Internetsperren

#zensursula and beyond

Christian Rüdiger Bahls; MOGiS
vortrag-26c3@mogis-verein.de

26C3, Berlin 27. Dezember 2009

Kurze Übersicht über den Talk

1. Past, Present & Future
   - Welche Rolle hat das BKA?
   - Die Sperrdisskussion
   - In der Schwebe ..
   - Ein Blick zum Horizont ..
2. A Todo
   - Politik
   - Gesellschaft
   - Begrifflichkeiten
3. Technik
   - DNS via HTTP(S)
   - Verteilte Infrastrukturen

Das BKA und der Herr Ziercke

- Vorbereitung zur Durchsetzung der Sperren müssen sehr früh begonnen haben.
- Wichtigstes Ereignis in diesem Zusammenhang ist die Bekanntgabe der Operation Himmel zu Weihnachten 2007
  Spon: Riesiger Kinderporno-Skandal schockiert Deutschland
- Operation lief seit mindestens April 2007 – Der Server wurde den Ermittlern schon im Mai 2006 mitgeteilt
  Heise: Wie erfolgreich war die Operation „Himmel“?
- Server wurde also über Monate weiterbetrieben um Verdächtige (Besitz und Besitzverschaffung) zu ermitteln.
- Weltweit 92.000 Anschlussinhaber ermittelt (12.000 in DE).
- Staatsanwaltschaften haben viele Verfahren eingestellt, nur ganz wenige Verfahren überhaupt mit Strafbefehl oder Verurteilung abgeschlossen.

Das BKA und der Herr Ziercke #2

- Im Mai 2008 erschien dann die polizeiliche Kriminalstatistik für das Jahr 2007.⇒ PKS 2007 - Gesamtausgabe
- Sie zeigte eine Steigerungsrate von 94.3% für Verfahren den Besitz bzw die Besitzverschaffung kinderpornographischer Schriften betreffend.
- Aus dieser Steigerungsrate wurde dann mittels eines 'Patches' die häufig erwähnten 111% Steigerungsrate.
  ⇒ Die Argumente fuer Sperren laufen ins Leere (Heise)
- Am 27.8.2008 im Rahmen einer Pressekonferenz zur organisierten Kriminalität ging dann Herr Ziercke mit seiner Forderung nach einer gesetztlichen Verpflichtung der Provider zur Sperrung von Webseiten in die Öffentlichkeit:
  ⇒ http://tinyurl.com/zierckefordertsperren

Die Sperrdiskussion

- Im Rahmen der Rio-Konferenz zum "Schutz vor Sexueller Gewalt" bringt Familienministerin Ursula von der Leyen die Sperrung von Webseiten ins Gespräch
  Abendblatt 19.11.2008: „Kinderseelen werden zerfetzt"
- Frau von der Leyen (später häufig als #zensursula abgekürzt) tritt danach sehr offensiv in der Öffentlichkeit auf.
- So führt sie auf Treffen mit Providern oder auch auf Pressekonferenzen die Dokumentation sexuellen Kindesmissbrauchs (Kinderpornographie) vor.
- Nach Protest von Providern wird die Arbeitsgruppe des Bundesfamilienministeriums ergebnislos aufgelöst (04.03.2009)
- Am 05. März 2009 wird die Immunität des (damaligen) SPD-Abgeordneten Tauss aufgehoben. Seine Wohnungen und sein Büro werden durchsucht. Die Presse berichtet "zeitnah"

Die Sperrdiskussion #2

- 17.04.2009 – Unter großen Druck der Politik und begleitet von der „Sperrwache“ unterzeichnen fünf Provider die Verträge.
- 04.05.2009 – Franziska Heine's Online-Petition „Internet - Keine Indizierung und Sperrung von Internetseiten“ beginnt
- 16.05.2009 – Umfrage Infratest dimap für die DKH: Welt: 92 Prozent der Deutschen für Sperrungen im Internet
- 20.05.2009 – Umfrage Infratest dimap für MOGiS: Zeit: Mehr als 90 Prozent gegen Sperrungen im Internet
- 27.05.2009 – Hintergrundgespräche mit der SPD (Franziska Heine, AK Zensur, CCC, MOGiS, u.v.a.m.)
- 14.06.2009 – SPD-Bundesparteitag bestätigt trotz eines Initiativantrags die Linie „Löschen **vor** Sperren“
- 17.06.2009 – Ende der Petition mit 134015 Mitzeichnern
- 18.06.2009 – Bundestag beschließt das, in der 2. und 3. Lesung neu eingebrachte, Zugangserschwerungsgesetz

