Internetzensur in China

Ausarbeitung zum Seminarthema
Internetzensur in China – Projekt „Goldener Schild“, „Grüner Damm“

Wintersemester 2010/2011
an der Humboldt Universität zu Berlin.

Daniel Schliebner

Herausgabe: 25. März 2011

Inhaltsverzeichnis

1. Einführung

Diese Arbeit umfasst eine Ausarbeitung des von mir im Wintersemester 2010/2011 gehaltenen Vortrages zum Thema *Internetzensur in China – Projekt „Goldener Schild“, „Grüner Damm“.*

Zu den Olympischen Sommerspielen im Jahr 2008 in Beijing (Peking) entstand in der breiten Öffentlichkeit erstmals ein reges Interesse an den Internet-Zensurmaßnahmen der chinesischen Regierung, da diese drastische Auswirkungen auf die journalistische Arbeit aller Pressevertreter der an den Olympischen Spielen partizipierenden Nationen zur Folge hatten. Hinter diesen Zensurmaßnahmen steht der bereits 1998 in Auftrag gegebene *Goldene Schild* (in westlicher Literatur zumeist auch *Große Firewall*) Chinas, ein Konglomerat verschiedener Technologien zur Kontrolle und Überwachung des chinesischen Internetverkehrs.

Das erste Kapitel dieser Arbeit soll darstellen, welche Entwicklung das Projekt seit seiner Initiierung 1998 durch die Kommunistische Partei Chinas (KPCh) genommen hat und durch welche Mechanismen eine Zensur und Kontrolle des Internetverkehrs in China möglich ist. Konkret wird dabei im zweiten Abschnitt des Kaptitels im Detail erläutert werden, an welchen Stellen Zensur eingesetzt wird und wie dies technisch funktioniert. Der dritte Abschnitt beschäftigt sich mit verschiedenen Ansätzen zur Umgehung der eingesetzten Filtermaßnahmen an den Backbone-Gateways und wägt dabei Vor- und Nachteile dieser ab, um ein Bild darüber zu geben, welche Umgehungsmaßnahmen realistische Anwendung finden können bzw. wie effektiv Chinas Goldener Schild arbeitet. Der vierte Abschnitt gibt einen partiellen Überblick über den Inhalt und den Umfang des durch den Goldenen Schild gefilterten Internetverkehrs, d. h. es werden konkrete Beispiele gefilterten Inhalts präsentiert, ohne dabei eine vollständige Listung des gefilterten Inhalts geben zu können; letzteres insbesondere daher, da sich die zensierten Inhalte einer ständigen Fluktuation ausgesetzt sehen. Der fünfte und letzte Abschnitt des ersten Kapitels diskutiert schließlich die Rolle westlicher Unternehmen und gibt Beispiele.

Das zweite Kapitel ist dem Projekt „Grüner Damm“ gewidmet, welches offiziell als Internet-Filtersoftware zum Zwecke des Jugendschutz anfang 2008 vom chinesischen Ministerium für Industrie und Informationstechnik (MIIT) in Auftrag gegeben wurde. Ziel sollte insbesondere die Filterung von pornographischen und gewalttätigen Inhalten sein. Allerdings geriet die Software schnell in den Fokus von Kritikern, da vom MIIT gefordert wurde, dass diese ab dem 01. Juli 2009 auf jedem in China ausgelieferten Computer vorinstalliert sein müsse. Daraufhin wurden schnell Bedenken öffentlich, nach welchen die Software auch zu Zensurzwecken genutzt werden könne. In der Tat offenbarte sich schnell, dass von der Software „Grüner Damm“ genutzte Blacklists blockierter URLs und Schlagwörter auch

politische Begriffe beinhalteten. Nicht zuletzt die darüber hinaus aufgetretenen zahlreichen Qualitätsmängel und Sicherheitslücken der Software führten schließlich dazu, dass das Projekt „Grüner Damm“ seit Juli 2010 de facto eingestellt ist. Neben einem kurzen Abriss der historischen Entwicklung im ersten Abschnitt des zweiten Kapitels, klärt der Zweite technische Details zu eingesetzten Filtern und der Funktionsweise der Software, wobei der dritte Abschnitt schließlich die aufgedeckten Sicherheitslücken erläutert.

2. Projekt Goldener Schild

2.1 Historische Entwicklung

Die Geschichte der Internetzensur in China ist im Wesentlichen so alt wie die Geschichte des Anschlusses Chinas an das globale Internet [12]. In der Tat gelang China im Januar 1996 erstmals global der Anschluss an das internationale Internet und bereits am 1. Februar des gleichen Jahres wurde eine erste Richtlinie zur Regulierung des chinesischen Internets durch den chinesischen Staatsrat heraugegeben. Diese Regulierungen wurden bis zum Dezember 1997 nicht zuletzt auch durch das chinesische Ministerium für Staatssicherheit (MfS) stetig weitergeführt und spezifizierten unter anderem fünf Arten abträglicher Aktivitäten, vgl. [10, 11]:

> *„(1) Eindringen in ein Computernetzwerk oder das Zunutzemachen von Netzwerkressourcen ohne Authorisation.*
> *(2) Entfernen, Verändern oder Hinzufügen von Funktionen zu einem Computernetzwerk ohne Authorisation.*
> *(3) Entfernen, Verändern oder Hinzufügen von Daten und Anwendungssoftware zum Zwecke der Speicherung, Verarbeitung oder Übertragung in einem Computernetzwerk ohne Authorisation.*
> *(4) Absichtliches Erzeugen und Verbreiten schädlicher Software wie etwa einem Computervirus.*
> *(5) Weitere Aktivitäten, welche sich schäglich auf die Sicherheit eines Computernetzwerks auswirken.“* [11]

Als Reaktion auf die Gründung der Demokratischen Partei Chinas (CDP) am 25. Juni 1998, einer der ersten oppositionellen Parteien Chinas, initiierte die Kommunistische Partei Chinas (KPCh) im selben Jahr schließlich das Projekt „Goldener Schild“, welches zugleich mit dem Verbot der CDP einherging. Ziel war offiziell die Stärkung der Exekutive, nicht zuletzt ist der Grund aber darin zu vermuten, dass oppositionelle Bewegungen in China (wie die der CDP) zunehmend Gebrauch von digitalen Medien, insbesondere der des Internets, machten. Dementsprechend lag es der KPCh nahe, eine staatliche Kontrolle des Internetverkehrs innerhalb Chinas zu initiieren. Mit der Realisierung und Entwicklung des Projektes wurde das MfS – damals unter der Führung von Xu Yongyue – beauftragt.

