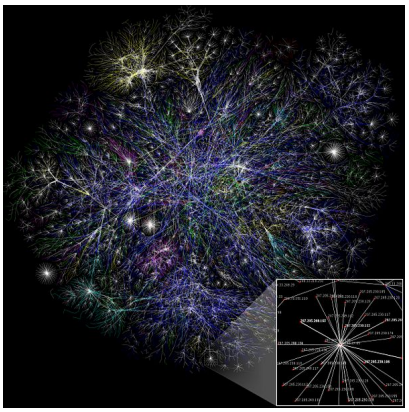

Abbildung 1: Visualisierung der verschiedenen Routen durch Teile des Internets. Quelle: `http://en.wikipedia.org/wiki/Image:Internet_map_1024.jpg`**, Abruf vom 18.05.2008**

Blogs sind größtenteils privat geführte Websites, die vom Aufbau her einem Tagebuch ähneln. Sie dienen dem Herausgeber (Blogger) dazu, Informationen, Gedanken, Erfahrungen und auch Meinungen mit dem Rest der Welt, oder anderen Blogger, auszutauschen. Aufgrund dieser mittlerweile unüberschaubaren Anzahl an Möglichkeiten, sich über Themen zu informieren, ist es für Staaten beinahe unmöglich geworden, unerwünschte Themen zu zensieren.
Wie die Visualisierung der verschiedenen Routen des Internets in Abbildung 1 zeigt, ist das Internet grundsätzlich dezentralistisch aufgebaut. Es gibt zwar kleinere und größere Kontenpunkte, aber durch Querverbindungen meist verschiedene Wege um von einem Punkt zum anderen zu gelangen. Dieser grundlegende Aufbau macht wirkungsvolle Filterungsmaßnahmen schwierig und teuer. Zudem basiert das Internet aus einer Fülle von Protokollen, die zwar teilweise aufeinander aufbauen, aber jedes für sich, für einen bestimmten Zweck geschaffen worden ist. Gleichzeitig sind diese Knotenpunkte und Protokolle aber auch der einzige Punkt, an dem Filterung effektiv und zugleich flächendeckend vollzogen werden kann. Die hohe Menge an Datenpaketen, die einen solchen Knotenpunkt mittlerweile durchfließen, zwingt einen jedoch, sich auf einzelne Protokolle zu beschränken. Somit können heutzutage niemals alle Datenpakete einer Filterung unterzogen werden, wodurch gleichzeitig immer eine Möglichkeit entsteht, sich der Filterung zu entziehen.

Zur Einführung und besserem Verständnis des Folgethemas wird in Abschnitt 2 dieser Seminararbeit zuerst ein Überblick über verschiedene Möglichkeiten zur Filterung des Internet, deren Wirkungsweise aber auch die daraus resultierenden Möglichkeiten zur Umgehung, geschaffen.
Anschließend wird in Abschnitt 3 die Funktionsweise der so genannten "Great Firewall of China" untersucht, indem Aufzeichnungen von TCP-Verbindungen mit einem Webserver innerhalb Chinas analysiert werden. Aus diesen Erkenntnissen werden in Abschnitt 3.2 Methoden entwickelt und getestet um die Wirkungsweise und damit die Zensur zu umgehen. Anschließend wird in Abschnitt 3.3 die Struktur des sich derzeit in Aufbau befindlichen "ChinaNet Next Carrying Network" untersucht sowie in Abschnitt 3.4 weitere Maßnahmen der Volksrepublik China um Zensur im Internet zu ermöglichen, aufgezählt.

