1 Censorship (& Privacy)

1.1 Einführung in Internetzensur

Internetzensur beschränkt, welche Informationen im Internet veröffentlicht oder abgerufen werden können. Sie wird von Regierungen und Organisationen eingesetzt.

Ziele der Zensur

- **Schutz von Rechten:** Blockierung urheberrechtlich geschützter Inhalte.
- **Sicherheit:** Schutz vor schädlichen oder sensiblen Inhalten (z. B. Malware, illegale Pornografie).
- **Politische Kontrolle:** Einsatz als Propagandamethode zur Förderung spezifischer religiöser oder politischer Agenden.

Die Umsetzung erfolgt in vier Hauptkategorien:

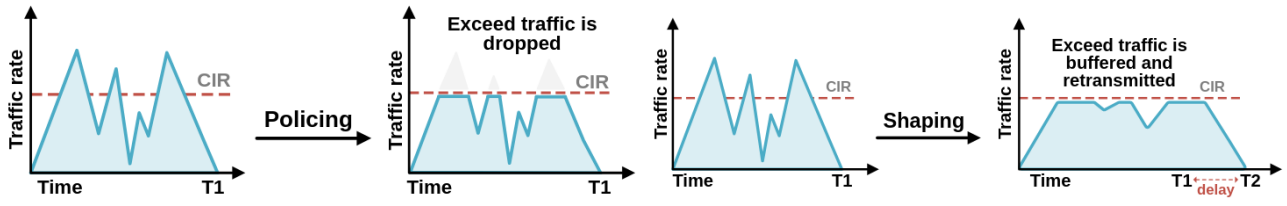
1. **Drosselung (Throttling):** Verlangsamung des Datenverkehrs.
2. **Blockierung:** Verhindern des Zugriffs auf spezifische Ressourcen.
3. **Entfernung:** Löschung von Inhalten an der Quelle.
4. **Abschaltung:** Vollständiges Kappen des Internets (Internet Shutdown).

1.2 Drosselung des Datenverkehrs (Throttling)

Die Drosselung reduziert die Bandbreite für spezifischen Netzwerkverkehr. Sie ist diskreter als eine vollständige Blockierung und oft schwerer als absichtliche Zensur zu erkennen (könnte wie eine schlechte Verbindung wirken). Sie kann geografisch oder anwendungsbasiert (z. B. Verlangsamung von YouTube) erfolgen.

Es gibt zwei technische Hauptmethoden zur Durchsetzung von Ratenlimits:

- **Traffic Shaping**: Hierbei werden Pakete, die das Ratenlimit überschreiten, **verzögert**. Sie werden in einem Puffer zwischengespeichert und später gesendet. Dies glättet den Datenstrom, verursacht aber Latenz.
- **Traffic Policing**: Hierbei werden Pakete, die das Ratenlimit überschreiten, rigoros **verworfen** (dropped). Dies führt zu Paketverlusten und zwingt das TCP-Protokoll, die Übertragungsrate drastisch zu senken.



1.3 Blockierung von Verbindungen

Behörden nutzen verschiedene Techniken, um den Zugriff auf Ressourcen zu unterbinden:

1.3.1 Domain-Entfernung

Behörden zwingen Registrare oder Nameserver, Domains aus ihren Verzeichnissen zu löschen. Die Seite existiert technisch noch, ist aber über ihren Namen nicht mehr auffindbar.

1.3.2 DNS-Manipulation

Da Browser IP-Adressen benötigen, ist das Domain Name System (DNS) ein häufiger Angriffspunkt.