Status quo

- Das Gesetz liegt bekanntlich beim Bundespräsidenten.
- Dieser wünscht von der Bundesregierung weitergehende Informationen.
- Es besteht die Chance, dass das Gesetz nicht ausgefertig wird.
- Im Zuge der Koalitionsverhandlungen zwischen FDP und CDU/CSU hat das BMI hat das BKA aufgefordert keine Listen zu erstellen oder zu verbreiten.
- Stattdessen soll das BKA für ein Jahr diese Inhalte verfolgen.
- Am Ende dieses Jahres soll das „Löschen“ evaliert werden.

Status quo #2

- **Aber:** Die Verträge gelten weiterhin.
- Die Provider sind also noch immer vertraglich verpflichtet zu sperren, sobald das BKA die Listen herausgibt.
- Die Infrastruktur besteht also bereits, sie funktioniert wohl auch. (Merkzettel: Beim nächsten Mal auf die Vergabe an einen deutschen Dienstleister, wie z.B. T-Systems bestehen)
- Der Innenminister des Landes Niedersachsens Herr Schünemann hat White IT, als Bündnis zum Kampf gegen den sexuellen Missbrauch von Kindern ins Leben gerufen.
- Das Hasso-Plattner-Institut der Uni Potsdam (Filter-Software) und Microsoft (Digital DNA) sind auch dabei.