2. METHODEN

2.1 Port- und IP-Sperre

Die einfachste und zugleich kostengünstigste Methode zur Filterung ist die Sperre von IP-Adressen. Da ein Paket des IP-Protokolls [10] immer Quell- und Zieladresse enthalten muss, und dies von einem Router bzw. Switch für ihre Funktionalität ohnehin untersucht werden muss, ist es ohne hohe Kosten möglich, diese Daten während der Bearbeitung mit einer internen Liste zu vergleichen und das Paket gegebenenfalls zu blockieren. Für den Absender des Pakets ist damit der Empfänger nicht mehr erreichbar.
Ebenso kostengünstig ist die Sperre einzelner Ports oder Portbereiche der Basis-Protokolle TCP [11] und UDP [9]. Auch diese Funktionalität ist seit einigen Jahren in allen höherwertigen Routern standardmäßig implementiert [13].
Beide Methoden haben jedoch grundlegende Probleme. Zum einen müssen die Sperrlisten auf alle Router ständig aktualisiert und synchronisiert werden, zum anderen ist der Speicherplatz für diese Listen begrenzt. Viel größer ist jedoch das Problem, dass beide Methoden nicht für die Filterung des HTTP-Protokolls geeignet sind. Heutzutage speichert ein Webserver nicht eine, sondern eine Vielzahl an Websites. Durch eine Blockade der IP-Adresse des Webservers würden somit alle Websites auf diesem Webserver blockiert werden, was in den wenigsten Fällen gewollt ist. Die Sperre des Ports würde hingegen gleich den gesamten Zugriff per HTTP sperren.
Dennoch ist diese Methode insbesondere für die Absicherung von Firmennetzwerken sehr beliebt, kann aber mittels Verwendung eines Proxy-Dienstes[1] (Abschnitt 2.3) oder eines alternativen Ports ebenso leicht umgangen werden.

2.2 DNS-Manipulation

Eine ebenso kostengünstige Möglichkeit der Filterung ist die Manipulation des Domain Name System (DNS). Da das IP-Protokoll lediglich auf Basis von IP-Adressen kommunizieren kann, Websites aber über eine Domain erreichbar sind, müssen diese zwei verschiedene Adressierungen übersetzt werden. Hierzu dient das DNS-Protokoll und ein dazugehöriger DNS-Server. Dieser übersetzt auf Anfrage des Absenders eine Domain in eine IP-Adresse, leitet aber auch Anfragen an andere DNS-Server weiter, sollte er selbst keine Kenntnis über die Domain haben. Ein DNS-Server kann nun so manipuliert werden, dass er falsche IP-Adressen für einzelne Domains zurück liefert, obwohl er für diese Domain nicht autoritativ ist. Als Resultat sendet der Benutzer seine Anfrage an eine falsche IP-Adresse und erhält in den meisten Fällen eine Fehlermeldung über eine nicht verfügbare Website oder Dienstleistung.
Grundsätzlich kann diese Maßnahme durch die Verwendung eines freien DNS-Servers[2] umgangen werden. Es besteht jedoch die Möglichkeit, das zudem sämtliche Pakete des DNS-Protokolls auf den manipulierten DNS-Server weitergeleitet werden. In diesem Fall hilft lediglich die Benutzung eines Proxy-Dienstes[2].

2.3 Proxy-Server

Proxy-Server sind im Gegensatz zu den bereits erwähnten Methoden, aufwändiger, bieten aber auch mehr Möglichkeiten zur Kontrolle und damit einhergehende Filterung. Proxy-Server sind meist als Gateways zum Internet realisiert. Im Gegensatz zu herkömmlichen Gateways, die Pakete zwischen zwei IP-Netzen übersetzen, agieren Proxy-Server aber stellvertretend für den ursprünglichen Absender. Dabei schickt der Absender seine Anfrage an den Proxy-Server, dieser erzeugt aus den empfangenen Informationen ein unabhängiges Daten-Paket und übermittelt es an den ursprünglichen Empfänger. Der Rückweg funktioniert analog. Die IP-Adresse des ursprünglichen Absenders wird dabei aber nicht an den Empfänger weitergesendet. Dementsprechend können Proxy-Server immer nur nur für ein bestimmtes Protokoll entwickelt und eingesetzt werden.
Aufgrund der Tatsache, dass sämtliche Anfragen über den Proxy-Server abgewickelt werden müssen, kann dieser Filtermaßnahmen implementieren, die nur schwer umgangen werden können. Dennoch sind Proxy-Server aufgrund ihrer hohen Kosten in kaum einem Staat landesweit in Betrieb. Einige wenige Ländern sind hier Süd-Arabien oder Burma [5] [1].
Auch einige Telekommunkationsunternehmen, unter anderem AOL, betreiben Proxy-Server, meist allerdings als Serviceangebot für Ihre Kunden, um beispielsweise Minderjährige vor pornographischen Websites zu schützen. Hauptsächlich anzutreffen sind Proxy-Server aber in Unternehmen, um ihre Mitarbeiter vor Spielen oder anderen Tätigkeiten während der Arbeitzeit abzuhalten, sowie auch in öffentlichen Bibliotheken. Unter anderem ist jede US-Bibliothek dazu verpflichtet, Proxy-Server zu betreiben [4].