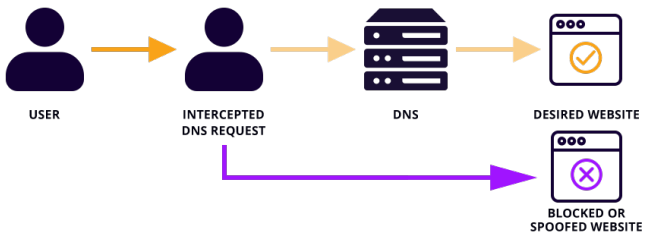


Figure 1: *Injection*

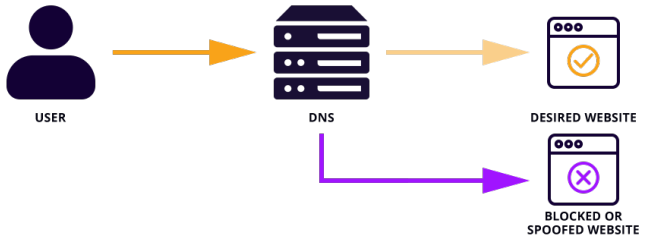


Figure 2: *Filtering*

- **DNS Injection (via Man-on-the-Side):** Dies ist eine Variante des *Man-on-the-Side* (MotS) Angriffs.
  1. Der Zensor liest den Verkehr mit, befindet sich aber nicht zwingend direkt im Pfad ("on-path").
  2. Erkennt der Zensor eine DNS-Anfrage für eine verbotene Domain, sendet er sofort eine gefälschte Antwort (Spoofed Response) mit einer falschen IP-Adresse zurück.
  3. *Race Condition:* Da die gefälschte Antwort meist schneller beim Client ankommt als die legitime Antwort des echten DNS-Servers, akzeptiert der Client die falsche IP. Die echte Antwort wird später verworfen.
- **DNS Filtering:** Hier steht der DNS-Server selbst unter der Kontrolle des Zensors (z. B. beim ISP). Er liefert direkt die falsche IP-Adresse oder einen Fehlercode (NXDOMAIN) zurück. Keine Race Condition erforderlich.

1.3.3 Man-on-the-Side (MotS) für HTTP

Ablauf eines MotS-Angriffs

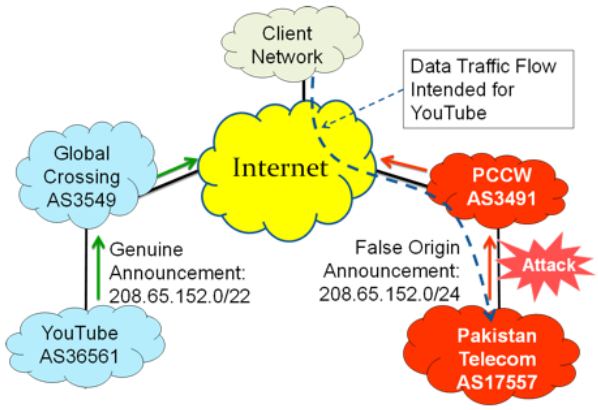
1. Client sendet legitime HTTP-Anfrage (GET)
2. Zensor (liest mit) erkennt verbotenen Inhalt/
3. Zensor injiziert ein TCP-RST (Reset) Paket
   käme es vom Server.
4. Der Client bricht die Verbindung ab oder wir
5. Die echte Antwort des Webservers kommt zu

MotS kann auch für direkte Webzugriffe genutzt werden, nicht nur für DNS.

1.3.4 BGP Hijacking

Das Border Gateway Protocol (BGP) steuert das Routing im Internet. Behörden können den Verkehr für bestimmte IP-Präfixe umleiten oder in ein "schwarzes Loch" führen.

Beispiel Pakistan/YouTube (2008): Pakistan Telecom wollte YouTube (IP-Bereich z. B. `208.65.152.0/22`) blockieren. Sie kündigten jedoch versehentlich eine spezifischere Route an (`208.65.152.0/24`). *Erklärung:* Im Internet-Routing gewinnt immer die spezifischere Route ("Longest Prefix Match"). Da `/24` genauer ist als `/22`, leitete das gesamte Internet den YouTube-Verkehr nach Pakistan, wo er verworfen wurde. Dies führte zu einem weltweiten YouTube-Ausfall.



1.3.5 IP-Blocking

Direktes Blockieren von IP-Adressen durch Firewalls beim ISP oder auf dem Endgerät.

- **Problem:** Viele Websites teilen sich dieselbe IP-Adresse (z. B. durch CDNs wie Cloudflare oder Virtual Hosting). IP-Blocking führt oft zu *Overblocking*, bei dem auch unschuldige Dienste blockiert werden.

1.4 Entfernung von Inhalten

Anstatt den Zugang zu blockieren, fordern Regierungen Plattformen (wie Google, Facebook) auf, Inhalte zu löschen.

- **Gründe:** Nationale Sicherheit, Urheberrecht, Privatsphäre, Diffamierung.
- **Requesters:** Gerichte (Judicial), Exekutive, Polizei.
- **Trend:** Die Anzahl der Anfragen steigt weltweit kontinuierlich an (siehe Google Transparency Reports).

1.5 Zensur-Werkzeuge und Technologien

1.5.1 Deep Packet Inspection (DPI)

DPI ist eine fortgeschrittene Methode zur Filterung, die nicht nur den Header (IP/Port), sondern auch den **Payload** (Inhalt) des Pakets analysiert. DPI-Systeme befinden sich meist direkt im Datenpfad ("on-path").

Funktionsweise von DPI

- Sucht nach Signaturen, Mustern und Schlüsselwörtern.
- Kann Protokolle identifizieren, auch wenn sie nicht auf Standard-Ports laufen.
- Ermöglicht granulare Steuerung (z. B. "Skype blockieren, aber HTTPS erlauben").

DPI und Verschlüsselung (TLS/SSL): DPI kann verschlüsselte Inhalte (Payload) ohne den privaten Schlüssel nicht lesen. Dennoch ist eine Zensur möglich durch:

- **SNI (Server Name Indication):** Der angefragte Hostname wird im TLS-Handshake oft unverschlüsselt übertragen (Client Hello).
- **Metadaten-Analyse:** Timing, Paketgrößen und Flow-Statistiken verraten oft die Art der Anwendung.
- **Fingerprinting (z. B. JA4+):** Analyse der TLS-Handshake-Parameter (Cipher Suites, Extensions), um den verwendeten Client (z. B. Tor-Browser vs. Chrome) zu identifizieren.