Zum Thema „White It“

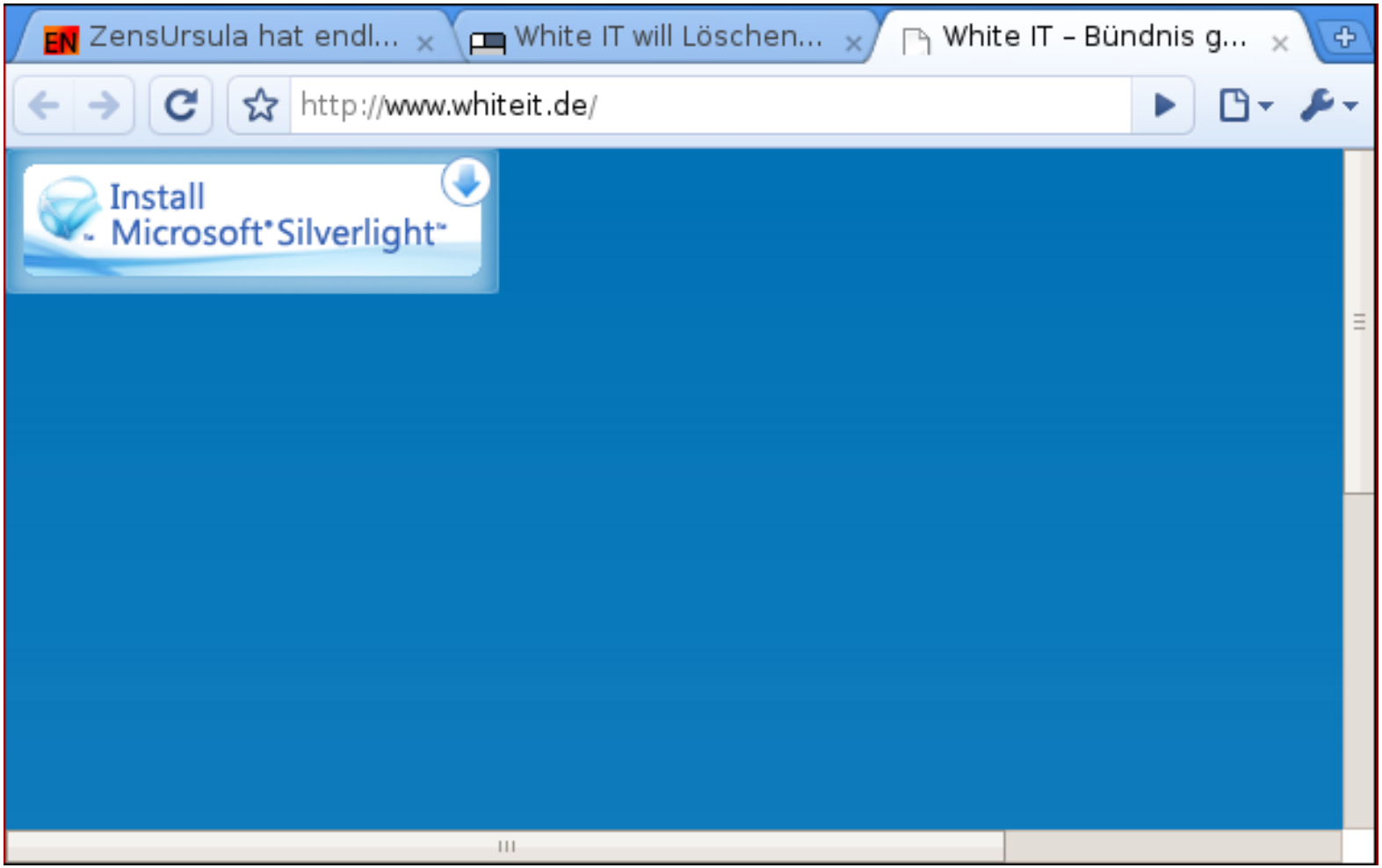


Abbildung: „White It“

Zum Thema „White It“ #2

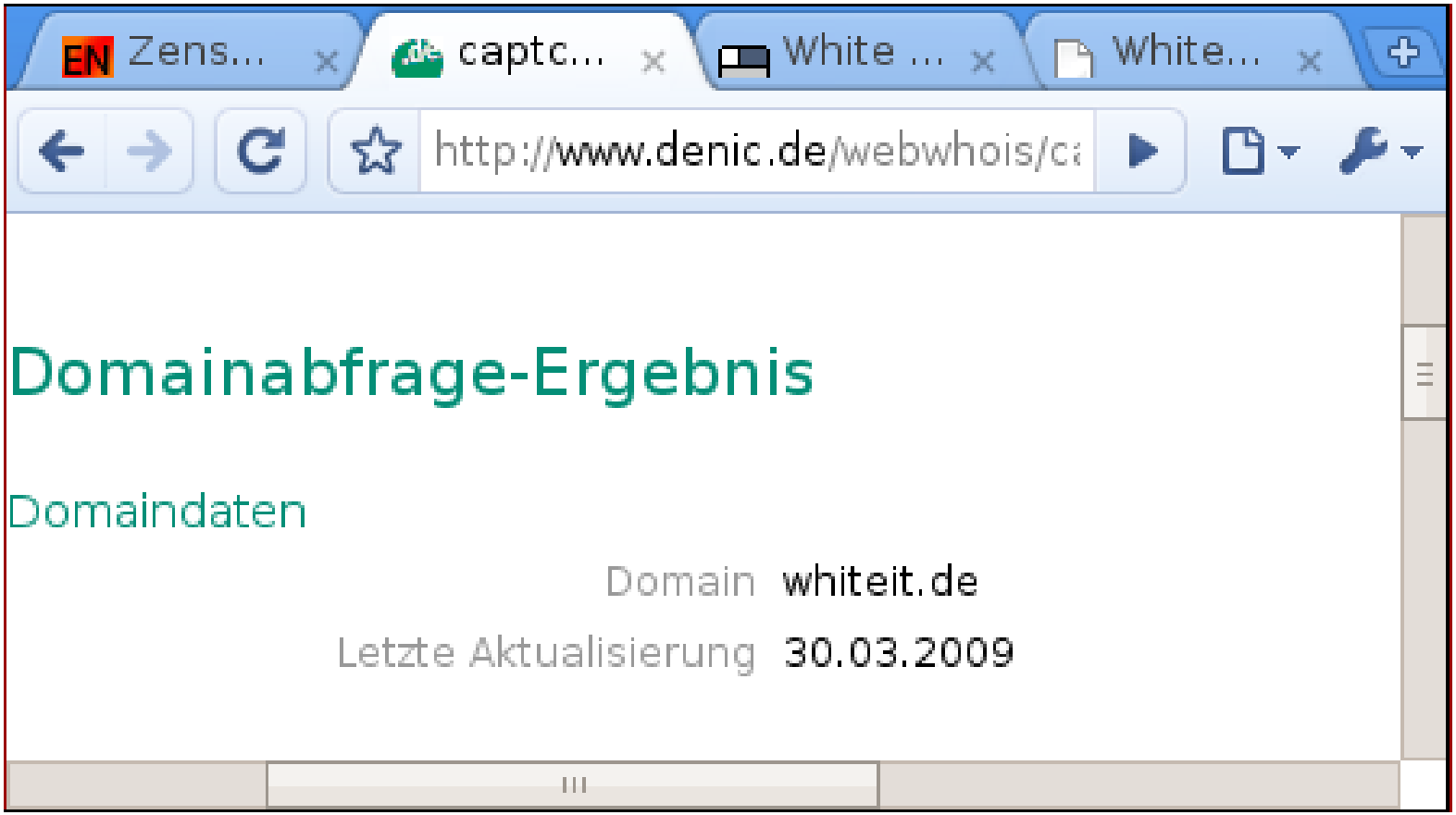


Abbildung: Ist „White It“ eine Sockenpuppe?

Zum Thema „White It“ #2

Abbildung: Ist „White It“ eine Sockenpuppe?

Ein Blick zum Horizont ..

- Es ist davon auszugehen, dass die Freiheit im Internet weiterhin unter Beschuss durch NeoCons sowie die Verwertungslobby bleiben wird.
- Innenminister Thomas de Maizière hatte vor der Wahl die ja schon mal die Einführung eines Internetausweises gefordert.
- Zur Akzeptanzverbesserung für Internetsperren, könnte man auf die Idee kommen eine Technik wie in England aufzusetzen.
- **Sperrung Wikipedia-Artikel zu Scorpions „Virgin Killer“**
- Diese Technik erlaubt die Erstellung von Nutzer-Profilen, sowie das Mitlesen vertraulicher unverschlüsselter Daten.
- Vorhandensein solcher Technologie begräbt Vertraulichkeit jeglicher Kommunikation ohne Ende-zu-Ende Verschlüsselung.

Forderungen an die Politik

- Die entsprechenden Bundes- und Landesbehörden müssen verpflichtet werden bei der Entfernung dieser Inhalte, besser international zusammenzuarbeiten.
- Die Arbeit des BKA bezüglich des Löschens kinderpornographischer Inhalte muss eng evaluiert werden.