Den Weg zur Fertigstellung ebneten zahlreiche Messen, an denen auch diverse westliche Unternehmen teilnahmen. Das Ziel dieser Messen war vornehmlich die für die Umsetzung benötigte Filtertechnik und -Software zu sichten und zu erwerben. Als eine der ersten Messen ist hier die „Security China 2000“ im November 2000 in Beijing zu nennen [3]. An ihr nahmen bereits zahlreiche (westliche) Unternehmen teil, zu deren Repertoire vor allem Netzwerktechnik sowie Mobilfunktechnik gehörten (etwa Nortel, Nokia, Ericsson oder Cisco, siehe [3, S. 8]). Als eine der ersten kritischen Auseinandersetzungen zum „Goldenen Schild“ ist dort unter anderem auch folgendes Zitat von Greg Walton zu lesen:

> *„Old style censorship is being replaced with a massive, ubiquitous architecture of surveillance: the Golden Shield. Ultimately the aim is to integrate a gigantic online database with an all-encompassing surveillance network – incorporating speech and face recognition, closed-circuit television, smart cards, credit records, and Internet surveillance technologies. This has been facilitated by the standardization of telecommunications equipment to facilitate electronic surveillance, an ambitious project led by the Federal Bureau of Investigation (FBI) in the US, and now adopted as an international standard.“* [3, S. 5]

Der nächste große Schritt zur Fertigstellung war die Veranstaltung „Information Technology for China's Public Security“ im September 2002, auf der Li Runsen - der damalige technische Leiter am MfS – das Projekt „Goldener Schild“ mehr als tausend Exekutivmitgliedern vorstellte, gefolgt von der Messe „Comprehensive Exhibition on Chinese Information System“ vom 06. bis 10. Dezember 2002. Beide Veranstaltungen fanden ebenfalls in Beijing statt, wobei an letzterer wiederum zahlreiche westliche Unternehmen teilnahmen. Die viertägige Messe nutzten über 300 Mitarbeiter des Projektes „Goldener Schild“, um diverse westliche Sicherheitsprodukte wie Filtersoftware, Backbone-Router und ähnliches in großem Maßstab einzukaufen. Bis Ende 2002 kostete das Projekt geschätzte 800 Millionen US Dollar [9].

Nach fünf Jahren Entwicklung ging das Projekt schließlich im November 2003 in den Test-Betrieb auf kommunaler Ebene und fand seine Fertigstellung schließlich mit der landesweiten Inbetriebnahme im Jahr 2006.

Bis heute unterliegt der gefilterte Inhalt, sowie das Ausmaß der Überwachung ständiger Fluktuation, jeweils abhängig von der aktuellen politischen Lage. Ein ausgezeichnetes Beispiel stellen etwa die Olympischen Sommerspiele 2008, wie in der Einleitung erläutert, dar [6], wobei aber z. B. auch zu politisch kritischen Anlässen, wie etwa dem Jahrestag des „Tian'anmen Massakers“, eine deutliche Veränderung im Verhalten der im Projekt „Goldener Schild“ eingesetzten Filter zu erkennen ist [7]. Wie diese Filter im Detail funktionieren und wo sie eingesetzt werden, soll unter anderem Gegenstand des nächsten Abschnitts sein.

2.2 Technische Diskussion

Die Internetzensur im Rahmen des Projektes „Goldener Schild“ besteht im Wesentlichen aus drei Aspeken:

1. Durch Zensoren überwachte Inhalte im Internet (Blogs, Foren, ...).
2. Delegierte Zensur.
3. Filter(-Software) an Backbone-Gateways.

Im Folgenden werden diese im Einzelnen diskutiert und erkläutert.

2.2.1 Zensoren

Die Ressource Mensch wird im Projekt „Goldener Schild“ durch ca. 30.000 bis 50.000 Zensoren repräsentiert [13]. Deren Aufgabe ist es, das chinesische Internet täglich nach politisch kritischen oder anstößigen Inhalten zu durchforsten. Konkret löschen und ändern sie dabei Beiträge in sozialen Netzwerken respektive Kommunikationsplattformen wie Chats, Blogs und Foren bzw. lenken von politischen oder anstößigen Diskussionen unter falschen Pseudonymen ab. Symbolisiert werden die Zensoren – auch gehandelt als „Internetpolizei“ – durch zwei Comicfiguren mit den Namen „Jingjing“ und „Chacha“, vgl. Abbildung 2.1.

Abbildung 2.1: Jingjing und Chacha. Abbildung aus [14].

2.2.2 Delegierte Zensur

Bei über 221 Millionen chinesischen Internet-Nutzern (Stand 2008, [8]) können die im vorangegangenen Abschnitt 2.2.1 erläuterten Maßnahmen selbstverständlich nicht den gesamten täglichen Internetverkehr kontrollieren. Neben der technischen Kontrolle des ein- und ausgehenden Internetverkehrs, welche in Abschnitt 2.2.3 im Detail erklärt wird, setzt die Regierung dabei zusätzlich auf den Effekt der delegierten Zensur (auch „Chillingeffekt“). Konkret gibt es innerhalb der Volksrepublik China zahlreiche, teils streng verfolgte, Auflagen und Registrierungspflichten für mannigfaltig ausgeartete Formen von Diensten. Diesen Pflichten unterliegen unter anderem die folgenden Anbieter:

1. Internet Service Provider (ISP),
2. E-Mail-Anbieter,
3. Anbieter von (auch ausschließlich privaten) Nachrichtendiensten,
4. Anbeiter von multimedialen (bzw. rundfunkähnlichen) Diensten,
5. Anbieter von Blogs, sowie
6. verschiedene weitere Dienst-Provider (etwa VPN).