2.4 Schlüsselwort-Filterung

Filterung anhand von Schlüsselwörtern kann auf verschiedene Arten geschehen. Die effektivste Methode hierbei ist, den Uniform Resource Locator (URL) aus dem HTTP-Protokoll zu filtern und zu analysieren. Die URL ist Bestandteil der GET- aber auch der POST-Methode des HTTP-Protokolls, und besteht aus der Domain sowie dem Pfad der Website, von dem bzw. an den Daten angefordert bzw. gesendet werden. Webbrowser zeigen die URL der aktuellen Website typischerweise in der Adressezeile an. Die GET- und POST-Methoden sind simple Methoden des HTTP-Protokolls um Daten anzufordern oder an den Webserver zu senden.
Bei der Analyse wird das Daten-Paket, welches die URL enthält, auf einem Router abgefangen und in einzelne Wörter zerlegt. Diese Wörter werden anschließend mit einer internen Liste verglichen und bei einem positiven Treffer das

[1]Eine Liste von freien Proxy- und DNS-Server kann unter [7, *Freerk*, HOWTO bypass Internet Censorship] eingesehen werden

Paket gefiltert. Zudem wird eine Fehlermeldung an den ursprüngliche Absender des Pakets gesendet, indem er über die ungültige URL unterrichtet wird [4].
Um Zeit und damit Kosten für die Analyse zu sparen, kann die IP-Adresse der eben gefilterten Website temporär komplett blockiert werden. Dass dabei möglicherweise auch andere Websites betroffen sind (Abschnitt 2.1), ist aufgrund der temporären Blockade nicht weiter von großer Bedeutung.
Eine andere Form von Filterung auf Basis von Schlüsselwörtern, ist die Filterung von Suchergebnissen bei Suchmaschinen. Viele relevante Informationen werden heutzutage über Suchmaschine gesucht. Suchergebnisse werden anhand den vom Benutzer eingegebenen Schlüsselwörtern gesucht. Dementsprechend bietet es sich an, Ergebnisse anhand dieser eingegebenen Schlüsselwörtern aber auch anhand der Suchergebnisse zu filtern. Eine Zusammenarbeit mit den jeweiligen Suchmaschinenbetreibern ist für die Umsetzung dieser Filtermethode jedoch unabdingbar. Wie Human Rights Watch [8] und die OpenNet Initiative [2] berichtet, hat unter anderem die Volksrepublik China eine solche Vereinbarung mit einigen Suchmaschinenbetreibern (Google, Yahoo!, MSN) geschlossen. Hierzu aber in Abschnitt 3 mehr.

3. THE GREAT FIREWALL OF CHINA

Die Volksrepublik China hat eine langjährige Tradition, Zensur auf verschiedenste Arten und Ebenen zu betreiben. Der dezentrale Aufbau des Internet und dessen Basis-Protokolle wurde hingegen konzipiert, um Ausfallsicherheit zu gewährleisten. Dieser Ansatz macht jedoch Zensur für die Regierung der Volksrepublik China nicht nur kostspielig und zeitaufwendig, sondern auch fehlerhaft. Dennoch verhindert die "Great Firewall of China"[2] (GFC), so werden die technischen Maßnahmen, die die Zensur des Internet innerhalb China ermöglichen, genannt, den Zugriff auf "verbotene Inhalte" wirkungsvoll.
Wie Cherry [4] schreibt, begann China Mitte der 90er mit der Zensur des Internet. Anfänglich noch mit direkter Blockierung bestimmter IP-Adressen und den damit verbundenen Nebeneffekten (Abschnitt 2.1), wurde das System sukzessive um die Maßnahme der DNS-Manipulation (Abschnitt 2.2) und seit Ende 2002 [14] um die Maßnahme der Schlüsselwort-Filterung sowie der Analyse des gesamten HTTP-Verkehrs erweitert. Wie sich in den folgenden Abschnitten aber genauer zeigen wird, filtert die GFC keine Pakete im wortwörtlichen Sinn, das heißt indem sie Pakete nicht mehr weiterleitet. Vielmehr nutzt Sie Eigenheiten des TCP-Protokolls aus um eine Verbindung und damit die Übertragung von Daten zu unterbrechen.