- Ziel muss sein eine Reaktionzeit von 24 h zu erreichen.
- Fälle mit einer Verweildauer > 72 h sind zu dokumentieren und zur Qualitätsicherung zu untersuchen.
  (Himmel lief über Monate unter Beobachtung der Polizei!)
- Zum Vergleich: 80% aller Webseiten, die von eco innerhalb des INHOPE-Netzwerkes weitergeleitet werden, werden innerhalb von 24 Stunden nach Meldung vom Netz genommen
  INHOPE: Die freiheitliche Alternative zu Zugangssperren

Was ist zu tun?

- Aus verschiedenen Gründen sind die Zugangs- und Hostingprovider nur bedingt in der Lage (oder Willens) unsere Freiheiten zu verteidigen.
- Eigentlich wäre ja zu erwarten, dass ein Provider die Gültigkeit seines (wahrscheinlich sittenwidrigen) Vertrages anficht.
- Das Zögern der Provider (und auch der Branchenverbände) und der teilweise Mangel an deutlichen Worten (**Herrn Süme** und **Herrn Rotert** mal explizit ausgenommen) verschafft Sperrbefürwortern eine Glaubwürdigkeit, die sie nicht verdienen.
- Es ist auch an uns die Rahmenbedingungen schaffen, unter denen Sperren nicht mehr argumentierbar sind.
- Projekte wie „White IT“ sollten wir im Blick behalten. Vielleicht es möglich da beobachtend teilzunehmen, ohne der Veranstaltung Credibility zu verleihen.