D. h., möchte ein Dienstleister in China etwa eine der vorhergehenden Leistungen anbieten, so verpflichtet er sich gegenüber der Regierung zu verschiedensten Kontroll- und Zensurmaßnahmen. Diese gleichen zum Teil den Aufgaben der Zensoren aus Abschnitt 2.2.1: kontrolliert und zensiert werden zumeist politische Inhalte. Insbesondere die ISPs spielen in diesem Konzept natürlich eine wesentliche Rolle, da durch sie der gesamte chinesische Internet-Datenverkehr gelangt. Eine Kontrolle dieser Anbieter ist also – aus Sicht der Exekutive – mehr als zweckmäßig. Des Weiteren ist die „China Telecom“, mit ca. 62% aller Breitbandanschlüsse der größte ISP Chinas, de facto in staatlicher Hand. „China Telecom“ stellte zu Beginn der Geschichte des Internets in China Anfang 1996 die ersten Backbones bereits und kann damit als erster ISP Chinas bezeichnet werden. Offiziell ist sie seit 2002 kein staatlicher Monopolbetrieb mehr, da ein Teil der Geschäftsaktivitäten in die „China Netcom“ ausgegliedert wurde. Es bleibt aber zweifelhaft, inwieweit „China Telecom“ als regierungsunabhängiges Unternehmen bezeichnet werden kann. Dass fast jeder Route über Gateways der „China Telecom“ führt, kann leicht durch eine Routenverfolgung zu einer chinesischen Domain (z. B. vermittels `tracert` [Windows] oder `traceroute` [Unix]) nachvollzogen werden:

```
> tracert www.google.cn
  ⋮
  8    26 ms    27 ms    29 ms  202.97.73.13
  9   288 ms   288 ms   281 ms  202.97.52.61
 10   356 ms   364 ms   376 ms  202.97.53.25
 11   494 ms   501 ms   516 ms  202.97.53.125
 12   513 ms   512 ms   504 ms  202.97.53.93
 13     *        *        *     Zeitüberschreitung der Anforderung.
 14   514 ms   524 ms   537 ms  bj141-130-94.bjtelecom.net [219.141.130.94]
 15   528 ms   530 ms   530 ms  219.142.13.142
 16   534 ms   530 ms   535 ms  203.208.62.43
 17   539 ms   522 ms   525 ms  203.208.62.125
 18   536 ms     *      523 ms  bg-in-f104.1e100.net [203.208.37.104]
```

Diese auferlegten Pflichten führen zu einer delegierten Zensur: um Strafen (finanzieller oder repressiverer Natur) zu entgehen, zensieren sich die Dienste selbst.

Ein weiterer Aspekt tritt im Hinblick auf den nächsten Abschnitt auf. Da gerade bei der Übertragung (in welcher Form dies auch immer sein mag) politisch kritischer Begriffe

teilweise der Route zu IP-Adressen oder sogar Subnetzen für eine gewisse Zeitspanne (von teils einigen Minuten bis hin zu einer Stunde) „geblockt“ wird (siehe Abschnitt 2.2.3 für Details), zensieren sich Internetnutzer in China teilweise sogar selbst, um ungestört surfen zu können. Dies ist auch bekannt unter dem Begriff des „Chillingeffekts“.

2.2.3 Filtertechniken

Den in China im Rahmen des „Goldenen Schilds“ eingesetzten Filtern liegen wohlbekannte Techniken zur Analyse und Filterung von Netzwerk-Traffic zugrunde. Insbesondere werden diese durch gewöhnliche, nicht zuletzt auch von westlichen Unternehmen (dies wird auch in Abschnitt 2.5 diskutiert) entwickelte Netzwerk-Applikationen (Firewalls, Intrusion Detection Systems (IDS)) bereitgestellt, welche hauptsächlich an den Backbone-Gateways Chinas installiert sind. Zum Tragen kommen hier unter anderem folgende Techniken der Filterung, Blockierung und Manipulation von Daten oder Datenpaketen:

1. IP-Blockierung,
2. DNS-Filterung und DNS-Poisoning,
3. URL-Filter,
4. Paket-Filter also Deep Packet Inspection (DPI).

Insbesondere die letzten beiden Filtertechniken werden symmetrisch verwendet, d. h., dass sowohl eingehende als auch abgehende Daten aus dem chinesischen Internet in den großen Backbones gefiltert werden. Ein konkretes Beispiel wird bei der Analyse der Paket-Filter besprochen.

Bei der IP-Blockierung wird das Routing einzelner IP-Adressen oder soger ganzer Subnetze verhindert [1]. Betroffen sind hier sowohl TCP-Protokolle (z. B. HTTP, FTP, SMTP, POP) als auch UDP-Protokolle (z. B. VoIP). Bei TCP-Protokollen wird hierbei generell nicht das Routing komplett unterbunden, sondern durch das Senden von TCP-RST Paketen oder fehlerhaften SYN-Paketen ein Abbruch der TCP-Verbindung durch den Client erreicht. Dies wird im Detail bei der Erläuterung der Paket-Filter besprochen.

DNS-Filter werden auf DNS-Servern innerhalb Chinas eingesetzt und blockieren gezielt unerwünschte Domain-Namen, indem sie die Auflösung der DNS in ihre IP unterbinden. Im Gegensatz dazu wird die Auflösung der DNS in eine IP beim DNS-Poisoning nicht unterbunden, sondern auf eine falsche IP umgeleitet. Ein prominentes Beispiel war die Seite *google.com*, siehe [1].

URL-Filter sind im Prinzip ein Spezialfall der nachfolgenden Paket-Filter. Hierbei werden HTTP-Protokolle nach der angefragten URL untersucht und (zusätzlich zur DNS-Filterung) wird dabei die URL nach unerwünschten Begriffen durchsucht. Wird ein solcher Begriff gefunden, so wird die Auflösung der URL blockiert (oder ggf. DNS-Poisoning verwendet). Ruft man beispielsweise die URL

`http://www.google.cn/search?q=falun+gong`

auf (auch von Clients außerhalb Chinas), so induziert dieser Aufruf ein Reset der TCP-Verbindung für eine kurze Zeitspanne - die Webseite `www.google.cn` bleibt blockiert. Wie diese Blockade technisch umgesetzt ist, beschreibt der folgende Absatz.

