Filterung und ~~Zensur~~ im Internet

Möglichkeiten, Wirkungsweise und wie man sie umgehen kann

Manuel Mausz

Inhalt (1)

- EINLEITUNG
- METHODEN
  - Port- und IP-Sperre
  - DNS-Manipulation
  - Proxy-Server
  - Schlüsselwort-Filterung

Inhalt (2)

- THE GREAT FIREWALL OF CHINA
  - Technische Wirkungsweise
  - Umgehung
  - ChinaNet Next Carrying Network
  - Weitere Maßnahmen Chinas
- DISKUSSION

Einleitung

Informationsbeschaffung

- ohne Internet, lokal
  - TV, Radio, Zeitung, Mund-zu-Mund, Telefon
  - Zensur möglich
- im Internet
  - Internet-Radio, -TV, -Zeitung
  - Blogs, Foren, Chat, soziale Netzwerke, u.v.m.
  - Zensur schwer möglich

➡ Warum?

Einleitung

Aufbau des Internet

- dezentralistischer Aufbau
- verschiedene Protokolle
- sehr hohe Datenmenge an großen Knotenpunkte
  - AMS-IX: ~250 Gb/s
  - DE-CIX: ~200 Gb/s
  - VIX (Uni Wien): ~10 Gb/s

Methoden

Port- und IP-Sperre

- Basis: IP-Protokoll
- Filterung auf Router- bzw. Switch-Ebene
- Vorteile
  - sehr kostengünstig
  - in Echtzeit
- Nachteile
  - sperrt ganze Bereiche, unter Umständen mehrere/viele Webseiten (Bsp: GoDaddy)
  - Proxy-Server, TOR

Methoden

DNS-Manipulation

- Basis: DNS-Protokoll
- Verfälschung („Sperre“) am DNS-Server
- Vorteile
  - kostengünstig
  - Effekt nur auf einzelne Domains
- Nachteile
  - grundsätzlich umgehbar
  - freie DNS-Server
  - Proxy-Server, TOR

Methoden

Proxy-Server

- Basis: je nach Proxy-Typ
- Proxy-Server kommuniziert anstelle des Absenders
- Filterung geschieht am Proxy-Server
- Vorteile
  - Filterung einfach möglich
- Nachteile
  - nicht für hohe Datenmengen / viele Benutzer geeignet
- im Einsatz: Süd-Arabien, Burma

Methoden

Schlüsselwort Filterung

- einzelne Protokoll-Fragmente werden analysiert
- Fehlermeldung kann zugestellt werden

- HTTP-Protokoll: z.B. URL
- Suchmaschine: z.B. Suchresultat
  - u.a. Google, Yahoo!, MSN in China

The Great Firewall of China

Internet-Zensur in China

- seit Mitte der 90er-Jahre
- IP-Blockade
- DNS-Manipulation
- Schlüsselwort-Filterung
  - seit Ende 2004
  - analysiert den gesamten HTTP-Verkehr
  - bekannt als GCF

Technische Wirkungsweise

TCP-Paket Aufzeichnung

Kommunikationspartner

```
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
```

HTTP-GET

3x RST

angeforderte Website + weitere RST

Technische Wirkungsweise

TCP-Paket Aufzeichnung

Kommunikationspartner

```
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
```

verschiedener Ursprung

RST
#1: seq vom GET
#2: #1 + 1460
#3: #1 + 3*1460

The Great Firewall of China

Technische Wirkungsweise

- analysiert den gesamten HTTP-Verkehr
- sendet 3 RST-Pakete mit unterschiedlichen Sequenznummern an Absender und Empfänger
- TTL-Werte der RST-Pakete unterschiedlich

- Tageszeitabhängige Filter-Effektivität (-25%)
- Filterung an zentralen Kontenpunkten

The Great Firewall of China

Umgehung

- Ignorieren der RST-Pakete auf beiden Seiten (iptables)

Weitere Wirkungsweise

- temporäre Blockade (~20 min)
- mittels RST- und gefälschten SYN+ACK-Paketen

The Great Firewall of China

Umgehung (2)

- Ignorieren der RST-Pakete auf beiden Seiten (iptables)
- Ignorieren der SYN+ACK-Pakete anhand unüblichen TCP-Flags
- einfacher: Verstecken
  - HTML-Kommentare (`Fa<!-- comment -->lun`)
  - URL-Encoding