3.1 Technische Wirkungsweise

Wie von Clayton *et al.* [5] ursprünglich untersucht und mittlerweile weitgehend bekannt und bestätigt [6] [14] [2], arbeitet die GFC ähnlich der Schlüsselwort-Filterung (Abschnitt 2.4), analysiert aber grundsätzlich alle HTTP-Pakete, während diese die einzelnen Router innerhalb Chinas passieren. Sobald ein Paket mit einem "verbotenen Inhalt" von einem Router entdeckt wird, erzeugt dieser, oder ein an den Router gekoppeltes Gerät, TCP-Pakete mit gesetztem RST-

[2]In Anlehnung an die chinesische Mauer

```
cam(54190)  → china(http) [SYN]
china(http) → cam(54190)  [SYN, ACK] TTL=39
cam(54190)  → china(http) [ACK]
cam(54190)  → china(http) GET /?falun HTTP/1.0<cr><lf><cr><lf>
china(http) → cam(54190)  [RST] TTL=47, seq=1, ack=1
china(http) → cam(54190)  [RST] TTL=47, seq=1461, ack=1
china(http) → cam(54190)  [RST] TTL=47, seq=4381, ack=1
china(http) → cam(54190)  HTTP/1.1 200 OK (text/html)<cr><lf> etc...
cam(54190)  → china(http) [RST] TTL=64, seq=25, ack zeroed
china(http) → cam(54190)  ...more of the web page
cam(54190)  → china(http) [RST] TTL=64, seq=25, ack zeroed
china(http) → cam(54190)  [RST] TTL=47, seq=2921, ack=25
```

Abbildung 2: Aufzeichnung der ein- und ausgehenden TCP-Pakete während des Aufrufs einer Website mit verbotenem Schlüsselwort in der URL. Quelle: [5, *Clayton et al.*, Ignoring the Great Firewall of China]

Flag[3] und sendet sie sowohl an den Absender als auch auch den Empfänger des ursprünglichen Pakets. Gemäß Definition des TCP-Protokolls muss sowohl der ursprünglicher Absender als auch der Empfänger annehmen, der Kommunikationspartner möchte die Verbindung abbrechen, und beendet den Datenaustausch.
Wie in Abbildung 2 ersichtlich ist, sendet die GFC dabei drei verschiedene RST-Pakete mit unterschiedlichen Sequenznummern[4], um sicherzustellen, dass diese auch vom Empfänger akzeptiert werden. Der Einfachheit halber wurde bei dieser Aufzeichnung der Pakete darauf geachtet, dass das Paket mit der GET-Methode die Sequenznummer 1 besitzt. Das erste RST-Paket besitzt somit die selbe Sequenznummer wie das "GET-Paket". Beim zweiten und dritten RST-Paket, wurde die Sequenznummer um 1460 Bytes[5] bzw. 3x1460 Byte erhöht. Gemäß Definition des TCP-Protokolls wäre in diesem Fall ausschließlich das zweite Paket vollständig korrekt.
Ebenfalls auffallend sind die unterschiedlichen TTL-Werte[6] zwischen dem SYN+ACK-Paket[7] und den RST-Paketen, die darauf hinweisen, dass die RST-Pakete von einem anderen Absender stammen. Unter der Annahme, dass die TTL-Werte auf den (üblichen) Wert 64 initialisiert wurden, sind die RST-Pakete 8 Hops[8] vom ursprünglichen Kommunikationspartner entfernt, erzeugt und versandt worden.
Crandall *et al.* [6] stellte zudem fest, dass die GFC innerhalb Tageszeiten, bei denen das Internet am meisten genutzt wird, erst sehr verspätet RST-Pakete versendet. Diese Verspätung kann dazu führen, das die Datenübertragung zum Zeitpunkt des Eintreffens der RST-Pakete schon abgeschlossen ist und somit keine Filterung mehr stattfinden kann. In