An Gateways werden für DPI diverse IDS eingesetzt. Diese dienen der Filterung und Analyse von einzelnen Datenpaketen in TCP-Protokollen. Betroffen sind demnach vornehmlich auf TCP aufbauende Protokolle wie HTTP, FTP, SMTP oder POP. In der Regel funktioniert die Paket-Filterung dabei wiefolgt [2]: der Client baut eine TCP-Verbindung zu einem Server auf und sendet verschiedene Datenpakete. Mittels DPI werden diese von den installierten IDS auf unerwünschte Begriffe untersucht. Falls kein solcher Begriff gefunden wird, läuft die Kommunikation ungestört ab. Andernfalls wird direkt nach dem mangelhaften Paket ein TCP-RST Paket an den Client gesendet. Dies hat zur Folge, dass die TCP-Verbindung auf Clientseite unterbrochen wird. Möchte der Client erneut eine Verbindung mit demselben Server herstellen, so bleibt diese (durch das Senden von TCP-RST Paketen) für eine längere Zeitspanne - unabhängig von den versendeten Datenpaketen - blockiert. Zu beobachten sind hier Zeitspannen von 5 bis zu 30 Minuten [2]. Im Spezialfall des HTTP-Protokolls veranschaulichen Abbildung 2.2 und 2.3 den soeben erläuterten Ablauf einer Blockade durch DPI.

```
cam(53382)   → china(http) [SYN]
china(http) → cam(53382)   [SYN, ACK]
cam(53382)   → china(http) [ACK]
cam(53382)   → china(http) GET / HTTP/1.0<cr><lf><cr><lf>
china(http) → cam(53382)   HTTP/1.1 200 OK (text/html)<cr><lf>
china(http) → cam(53382)   ... more of the web page
cam(53382)   → china(http) [ACK]
               ... and so on until the page was complete
```