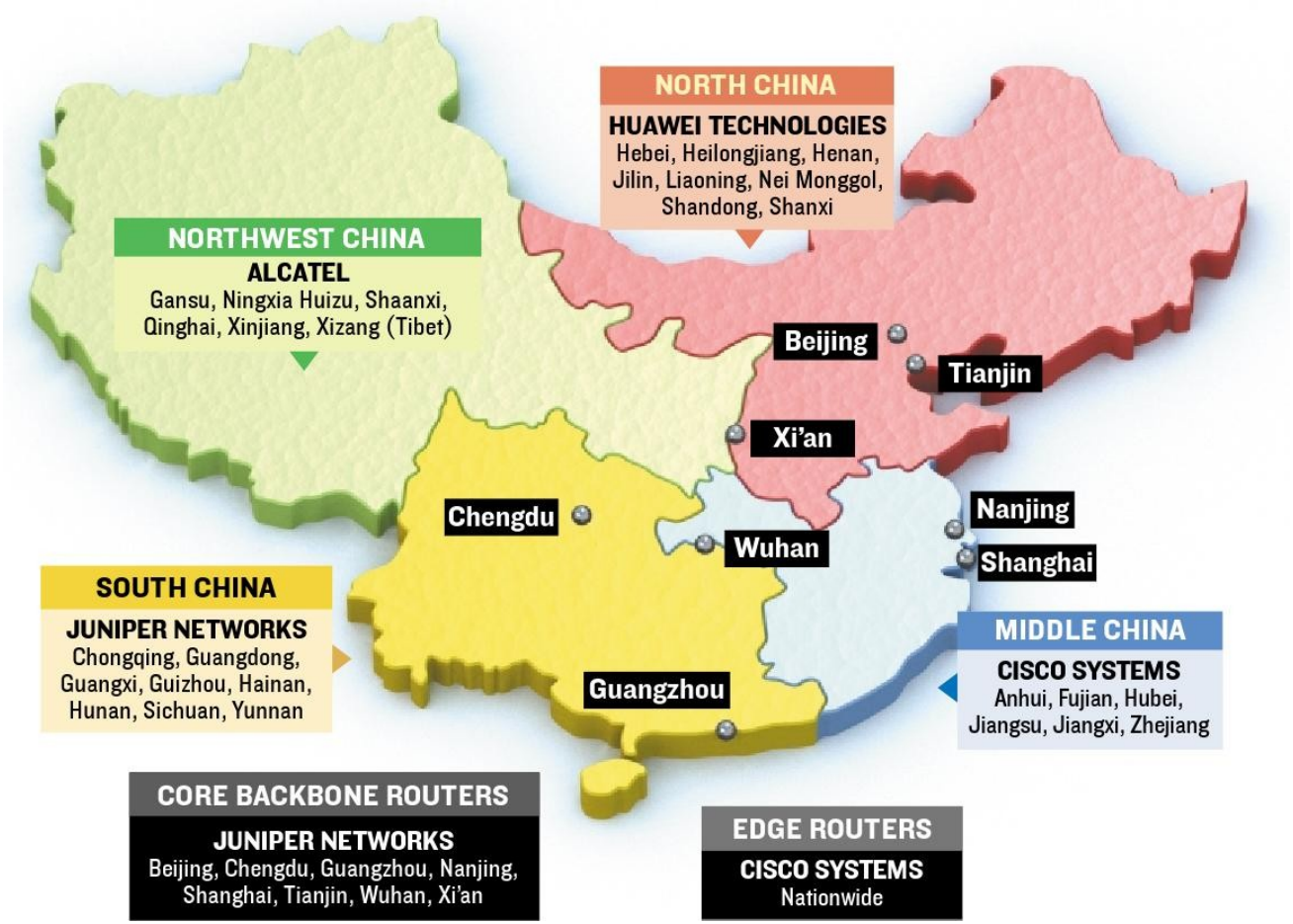
The Great Firewall of China

ChinaNet Next Carrying Network (China Telecom)

- Infrastruktur datiert auf 1993 zurück
- erst 16% der Bevölkerung online
- nicht für „Breitband“-Services (VOIP, Video, etc.) geeignet

➞ neues Netz

ChinaNet Next Carrying Network



höchst zentralistischer Aufbau!