[3]Ist Teil des TCP-Protokolls [11] und setzt eine TCP-Verbindung, also die Kommunikation zwischen zwei Teilnehmern, zurück (Reset). Folgend kurz RST-Paket genannt.
[4]Stellt die Reihenfolge der TCP-Pakete beim Zusammenbau der gesendeten Daten auf Empfängerseite sicher. Sie erhöht sich pro Paket um die Anzahl der bereits gesendeten Bytes.
[5]Ein TCP-Paket mit 1460 Bytes Nutzdaten wird auch "full-size"-Paket genannt
[6]"**T**ime **T**o **L**ive" (TTL) ist Teil des IP-Protokolls [10]. Der TTL-Wert wird beim Erzeugen des Pakets vom Absender initialisiert und auf dem Weg zum Empfänger von jedem Router decrementiert. Auf diese Weise kann verhindert werden, das Pakete endlose Zeit unterwegs sind.
[7]Zweites Paket im Drei-Wege-Handshake (Verbindungsaufbau) des TCP-Protokolls. Dient zur Synchronisierung der Sequenznummern.
[8]Weg von einem Router zum nächsten

Messungen war dies bei bis zu 25% aller Verbindungen der Fall. Es ist daher davon auszugehen, das die GCF nicht Teil des Routers, sondern vielmehr ein eigenständiges, an den Router gekoppeltes Gerät ist.
Clayton *et al.* [5] untersuchte auch die RST-Pakete, die von der GFC an den ursprünglichen Kommunikationspartner innerhalb Chinas versendet werden und stellte dabei fest, dass diese einen anderen TTL-Wert besitzen und somit scheinbar von einem anderen Router stammen. Es ist daher anzunehmen, dass es mehrere Filterpunkte auf dem Weg zum Empfänger gibt oder aber der TTL-Wert für die RST-Pakete nicht immer auf 64 initialisiert wird. Eine genaue Erklärung hierfür gibt es aber bislang nicht.

3.2 Umgehung der GCF

Wie nun gezeigt, filtert die GFC keine Pakete im wortwörtlichen Sinn, sondern vertraut darauf, dass mindestens einer der Kommunikationspartner die erzeugten RST-Pakete richtig interpretiert und die Verbindung abbricht. Würden nun beide Kommunikationspartner so konfiguriert werden, das sie RST-Pakete gänzlich ignorieren, wäre die GCF wirkungslos. Das diese Methode tatsächlich funktioniert, beweist Clayton *et al.* [5] unter Zuhilfenahme von *iptables*, der Standard Firewall für Linux.
Durch diese Umgehung zeigt sich jedoch eine weitere Filtermaßnahme der GCF: Nach Erkennung eines "verbotenen Inhaltes", werden weitere Verbindungen zwischen den Kommunikationspartnern für ein Zeitfenster von durchschnittlich 20 Minuten blockiert – unabhängig vom Inhalt der Übertragung. Für diese Blockade versendet die GCF zum einen weiterhin gefälschte RST-Paketen, zum anderen nimmt sie sich eine zweite Eigenheit des TCP-Protokolls zu eigen. Während des Aufbaus der TCP-Verbindung sendet sie ein SYN+ACK-Paket mit gefälschter Sequenznummer an den Absender. Dieser geht davon aus, dass das Paket korrekt sei und verwendet diese Sequenznummer als Basis für weitere Pakete. Da nun Absender und Empfänger unterschiedliche Sequenznummern verwenden, also nicht synchronisiert sind, bricht die Datenübertragung ab. Diese Maßnahme funktioniert jedoch nur, wenn das gefälschte SYN+ACK-Paket vor dem korrekten SYN+ACK-Paket eintrifft. Wie Clayton *et al.* [5] zeigte, lässt sich aber auch das gefälschte SYN+ACK-Paket anhand einiger unüblichen TCP-Flags erkennen und somit ebenfalls umgehen.
Eine einfachere Methode zur Umgehung der Filtermaßnahmen, bei der nicht beide Kommunikationspartner modifiziert werden müssen, ist das Trennen "verbotener Inhalte" mittels HTML-Kommentare (Bsp: "`Fa<!-- comment -->lun`"). Aber auch das Ersetzen der Inhalte durch Bilder oder die Verwendung der im Internet bekannten Leetspeak[9], wäre möglich.
Zur Umgehung der Filtermaßnahmen innerhalb einer URL, lässt sich die URL-Kodierung, gedacht für die Einbindung von Zeichen, die außerhalb des in URLs erlaubten Bereiches liegen, verwenden [14] [6].