Abbildung 2.2: Normale Kommunikation von Client und Server. Abbildung aus [2].

```
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>
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 2.3: Reset der TCP-Verbindung mittels DPI. Abbildung aus [2].

Aufgrund des recht langen Timeout ist diese Methode für Internetnutzer besonders nervig: bei Shared-Hostings werden teils verschiedene Webseiten blockiert, welche nicht zwandsläufig mit der ursprünglich blockierten Webseite zusammen hängen. Dies fördert insbesondere auch die bereits angesprochene delegierte Zensur aus Abschnitt 2.2.2.

2.3 Umgehung

Natürlicherweise stellt sich die Frage, wie die Zensurmaßnahmen durch den „Goldenen Schild“ umgangen werden können, da diese zu teils starken zensorischen Maßnahmen ausarten. Im folgenden werden neun Möglichkeiten der Umgehung vorgestellt. Dabei hat jede Vor- und Nachteile. Gänzlich befriedigend ist letztendlich jedoch keine. Der Einsatz der jeweiligen Umgehungsmaßnahme hängt dabei stark von der konkreten Anwendung ab, zu der sie genutzt werden soll. Zum unzensierten Surfen im Internet sind dabei durchaus einige Maßnahmen geeignet.

Regionale Websites sind selbstverständlich nicht von den Zensurmaßnahmen im Rahmen des Projekt „Goldener Schild“ betroffen, da die beschriebenen Zensurmaßnahmen an den Gateways eingesetzt werden. Das Betreiben einer Webseite erfordert jedoch eine staatliche ICP-Lizenz, welche vom MIIT vergeben wird. Die Wahrscheinlichkeit, Inhalte über diesen Weg bereit stellen zu können, welche durch die Zensurmaßnahmen des „Goldenen Schild“ gefiltert würden, ist also eher gering.

Gegen DNS-Filterung und DNS-Poisoning kann ein DNS-Server außerhalb Chinas verwendet werden. Auch möglich wäre ein Proxy-Server, welcher nicht im chinesischen Netz betrieben wird. Hiermit würden die Filtermaßnahmen umgangen, allerdings sind zumeist auch die IP-Adressen dieser externen DNS- und Proxy-Server durch IP-Blockierung gesperrt, sodass der Einsatz in der Regel nicht gelingt; es entsteht auf natürliche Weise ein Katz-und-Maus-Spiel. Die direkte Eingabe der IP-Adresse an Stelle einer URL ist ebenso hilfreich gegen DNS- und URL-Filter hat aber den Nachteil, dass zum einen die IP-Adresse des Ziel-Servers bekannt sein muss und zum anderen greifen dennoch unter Umständen die IP-Blockierungsmechanismen. Insbesondere ist anzunehmen, dass die im Falle von DNS-Filterung und DNS-Poisoning blockierten oder manipulierten DNS-Auflösungen zu bestimmten IP-Adressen auch durch die IP-Blockierung gesperrt sind.

Ein ganz anderer Ansatz, zumindest Filtermechanismen zu umgehen, welche anhand der aufgerufenen URL filtern, besteht in der (Um-)Codierung der Zeichen innerhalb der URL gemäß RFC 2396 (etwa die Verwendung hexadezimaler anstatt ASCII Zeichen). Faktisch ist diese Methode derzeit nicht mehr umsetzbar, da die eingesetzte Filtersoftware mittlerweile auch mit umcodierten URLs umgehen kann.

Da auf der Basis von DPI die meisten Filter greifen, ist es interessant zu untersuchen, welche Methoden die Analyse der versendeten Datenpakete unterbinden können. Der offensichtliche Ansatz, verschlüsselte Verbindungen (z. B. VPN, HTTPS) zu verwenden, ist hierbei zwar zielführend, jedoch wird der Quality of Service (QoS) solcher Verbindungen künstlich verlangsamt, sodass der Einsatz nur in begrenztem Umfang zu empfehlen ist. Den gleichen Nachteil hat auch der Einsatz von Anonymisierungs-Software oder Onion-Routing-Software (z. B. TOR, JAP). Hinzu kommt, dass auch die im Onion-Routing eingesetzten Mix-Kaskaden durch IP-Blockierung gesperrt sein können.

Um möglichst wenig Information in ein versendetes TCP-Datenpaket zu legen, kann es sinnvoll sein, die MTU des verwendeten TCP-Protokolls zu verringern. In Folge dessen

enthält ein Datenpaket weniger Informationsgehalt. Der Nachteil ist jedoch, dass so die Übertragungsgeschwindigkeit durch die erhöhte Anzahl der Datenpakete verlangsamt wird.

Wie in Abschnitt 2.2.3 beschrieben, funktioniert die Filterung durch DPI unter anderem dadurch, dass bei Vorhandensein von zensiertem Inhalt in Datenpaketen ein TCP-RST Paket an den Client gesendet wird. Die Folge ist der Abbruch der Verbindung *durch den Client*. Ignoriert man den RST-Befehl, so kann dies unter Umständen zur Folge haben, dass die Zensurmaßnahmen dadurch außer Kraft gesetzt sind [2]. In der Tat ist dies eine praxistaugliche Umgehungsmaßnahme mit dem Nachteil, dass sie eventuell nur teilweise zielführend ist: teilweise wird der Clientseitige Abbruch der TCP-Verbindung auch anderweitig erreicht, indem etwa ein fehlerhaftes SYN-Paket gesendet wird. Gelingt es, dieses als „künstlich“ zu identifizieren, so kann aber auch dieses Paket manuell ignoriert werden, siehe [2].

Die letzte vorgestellte Möglichkeit der Umgehung bietet die Webapplikation *Picidae* (`http://pici.picidae.net`). Picidae erstellt Abbilder von Webseiten in Form von Bildern, wobei interaktive Bereiche der Webseite (in Begrenztem Umfang) ausgespart werden. Dies hat zur Folge, dass eine DPI im herkömmlichen Sinne nicht mehr möglich ist. In der Tat ist das Surfen teilweise gut möglich, jedoch sind bekannte Picidae-Server in China gesperrt. Es stellt sich also die Schwierigkeit, einen verfügbaren Picidae-Server zu finden. Auch moderne 2.0 Webseiten sind nur begrenzt nutzbar.

2.4 Gefilterte Inhalte - Ein Kurzüberblick