Nachteile von DPI: Rechenintensiv, zeitaufwendig (Latenz), fehleranfällig bei unbekannten Angriffsmustern.

1.5.2 Zwangsfilterung (Mandatory Filtering)

Dies bezieht sich auf gesetzlich oder technisch erzwungene Filtermaßnahmen:

- **Infrastruktur:** Filterung durch ISPs oder DNS-Server.
- **Geräte:** Vorinstallierte Software (Spyware/Filter) auf Smartphones/PCs.
- **Anwendungen:** "SafeSearch"-Zwang in Suchmaschinen.
- **EU-Regulierung:**
  - *Urheberrechtsrichtlinie (Art. 17):* Plattformen müssen proaktiv Copyright-Verstöße verhindern (Upload-Filter).
  - *Digital Services Act (DSA):* Reguliert illegale Inhalte und Transparenz auf Online-Plattformen.

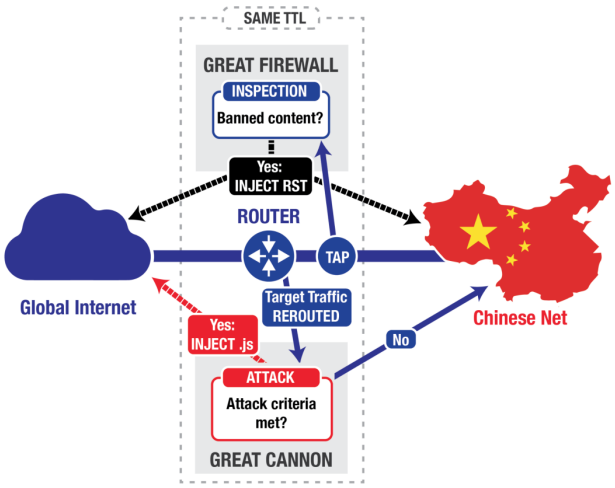
1.6 Fallstudie: China

China betreibt das weltweit komplexeste Zensursystem.

1.6.1 Great Firewall of China (GFW)

Das primäre **defensive** System. Es kontrolliert den Datenverkehr an den Internet-Gateways zwischen China und der Welt.

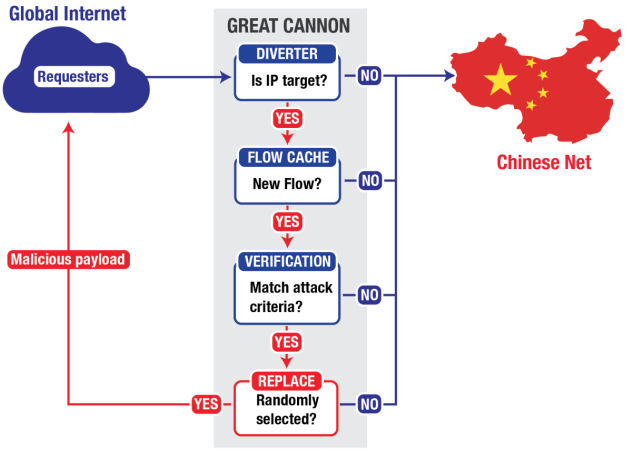
- **Methoden:** DNS Hijacking, IP Blocking, Keyword Filtering, RST-Injection (Abbruch von TCP-Verbindungen bei Erkennung verbotener Muster).
- **Anti-Umgehung:** Die GFW nutzt Machine Learning und "Active Probing" (aktives Verbinden zu verdächtigen Servern), um VPN- und Tor-Server zu erkennen und zu blockieren.



1.6.2 Great Cannon (GC)

Ein **offensives** Werkzeug, das sich von der GFW unterscheidet.

- **Funktion:** Man-in-the-Middle (MitM) Angriffssystem.
- **Vorgehensweise:** Es fängt den Datenverkehr unbeteiligter Nutzer ab, die chinesische Webseiten (z. B. Baidu) aufrufen. Es injiziert bösartigen JavaScript-Code in die Antworten dieser legitimen Seiten.
- **Ziel:** Der Browser des unschuldigen Nutzers führt das Skript aus und nimmt (ohne Wissen des Nutzers) an einem DDoS-Angriff gegen Zensurgegner teil (z. B. Angriff auf GitHub 2015).


Global Internet
Requesters
GREAT CANNON
DIVERTER
Is IP target?
NO
YES
FLOW CACHE
New Flow?
NO
YES
VERIFICATION
Match attack criteria?
NO
YES
REPLACE
Randomly selected?
NO
YES
Malicious payload
Chinese Net