Ein Blick auf Begrifflichkeiten – Digital Natives ...

- **Digital Naïves?**
- Denn auch als solche wurden wir in der Debatte dargestellt.
- Ich denke deswegen wir sollten uns weder als solche bezeichnen noch bezeichnen lassen.
- Denn nicht wir sind die Eingeborenen, denen das Wissen um wichtige Kulturtechniken, wie die von Frau von der Leyen geforderte Anstandsregeln im Netz, fehlt. (Die Netiquette hat übrigens sogar eine eigene RFC $\Rightarrow$ 1855)
- Zudem existieren wir nicht nur ausschließlich im Internet.
- Zuallererst sind wir doch Bürger, die dann zusätzlich sehr intensiv das Internet zur Meinungsbildung und -äußerung (sowie zum Zeitvertreib) nutzen.

Ein Blick auf Begrifflichkeiten – Netzneutralität ...

- **Ein neutrales Netz?**
- Das Netz soll keine Inhalte oder Dienste diskriminieren.
- Genau das würde das Netz ohne Manipulation von außen tun.
- Im Zeitalter solcher Kampfbegriffe wie **Killerspiele**, **Raubkopierer**, **Internationaler Terrorismus** und **Kinderpornographie** ist diese Position aber schwer zu vermitteln.
- Als Begriff deswegen für unsere Ziele nicht wirklich brauchbar.
- Deswegen sollten wir nicht weniger fordern als eine **ungehinderte Ende-zu-Ende-Kommunikation**, in welcher Form auch immer sie stattfindet.

Technik

- Wir haben keine Kontrolle über die Infrastruktur.
- Vodaphone filtert in UMTS-Netzen zum Beispiel den Port 53. (DNS-Proxy & freie DNS Server funktionieren da nicht mehr)
- Technische Lösungen zur Umgehung einer Zensur werden also nur bedingt weiterhelfen.
- Auch wenn die Sperren nicht kommen sollten wir trotzdem Technik zu deren Umgehung (weiter-)entwickeln.
- Dies auch zur Unterstützung demokratischer Bewegungen in anderen Ländern.
- Im folgenden drei Beispiele.
  - DNS-via-HTTP(S)-Tunnel.
  - DNS-with-Cache-in-DHT (Kademlia).
  - HTTP-Proxy-with-Cache-in-DHT.

Technik – DNS-via-HTTP(S)-Tunnel

- Prototyp in Python (Twisted)
- Läuft als eigener Prozess, asynchrones Eventhandling
- Erlaubt verschiedene Backends (recursive, forwarding (DNS & HTTP(S)), DHT) kann also beliebig verkettet werden
- Eingebetteter HTTP-Server erzeugt JSON:
  - `http://139.30.91.160:8882/SHORT/IN/A/heise.de`

    ```
    [{'__type__':'Record_A', 'address':'193.99.144.80', 'ttl':8175}]
    ```
  - `http://139.30.91.160:8882/PROXY/IN/A/heise.de`

    ```
    [[{'__type__':'RRHeader', 'name':'heise.de',
    'auth':false, 'ttl':18658, 'cls':'IN', 'type':'A',
    'payload':{'__type__':'Record_A', 'address':'193.99.144.80',
    'ttl':18658}}], [], []]
    ```
- Idee: Browser-Addon, welches Namesauflösung über DNS ersetzt durch eine Namensauflösung über HTTP(S)