Vornehmlich gefiltert werden Webseiten, URLs oder Datenpakete, welche die Wörter Taiwan, Tibet und Tiananmen enthalten. Darüber hinaus werden u. a. Webseiten mit Bezug zu Falun Gong, Dalai Lama, Youtube, Flickr, Wikipedia, Nachrichtenseiten, SourceForge und Amnesty International teilweise oder ganz blockiert. Eine lange Liste findet sich z. B. unter [1]. Konkret werden spezielle Webseiten in

`http://cyber.law.harvard.edu/filtering/china/Chinahighlights.html`

vorgestellt. Nicht zuletzt werden auch Inhalte mit sexuellem, obszönem und gewalttätigem Bezug gefiltert. Wie die folgende Grafik veranschaulicht, ist die Mehrzahl des gefilterten Inhalts tatsächlich politischer Natur.

Abbildung 2.4: Gefilterte Seiten. Grün: Saudi-Arabien, Rot: China. Abbildung aus [1].

Diese Interpretation ergibt sich aus der Analyse der Autoren von [1]. Die durch das saudi-arabische Internet geblockten Inhalte waren fast ausschließlich sexueller Natur, sodass zu schließen ist, dass der rot markierte Bereich in Abbildung 2.4 größtenteils nichtsexuelle Webseiten darstellt, zumal von den 203217 getesteten Webseiten lediglich 795

URLs mit sexuellem Inhalt in Verbindung standen. Obszöne oder gewalttätige Inhalte standen bei der Studie nicht zur Disposition. Die nachfolgende Grafik gibt noch einmal einen Überblick über den Anteil blockierter Webseiten innerhalb der Google Top 10 (bzw. Top 100) für ausgesuchte Begriffe.

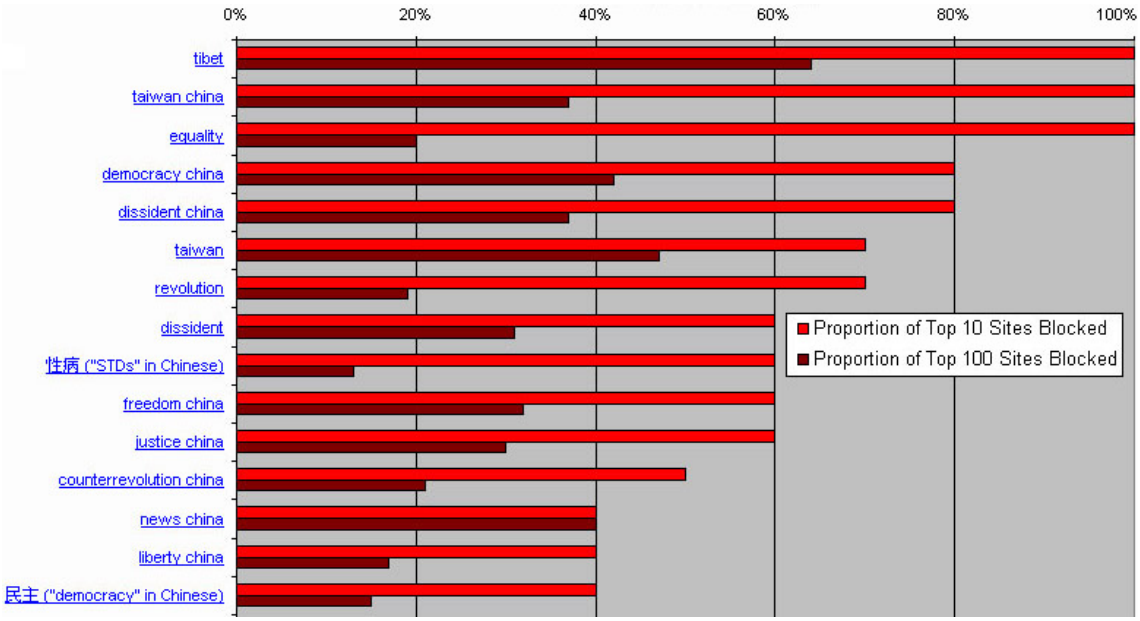

Abbildung 2.5: Gefilterte Seiten nach Begriff. Abbildung aus [1].

2.5 Die Rolle westlicher Unternehmen

Eine zentrale Frage, die sich stellt, ist die der Rolle westlicher Unternehmen im Projekt „Goldener Schild“ und damit in der Internet-Zensur Chinas. Derzeit ist bekannt, dass etwa Yahoo und MSN zensurrelevante Suchergebnisse filtern, um ihre ICP-Lizenz zu behalten und somit ihre Marktposition in China zu stärken. Aus denselben Gründen tut dies seit Juli 2010 auch Google.cn (bzw. Google.com.hk) [15]. Ein weiteres Detail in der Unterstützung der chinesischen Zensurmaßnahmen stellt Yahoo's Shi Tao Affäre dar. Während des 15. Jahrestages des Tiananmen-Massakers gab dieser eine interne Leitlinie an die Asia Democracy Foundation weiter, welche vorschrieb, wie sich während des Jahrestages zu verhalten sei. Yahoo half schließlich der chinesischen Regierung durch Herausgabe seiner Verbindungsdaten, ihn zu überführen [20].

Eine wesentliche Frage in der Unterstützung durch den Westen liegt in der Bereitstellung von Hardware und Software. So wird diverse westliche Filtersoftware an den Backbone-Gateways zur Filterung und Zensur eingesetzt. Wie in Abschnitt 2.2.3 beschrieben, kommen dabei zahlreiche Mechanismen zum Einsatz, die durch herkömmliche IDS und Firewall-Software erreicht werden können. Des Weiteren kommt eine große Zahl der Backbone-Router in China aus dem Westen, etwa von Cisco [7]. Weitere bekannte Software- und Hardware-Lieferanten sind Juniper Networks, Ericsson und Nortel Networks, [7, 3, 6].

3. Projekt Grüner Damm

3.1 Historische Entwicklung

Die Software „Grüner Damm“ wurde offiziell als Internet-Filtersoftware zum Zwecke des Jugendschutzes Anfang 2008 vom MIIT in Auftrag gegeben. Ihr ausgeschriebenes Ziel kann dem folgenden Zitat entnommen werden.

> *„In order to build a green, healthy, and harmonious online environment, and to avoid the effects on and the poisoning of our youth's minds by harmful information on the internet, . . .“* [16]

Das Ziel war also insbesondere die Filterung von pornographischen und gewalttätigen Inhalten. Mit der Entwicklung wurde die Softwarefirma *Zhengzhou Jinhui Computer System Engineering Ltd.* beauftragt, welche im Oktober 2008 eine erste Testversion veröffentlichte. Die Kosten bis dahin beliefen sich bereits auf 7 Mio. USD. „Grüner Damm“ geriet anschließend schnell in den Fokus von Kritikern, da vom MIIT gefordert wurde, dass diese ab dem 01. Juli 2009 auf jedem in China ausgelieferten Computer vorinstalliert sein müsse.

Abbildung 3.6: Screenshot des Hauptmenüs von „Grüner Damm“.

Daraufhin wurden schnell Bedenken öffentlich, nach welchen die Software auch zu Zensurzwecken genutzt werden könne. Nicht zuletzt auch aufgrund einer hohen Anzahl an Sicherheitslücken manifestierte sich ein erheblicher Widerstand in Form eines offenen Briefes mit 22 Unterschriften namhafter großer Unternehmen weltweit an China. Insbesondere weigerten sich Hewlett-Packard und Dell, „Grüner Damm“ vorzuinstallieren. Am 14. August 2009 wurde daher die Forderung der Vorinstallation relativiert. In der nachfolgenden Zeit stellten sich des Weiteren die Bedenken, dass die Software auch als Zensurwerkzeug benutzt werden könne, als wahr heraus. In der Tat beinhalteten die in „Grüner Damm“ genutzten Blacklists blockierter URLs und Schlagwörter auch politische Begriffe. Nicht zuletzt die darüber hinaus aufgetretenen zahlreichen Qualitätsmängel und Sicherheitslücken der Software führten schließlich dazu, dass das Projekt „Grüner Damm“ seit Juli 2010

de facto eingestellt ist, obwohl noch im März 2010 Initiativen öffentlich wurden, „Grüner Damm“ auch auf Mobiltelefonen vorzuinstallieren [5]. Abbildung 3.6 zeigt einen Screenshot des Hauptprogramms.

3.2 Technische Diskussion

Die prinzipielle Funktionsweise von „Grüner Damm“ ist schnell erklärt: einmal installiert, läuft die Software im Hintergrund und filtert Nutzereingaben sowie Datenverkehr. Bei aktiven Zenszurmaßnahmen werden dabei umfassende Logs angelegt, welche unter Umständen sogar Screenshots vom zensierten Inhalt beinhalten. Die aktuell offene Anwendung wird in diesem Fall geschlossen und eine entsprechende Meldung von „Grüner Damm“ angezeigt. Konfigurierbar ist die Software über ein Master-Passwort. Zum Abgleich verwendete White- und Blacklists erlaubter und vebotener URLs, sowie verbotener Wörter werden automatisch geupdatet. Offiziell soll „Grüner Damm“ unter Windows 98 und neuer lauffähig sein.