The Great Firewall of China

weitere Maßnahmen

- 30 000 bis 50 000 „Internet Cops“
- staatliche Lizenz für ISP und Internet Cafés
- Verpflichtung zur Analyse aller Datenpakete

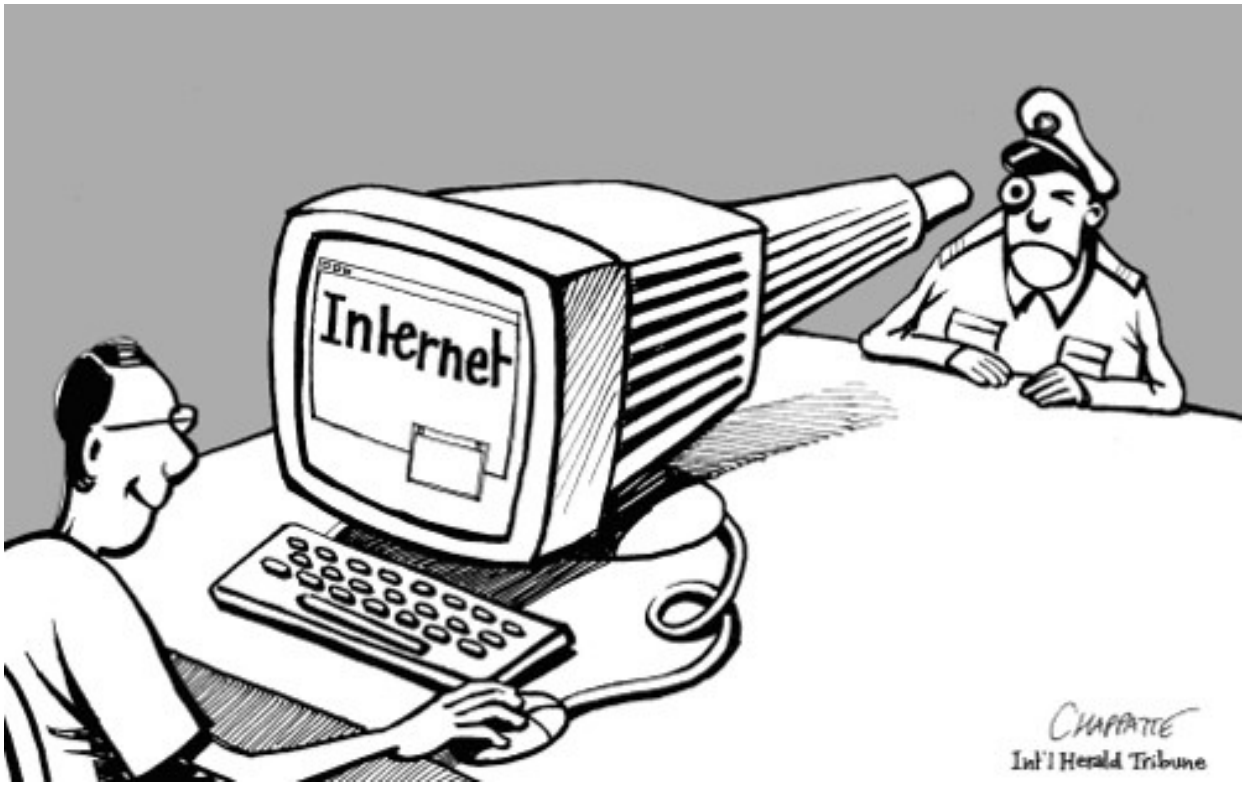
- phonetisch ähnliche Wörter ebenfalls gesperrt
- Zensur bei Suchmaschinen (auch westliche)

Diskussion

- Internet-Zensur auch in westlichen Ländern
  - Italien: online Glücksspiele
  - Arcor: youporn.com
- Aufbau wird immer zentralistischer
- Know-How von China erwerben?

- Hardware derzeit nicht leistungsstark genug
- kann dieser Zeitpunkt erreicht werden?

Filterung und ~~Zensur~~ im Internet



Vielen Dank für Ihre Aufmerksamkeit!