Verteilte Infrastrukturen – DHT-DNS-Cache

- Wir sind viel zu abhängig von zentralen Infrastrukturen.
- Gerade auch die Sperrdebatte hat gezeigt wie anfällig DNS ist.
- Es ist also naheliegend auf eine dezentrale Infrastruktur auszuweichen.
- **Idee:** Namensauflösung über P2P (ähnlich Bittorrent)
- **Prototyp** in Python (Twisted + Entangled [Kademlia DHT])
- Sucht Namen zuerst in der verteilten Hashtable dann Fallback auf recursive oder forwarding (DNS + HTTP(S)) Resolver speichert das Resultat in der DHT
- Es hat einen **Bug** oder auch **Feature:** Werte in der Hashtable können nicht gelöscht und nur bedingt geändert werden.
- Dazu muss noch ein Trust-Management her.
  DNSSEC wird da natürlich helfen ;-)

Verteilte Infrastrukturen – DHT-HTTP-Proxy

- Wie sichert man Inhalte gegen eine zentrale Inhaltskontrolle?
- Googles Cache und Archive.org helfen da nur bedingt. (zentrale Infrastruktur + Inhaltskontrolle)
- Diese cachende Infrastruktur sollte einen legitimen Nutzen haben (Browser-betriebene verteilte Suchmaschine? :)
- Bei der Entwicklung der Software Ease-of-Use im Focus.
- Die Infrastruktur sollte überwiegend ($> 90\%$?) legitime Nutzer haben, auch dies beim Design beachten.
- **Experimenteller Prototyp:** HTTP-Proxy (aus Twisted) mit Cache in DHT (Kademlia aus Entangled)
- Webseiten werden verschlüsselt in der DHT gespeichert,
- DHT-Knoten kann Inhalte nur unter Kenntnis der zugehörigen URL entschlüsseln, diese wird nirgendwo gespeichert.
- **Aber:** Die Möglichkeit Inhalte zu entfernen besteht, braucht aber die Kooperation der Node-Betreiber.

Verteilte Infrastrukturen – Sind wir halt die Cloud :)