Im Folgenden soll näher auf die eingesetzten Filter eingegangen werden. Zum einen benutzt „Grüner Damm“ einen Bildfilter, welcher mithilfe von Computer-Vision-Technologien Bilder mit vielen Hauttönen heraus filtert. Ausgenommen davon sollen Nahaufnahmen von menschlichen Köpfen sein. Zur technischen Umsetzung wurden Teile der Open Source Software OpenCV implementiert. Als zweites kommen Textfilter zum Einsatz. Diese filtern eingegebenen Text und gleichen diesen mit Black- und Whitelists ab. Sofern ein Begriff in einer Blacklist auftaucht, wird die Anwendung geschlossen. Für die Filterung des Internetverkehrs werden URL-Filter eingesetzt. Durch das Einschleusen einer speziellen DLL (`SurfGd.dll`) in die Windows Socket API wird das Abhöhren der Internetverbindung ermöglicht. Auch hier erfolgt ein Abgleich mit den White- und Blacklists. Diese sind u. a. in den folgenden Dateien enthalten: `xwordl.dat`, `xwordm.dat`, `xwordh.dat`, `FalunWord.lib`, `*fil.dat`, `adwapp.dat` und `TrustUrl.dat`; vgl. auch [4].

3.3 Sicherheitprobleme und Bugs

Aufgrund der teils sehr simplen und plagiierten Implementierung existiert eine Reihe bekannter Sicherheitsprobleme und Bugs. Insbesondere ergeben sich nicht zuletzt auch rechtliche Bedenken, da teilweise Code und andere Daten unrechtmäßig verwendet wurden. Der folgende Abschnitt beschäftigt sich vorerst mit Bugs in der Software selbst.

Der geschilderte Bildfilter filtert Bilder mit realtiv großen Flächen an Hauttönen. Allerdings konnte leicht festgestellt werden, dass die implementierten Filter viele falschpostive und falsch-negative Ergebnisse lieferten [21]. Ein Beispiel für ein Bild, welches unter Umständen fälschlicherweise gefiltert würde, ist in Abbildung 3.7 zu sehen. Aufgrund der hohen Anzahl an Hauttönen ist es wahrscheinlich, dass dieses Bild als pornographisches Material erkannt und gesperrt würde.

Hinzu kommen zahlreiche Sicherheitslücken in der Software selbst. Zum einen erzeu-

Abbildung 3.7: Bild mit vielen Hauttönen, [17].

gen bestimmte URLs einen Buffer-Overflow [4], welcher wiederum Manipulationen des Execution-Stacks zulässt. Zum anderen treten analoge Probleme auch beim Einlesen der Black- und Whitelists auf. Das Master-Passwort, welches benutzt wird, um die Software nur für autorisierte Personen einstellbar zu machen, ist wiederum in einer als DLL-Datei getarnten Textdatei unter `C\Windows\System32\kwpwf.dll` als simpler MD5-Hash abgelegt; eine Manipulation fällt entsprechend einfach. Hinzu kommt schließlich, dass auch die Black- und Whitelistdateien mit einem einfachen (schlüssellosen) Verschlüsselungsverfahren verschlüsselt sind. Eine Manipulation fällt dementsprechend auch hier sehr einfach. Detaillierte Beschreibungen können auch [4] entnommen werden. Schließlich besitzt „Grüner Damm“ kaum Kompatibilität zu verschiedenen Betriebssystemen oder Browsern. Konkret ist sie nur unter Windows 98 und neuer lauffähig, allerdings nur auf x86 Architekturen [18]; andere Betriebssyteme sind ausgeschlossen. Zur Filterung des Internetverkehrs eignen sich des Weiteren ebenfalls nur Microsofts Internet Explorer und Googles Chrome; Firefox wird nicht unterstützt [19].

Aufgrund der zahlreichen Sicherheitslücken wurde die Software, wie bereits geschildert, im Juli 2010 eingestellt. Hinzu kamen noch weitere Lizenzverletzungen. So wurde für die Bildverarbeitung Code von der OpenSource Software OpenCV ohne Genehmigung verwendet. Zudem enthalten die Black- und Whitelists Teile der Content-Filter Software *CyberSitter*. Im vorherigen Abschnitt wurde zudem erwähnt, dass die Verschlüsselung der Black- und Whitelisdateien recht einfach ist. Daher verwundert es nicht, dass diese recht schnell nach Veröffentlichung von „Grüner Damm“ gehackt wurden. Heraus kam, dass lediglich ca. 30% der enthaltenen URLs und Wörter unpolitisch waren. Die Bedenken der Kritiker, die Software könne zu Zensurzwecken missbraucht werden, war also berechtigt.

4. Fazit

Wie die vorliegende Ausarbeitung aufzeigt, wird in China aktiv und in großem Ausmaß im Rahmen des Projektes „Goldener Schild“ Zensur des Internetverkehrs betrieben. Die besprochenen Zensurmaßnahmen dienen dabei nicht nur der Zensur von rechtswidrigem Inhalt und Pornographie, sondern zensieren insbesondere auch politische Inhalte, wie etwa Webseiten zu Taiwan, Tiananmen und Tibet, sowohl als auch Webseiten, welche der Informationsverbreitung dienen (z. B. Youtube, Wikipedia oder diverse Nachrichtenseiten westlicher Zeitschriften), siehe Abschnitt 2.4. Wie die geschichtliche Entwicklung zeigt, waren und sind am Aufbau dieses Projektes vor allem auch westliche Unternehmen beteiligt. Somit stellt sich in diesem Kontext die Frage, inwieweit der Westen an dem Erfolg des Projektes „Goldener Schild“ seit seiner Initiierung 1998 wesentlichen Beitrag geleistet hat, vgl. Abschnitt 2.5. Wie in Abschnitt 2.3 dargelegt wurde, ist es zwar möglich, die technischen Maßnahmen zur Zensur (wie z. B. Paket-, IP- und DNS-Filter) zu umgehen, jedoch stellte keine der vorgestellten Lösungen eine vollständig zufriedenstellende Lösung dar. So war es zwar möglich, mithilfe verschiedener Maßnahmen zensierte Inhalte abzurufen, jedoch hatte jede vorgestellte Lösung ihre eigenen Nachteile, wie z. B. geringere Übertragungsgeschwindigkeit, nur partiell abrufbare Inhalte oder hoher Umgehungsaufwand.