3.3 ChinaNet Next Carrying Network

Die Infrastruktur von *China Telecom*, mit über 190 Millionen Kunden das größte Telekommunikationsunternehmen in der Volksrepublik China, existiert seit dem Jahr 1993,

[9]Dabei werden einzelne Buchstaben durch ähnlich aussehende Ziffern oder Zeichenfolgen ersetzt.

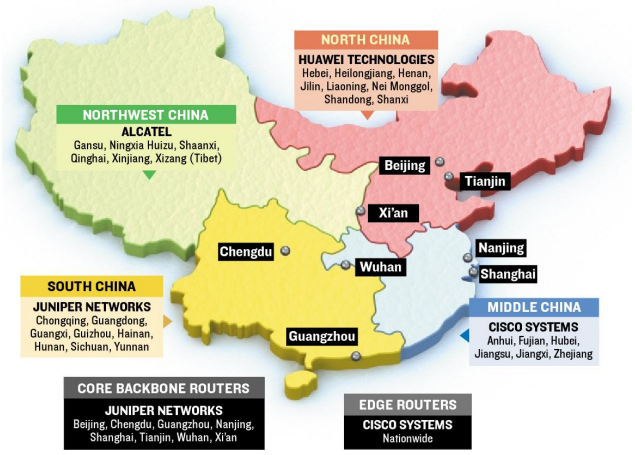

Abbildung 3: Zentralisierter Aufbau des "ChinaNet Next Carrying Network" (CN2). Aufteilung der Regionen auf einzelne Hersteller. Quelle: [4, *S. Cherry*, The net effect]

so Cherry [4]. Dies klingt, verglichen mit europäische Verhältnisse, nicht weiter ungewöhnlich. Beachtet man jedoch die Tatsache, das erst knapp 16% der Bevölkerung Chinas einen Zugang zum Internet haben[10] und die alte Infrastruktur nicht für den Betrieb von aufstrebenden Diensten wie Voice over IP oder Video-Streaming, die vor allem sehr viel Bandbreite benötigen, gebaut wurde, verwundert es nicht, das die Regierung Chinas bereits an einer Alternative arbeitet. Diese Alternative nannte *China Telecom* "ChinaNet Next Carrying Network" (CN2) und investierte dafür 100 Millionen US-Dollar.
CN2 soll nicht nur den Zugang zum Internet (unter anderem durch Einsatz von IPv6 und QoS) schneller machen, es soll vor allem auch die Zensur in China weiterhin ermöglichen. Hierzu wurde schon während der Entwicklung des Netzaufbaus darauf geachtet, möglichst zentrale Knotenpunkte zu konzipieren. Die Router-Hardware, die für CN2 benötigt werden, wurde auf drei westliche und einen chinesischen Hersteller aufgeteilt. Die acht Core-Router, die auf acht Ballungszentren im gesamten Land verteilt werden, werden von *Juniper* geliefert. Sie sind die Knotenpunkte, die Datenpaket auf dem Weg ins Land hinein, innerhalb größerer Regionen des Landes aber auch aus dem Land hinaus, passieren müssen. Die Verbindungen der Core-Router zu einzelnen Städten und Provinzen stellen die Router des Herstellers *Cisco* her. Die Verteilung innerhalb der einzelnen Städte wurde auf Hardware der Hersteller *Alacatel*, *Huawei*, *Juniper* und *Cisco* aufgeteilt. Dabei wurde das gesamte Land in 4 Bereiche (Abbildung 3) geteilt, wobei jedes Unternehmen, eine andere Region zugewiesen bekam.
Obgleich ein Datenpaket bei CN2 ähnlich viele Router passieren muss, wie bei einem dezentralen, aber historisch gewachsenem Netz, so besitzt CN2 einen höchst zentralistischen Aufbau und bietet dementsprechend viele Möglichkeiten zur Zensur. Laut Seth Finkelstein, ein Experte für Internet-Zensur [4], kann und wird Filterung sogar an jedem Router stattfinden.