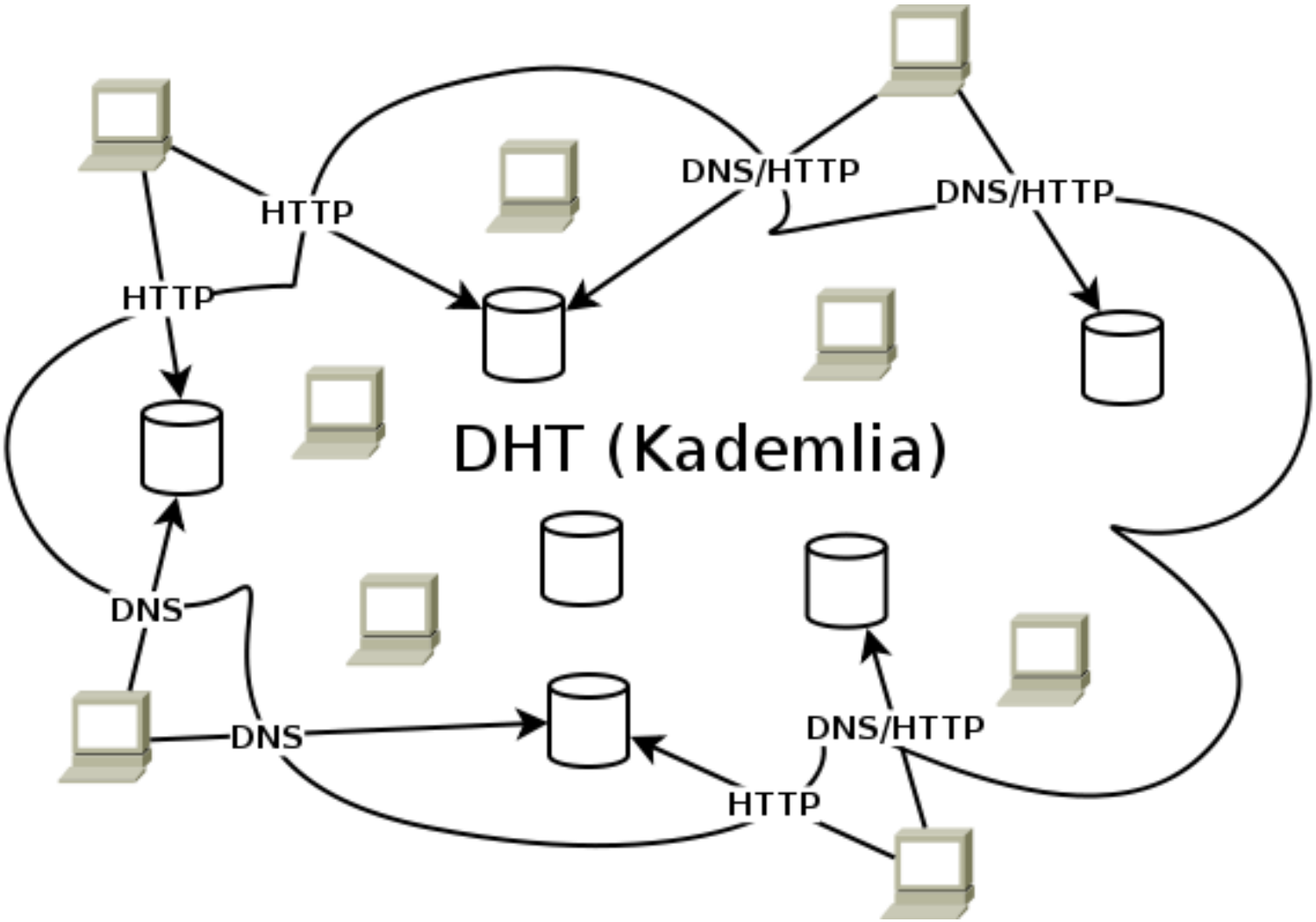


Abbildung: Distributed Hashtable (DHT) als Web/DNS-Cache

Verteilte Infrastrukturen – Demo

This frame shall remind me,
that i wanted to do a demo ;-)

Danke für die Aufmerksamkeit :)

This is space has intentionally been left blank to make room for Questions & Remarks :-)

Argumente gegen Sperren #1 – Gesellschaft

- Das Vorhandensein von Kinderpornographie im Internet ist ein Spiegel gesellschaftlicher Zustände.
- Generell ist Technologie zur Lösung gesellschaftlicher Probleme nur bedingt geeignet.
- Weiterhin ist solcherart Technik Inhalte-neutral.
- Sperr-Technik ist also immer darauf angewiesen von Menschen geeignet bedient zu werden.
- Mit der geplanten (und bald umgesetzten) Infrastruktur kann jede beliebige Form von Inhalten im Internet (dem Web/WWW) unterdrückt werden.
- In diesem Zusammenhang ist es bedenklich, dass das BKA dazu ermächtigt wird, eine geheime Liste von zu sperrenden Servern zu führen und die Sperrung durch die Provider zu erwirken.$\Rightarrow$ Gewaltenteilung & Rechtsweggarantie

Argumente gegen Sperren #2 – (Vor-)Zensur

- Da ganze Server gesperrt werden, wird auch die Verbreitung zukünftiger Inhalte verhindert ⇒ Vorzensur.
- Kanonisches Beispiel: der australische Zahnarzt, in dessen Webseite eingebrochen und dann illegale Inhalte verbreitet wurden. Der Zahnarzt stand auch nach Bereinigung seiner Webseite weiterhin auf der Sperrliste.
  NEWS.com.au: Blacklist includes dentist, kennel, tuckshop
- Zudem ist die Kinderpornographiedefinition ziemlich weich.
- Kinderschützer sagen auch relativ offen, dass es nicht nur um die Dokumentation sexuellen Kindesmissbrauchs, sondern auch um fiktive Inhalte wie Comics und Texte geht.Anfixthese
- Es wäre denkbar, dass Berichte von Opfern zensiert werden.
- Um dem vorzubeugen war die Minimalforderung immer die nach einem Richter-**vor**-behalt.