Zusammenfassend lässt sich also feststellen, dass es in China de facto seit 2006 eine massive und nicht vergleichbare Zensur des Internets gibt. Die Zensur schränkt dabei die Informationsfreiheit der chinesischen Bevölkerung in großem und nicht zu vertretendem Maße ein. Starke Kritik aus dem Westen gibt es etwa durch „Amnesty International“ oder „Reporter ohne Grenzen“, jedoch konnte keine dieser Proteste bisher dazu beitragen, dass die Zensur des chinesischen Internets vermindert wird. Einzig Wirkung zeigen können hier wohl nur Proteste seitens westlicher Unternehmen, welche jedoch aus wirtschaftlichen Gründen Lieferungen ihrer Netzwerkprodukte nach China nicht einschränken werden. Nicht zuletzt haben die Recherchen zu diesem Seminarvortrag gezeigt, dass es generell auch an wissenschaftlicher Auseinandersetzung mit diesem Thema fehlt.

Ein durchaus positives Beispiel, was Proteste seitens des Westens bewirken können, ist das in dieser Arbeit ebenfalls vorgestellte Softwareprojekt „Grüner Damm“. Seine Entwicklung zielte offiziell und ursprünglich auf den Schutz der chinesischen Jugend vor kriminellen und pornographischen Inhalten ab. Als Contentfilter-Software entwickelt, stellte sich aber leider zeitnah nach der Veröffentlichung im Oktober 2008 heraus, dass gefilterte Inhalte erneut auch politischer Natur waren. Neben zahlreichen Sicherheitsproblemen der Software selbst und plagiierten Inhalten war nicht zuletzt auch der massive Widerstand westlicher Unternehmen nach Bekanntwerden der Forderung im Juli 2009, „Grüner Damm“ müsse auf jedem in China ausgelieferten Rechner vorinstalliert werden, dafür verantwortlich, dass das Projekt seit Juli 2010 de facto eingestellt ist: Die breite Ablehnung und zahlreiche ju-

ristische Verfahren zusammen mit der mangelhaft programmierten Software führten dazu, dass „Grüner Damm“ nicht weiter finanziert und somit letztlich eingestellt wurde.

Das Softwareprojekt „Grüner Damm“ ist somit als weiterer Versuch der chinesischen Regierung zu interpretieren, ihre Bürger zu überwachen und abrufbare Internetinhalte zu zensieren. Letztlich scheiterte dieses Projekt mehr oder weniger nur an seiner mangelhaften Umsetzung.

Literaturverzeichnis

[1] J. Zittrain and B. Edelman. Empirical Analysis of Internet Filtering in China. Technical Report, URL: *http://cyber.law.harvard.edu/filtering/china/*, März 2003. Abgerufen: 24.03.2011.

[2] R. Clayton, S. J. Murdoch, and R. N. M. Watson. Ignoring the great firewall of china. *Lecture Notes in Computer Science*, 4258:20-35, 2006. Abgerufen am: 24.03.2011.

[3] G. Walton. China's Golden Shield. Technical Report, URL: *http://www.dd-rd.ca/site/_PDF/publications/globalization/CGS_ENG.PDF*, Oktober 2001.

[4] S. Wolchok, R. Yao, and J. A. Halderman. Analysis of the Green Dam Censorware System. Technical Report, URL: *http://www.cse.umich.edu/~jhalderm/pub/gd/*, Juni 2009. Abgerufen am: 24.03.2011.

[5] Lindsey Ma. Green Dam Goes Mobile? OpenNet Initiative, URL: *http://opennet.net/blog/2010/03/green-dam-goes-mobile*. Abgerufen am: 24.03.2011.

[6] Monika Ermert. Kein Anschluss unter dieser Mailbox. Heise Online, URL: *http://heise.de/-301388*. Abgerufen am: 24.03.2011.

[7] Michael Metzger. Web 0.0 in China. ZEIT ONLINE, URL: *http://www.zeit.de/online/2009/23/web2.0-china-zensur/*. Abgerufen am: 24.03.2011.

[8] H. Schmundt und W. Wagner. Chinesische Mauer 2.0. *Der Spiegel*, Ausgabe 18/2008.

[9] Epoch Times. URL: *http://www.epochtimes.com/gb/3/10/22/n397830p.htm*. Abgerufen am: 24.03.2011. Übersetzt mit *http://translate.google.de*.

[10] J. L. Qiu. Virtual Censorship in China. Keeping the Gate Between the Cyberspaces. *International Journal of Communications Law and Policy*, 4, 1999, DOI: 10.1.1.106.532.

[11] S. Guan. Intercultural communication. *Beijing University Press*, 1995.

[12] Hu Weiwei. The Internet Timeline of China 1987-1996. CNNIC, URL: *http://english.cri.cn/6826/2009/03/19/1601s466124.htm*. Abgerufen am: 24.03.2011.

[13] Amnesty International. What is internet censorship? URL: *http://www.amnesty.org.au/china/comments/10926/*, 2008. Abgerufen am: 24.03.2011.

[14] J. Kubieziel. Eine Zensur findet statt. URL: *http://events.ccc.de/congress/2009/*. Abgerufen am: 24.03.2011.

[15] Benjamin Beckmann. Google erhält China-Lizenz durch Kompromiss. Computerbase, URL: *http://www.computerbase.de/news/internet/webdienste/2010/juli/google-erhaelt-china-lizenz-durch-kompromiss/*. Abgerufen am: 24.03.2011.

[16] Human Rights In China. Chinese Government Orders Computer Manufacturers to Pre-install Filtering Software. URL: *http://www.hrichina.org/public/contents/169820*. Abgerufen am: 24.03.2011.

[17] Wikipedia. URL: *http://en.wikipedia.org/w/index.php?title=Green_Dam_Youth_Escort&oldid=411722368*. Abgerufen am: 24.03.2011.

[18] Jonathan Fildes. China's computers at hacking risk. BBC News, URL: *http://news.bbc.co.uk/2/hi/technology/8094026.stm*. Abgerufen am: 24.03.2011.

[19] Radio Free Asia. Chinese Slam 'Compulsory' Filters. URL: *http://www.rfa.org/english/news/china/china-internet-filtering-06102009095405.html*.

Abgerufen am: 24.03.2011.

[20] FAZ.NET. Journalist mit Unterstützung von Yahoo verhaftet. URL: *http://www.faz.net/-00ost2*. Abgerufen am: 24.03.2011.

[21] H. Ben and G. Shipeng. Doraemon passes, Garfield filtered-controversies over „Green Dam Youth Escort". Southern Weekly, URL: *http://www.infzm.com/content/29902*. Abgerufen am: 24.03.2011. Übersetzt mit *http://translate.google.de*.