[10]Quelle: Focus Online, `http://www.focus.de/digital/internet/internet_aid_265095.html`

3.4 Weitere Maßnahmen

Die Regierung der Volksrepublik China überlässt die Zensur im Internet nicht gänzlich ihrer ausgefeilten Technik. Unter anderem sind zwischen 30 000 und 50 000 "Internet Cops" im Einsatz, die das Netz neben ihrer Tätigkeit zur Verbrechensaufklärung im Zusammenhang mit dem Internet, auch nach "subversiven Inhalten" absuchen. Wird eine solche Seite gefunden, so landet sie auf dem Index. Zusätzlich wird durch diese Maßnahme die Last bei der Filterung der Datenpakete in den Routern reduziert.

Eine weitere Zensurmaßnahme ist die staatliche Lizenz für Internet Anbieter (ISP) und Internet Cafés, die für den Betrieb benötigt wird. Internet Cafés sind verpflichtet pornographische Inhalte zu filtern. Andernfalls kann ihr Geschäft geschlossen werden. ISP müssen sogar den gesamten Verkehr, der ihr Netz durchquert, aufzeichnen und analysieren. Sollte ein Kunde gegen geltende Gesetze verstoßen, so müssen die relevanten Daten an 3 staatliche Behörden weitergeleitet und anschließend gelöscht werden, so Cherry [4].

Wie Crandall *et al.* [6] bei ihrer Arbeit zum Aufbau einer Liste von gesperrten Wörtern untersuchte, enthält diese Liste nicht nur historische und politische Geschehnisse der Vergangenheit und Gegenwart, sondern auch Namen wie 北莱茵-威斯特法伦 ("Nordrhein-Westfalen"), ein Bundesland innerhalb Deutschlands. Durch weitere Analyse stellte man fest, dass alleine die chinesischen Zeichen 法伦 ("falen") ausreichen, um eine Sperre zu initiieren. Der Grund hierfür, so wird vermutet, liegt darin, den Namen der aus China stammenden, verbotenen, religiösen Bewegung "Falun Gong", zwar grundsätzlich falsch aber phonetisch ähnlich zu verwenden, um damit die Filterung zu umgehen.

Auch große westliche Suchmaschinenbetreiber, darunter unter anderem Google, Yahoo! und MSN, zensieren Ihre Suchergebnisse und Angebote, um nicht von der Regierung verboten zu werden. Laut Human Rights Watch [8] wurde die Liste der "verbotenen Wörter", die Google für ihr chinesisches Angebot intern verwendet, sogar von Google selbst erstellt. Auf diese Tatsache angesprochen, antwortete Andrew McLaughlin, Senior Policy Counsel bei Google: "We concluded that although we weren't wild about the restrictions, it was even worse to not try to serve those users at all. We actually did an evil scale and decided not to serve at all was worse evil."[11]

4. DISKUSSION

Obwohl diese Arbeit ausschließlich die Zensur des Internet in östlichen Ländern behandelt, so findet diese heutzutage vermehrt auch in westlichen Ländern Anwendung – wenn auch um einiges subtiler. So müssen ISP in Italien seit 2006 sämtlichen Zugang zu Internet Seiten sperren, die Online Glücksspiele anbieten[12]. Im Oktober 2007 musste der deutsche ISP *Arcor* den Zugriff auf die pornographische Website *youporn.com* per einstweiliger Verfügung sperren[13]. Im Hauptsacheverfahren wurde dem Einspruch Arcors aber stattgegeben und die Sperre wieder aufgehoben.

Auch der Aufbau des CN2 birgt Gefahren für andere Länder. Obgleich das Internet dezentralistisch aufgebaut ist, so gleicht es sich aufgrund ökonomischer Faktoren aber auch durch Zusammenschlüsse und Übernahmen von großen ISP und Carrieren und dem damit verbundenen Abbau von Redundanzen, immer mehr dem Aufbau eines zentralistisch Netzes an. Somit wäre es für Staaten unter Zuhilfenahme des in China gewonnenen Know-Hows durchaus möglich, das Internet ähnlich zu zensieren.

Dennoch bietet der heutige Stand der Technik keine Möglichkeit das Internet zu filtern und dabei keinen Weg zur Umgehung offen zu lassen. Es stellt sich jedoch die Frage, ob bei der immer leistungsstärker werdenden Router-Hardware, ein Zeitpunkt erreicht werden kann, an dem Datenpakete in Echtzeit analysiert und somit direkt gefiltert werden können.

[11] Quelle: `http://blog.searchenginewatch.com/blog/060130-154414`

[12] Quelle: `http://opennet.net/research/regions/europe`

[13] Quelle: `http://www.heise.de/newsticker/meldung/106513`

5. REFERENCES

[1] D. Bambauer, R. Deibert, R. Rohozinski, N. Villeneuve, and J. Zittrain. Internet filtering in burma in 2005: A country study, Oct. 2005. `http://opennet.net/studies/burma/`.

[2] D. Bambauer, R. Deibert, R. Rohozinski, N. Villeneuve, and J. Zittrain. Internet filtering in china in 2004-2005: A country study, Apr. 2005. `http://opennet.net/studies/china/`.

[3] R. K. C. Chang and K. P. Fung. Transport layer proxy for stateful UDP packet filtering. In *Computers and Communications, 2002. Proceedings. ISCC 2002. Seventh International Symposium on*, pages 595–600, July 2002.

[4] S. Cherry. The net effect: as china's internet gets a much-needed makeover, will the new network promote freedom or curtail it? *IEEE Spectrum*, 42(6):38–44, June 2005.

[5] R. Clayton, S. J. Murdoch, and R. N. M. Watson. Ignoring the great firewall of china. In *Privacy Enhancing Technologies*, volume Volume 4258/2006, pages 20–35. Springer Berlin / Heidelberg, 2006.

[6] J. R. Crandall, D. Zinn, M. Byrd, E. Barr, and R. East. Conceptdoppler: a weather tracker for internet censorship. In *CCS '07: Proceedings of the 14th ACM conference on Computer and communications security*, pages 352–365, New York, NY, USA, 2007. ACM.

[7] Freerk. *HOWTO bypass Internet Censorship*, 2008. `http://www.zensur.freerk.com/`.

[8] R. MacKinnon, B. Adams, S. Richardson, A. Ganesan, and I. Gorvin. "race to the bottom"corporate complicity in chinese internet censorship. *Human Rights Watch Report*, 18(8), Aug. 2006.

[9] J. Postel. User Datagram Protocol. RFC 768 (Standard), Aug. 1980. `http://www.ietf.org/rfc/rfc768.txt`.

[10] J. Postel. Internet Protocol. RFC 791 (Standard), Sept. 1981. Updated by RFC 1349, `http://www.ietf.org/rfc/rfc791.txt`.

[11] J. Postel. Transmission control protocol. RFC 793 (Standard), Sept. 1981. Updated by RFC 3168, `http://www.ietf.org/rfc/rfc793.txt`.

[12] R. Rosenberg. Controlling access to the internet: The role of filtering. *Ethics and Information Technology*, 3(1):35–54, Mar. 2001.

[13] R. Zalenski. Firewall technologies. *IEEE Potentials*, 21(1):24–29, Feb./Mar. 2002.

[14] J. Zittrain and B. Edelman. Internet filtering in china. *IEEE Internet Computing*, 7(2):70–77, Mar./Apr. 2003.