Argumente gegen Sperren #3 – Löschen ist effizienter

- Es sollte Prämisse staatlichen Handelns sein, kriminelle Inhalte aus dem Internet zu entfernen, statt sie nur mit Stopp-Schildern zu überdecken.
- Alles andere demonstriert nur die Kapitulation des Staates vor Kriminalität im Internet.
- Mit dem Blick auf die internationale Situation:
- Eine kinderpornographische Webseite muss nur einmal, durch das Handeln eines einzelnen Staates, entfernt werden.
- Um den selben Effekt weltweit mit Sperren zu erreichen, muss in jedem Land, bei jedem Provider gesperrt werden, ansonsten werden dieser Inhalte weiterhin international verbreitet.
- Es gibt also die Möglichkeit durch internationale Zusammenarbeit Synergien bei der Bekämpfung der Dokumentation sexuellen Missbrauchs zu nutzen.

Argumente gegen Sperren #4 – Löschen ist schneller

- Die Verweilzeit kinderpornographischer Inhalte im Internet ist durchschnittlich 30 Tage, nach Kenntnisnahme!
- Dies im Kontrast zu Banktrojaner- und Phishing-Seiten diese werden nach 4-8 Stunden aus dem Netz entfernt.
  „The Impact of Incentives on Notice and Take-down“
  Tyler Moore and Richard Clayton, University of Cambridge
- Notice and Takedown ist jederman möglich.
- Die meisten Provider haben Acceptable Use Policies [AUP] diese sind deutlich enger gefasst, als die örtlichen Gesetze.
- Hinweis dass Kunden illegale Inhalte hosten, mit Verweis auf die AUPs, führt zur sofortigen Entfernung und häufig Kündigung durch den Provider.
- Alvar Freude (AK Zensur) hat 60 Server in 12h abschalten lassen: AK Zensur: Löschen statt Verstecken, es funktioniert
- Das funktioniert sogar mit Child-Modeling-Seiten in Japan

Argumente gegen Sperren #5 – kommerzieller Massenmarkt?

- Den behaupteten kommerziellen Massenmarkt gibt es wahrscheinlich nicht. Auch wäre dann wohl die Devise: Follow the Money!
- Auch gibt es gar nicht so viele Webseiten, wie behauptet
- Im Jahr 2008 betrafen, bei der eco Internetbeschwerdestelle, von 2.562 Beschwerden über Kinderpornografie nur 449 den Dienst WWW. MOGiS: Antwort der Internet-Beschwerdestelle
- Unter diesem Aspekt sind die Kosten der Sperren horrend ($>$ 100.000.000 Euro, von den Providern zu leisten)
- Dieses Geld fehlt dann für Initiativen, wie zum Beispiel: Forum: Provider gegen Kindermissbrauch im Internet
- Auch werden diese Mittel zum Teil als Steuereinnahmen ausfallen und damit bei der Prävention und Bekämpfung solcher Inhalte fehlen.

Argumente gegen Sperren #6 – Welche failed states?

- Stehen die Server in rechtlosen Staaten?

```
SELECT * FROM blockinglists WHERE country IN ('SO', 'ZW',
'SD', 'TD', 'CD', 'IQ', 'AF', 'CF', 'GN', 'PK', 'CI', 'HT',
'MM', 'KE', 'NG', 'ET', 'KP', 'YE', 'BD', 'TL', 'TP', 'UG',
'LK', 'NE', 'BI', 'NP', 'CM', 'GW', 'MW', 'LB', 'CG', 'UZ',
'SL', 'GE', 'LR', 'BF', 'ER', 'TJ', 'IR');
hostname|hostid|ip|reverse|country|whois|abusemail
--------+------+--+-------+-------+-----+---------
(0 rows)
```

- Über 90% der Server in: USA ($>$ 50%), Niederlande, Kanada/Russland/Deutschland, Südkorea, Portugal, Großbritannien
- Von der Norwegischen Sperrliste:

```
US:1292, NL:146, CA:79, RU:75, DE:69, KR:62, PT:61, GB:54,
CZ:37, SE:32, UA:15, JP:12, AU:11, HK:8, BZ:8, CN:6, BS:5,
FR:4, PA:3, ES:3, DK:3, TW:2, BY:2, TR:1, TH:1, SK:1, RO:1,
NO:1, MX:1, LV:1, IT:1, BR:1, AR:1
```

Argumente gegen Sperren #7 – Wo stehen die Server?

Herkunft der Einträge auf der Norwegischen Sperrliste

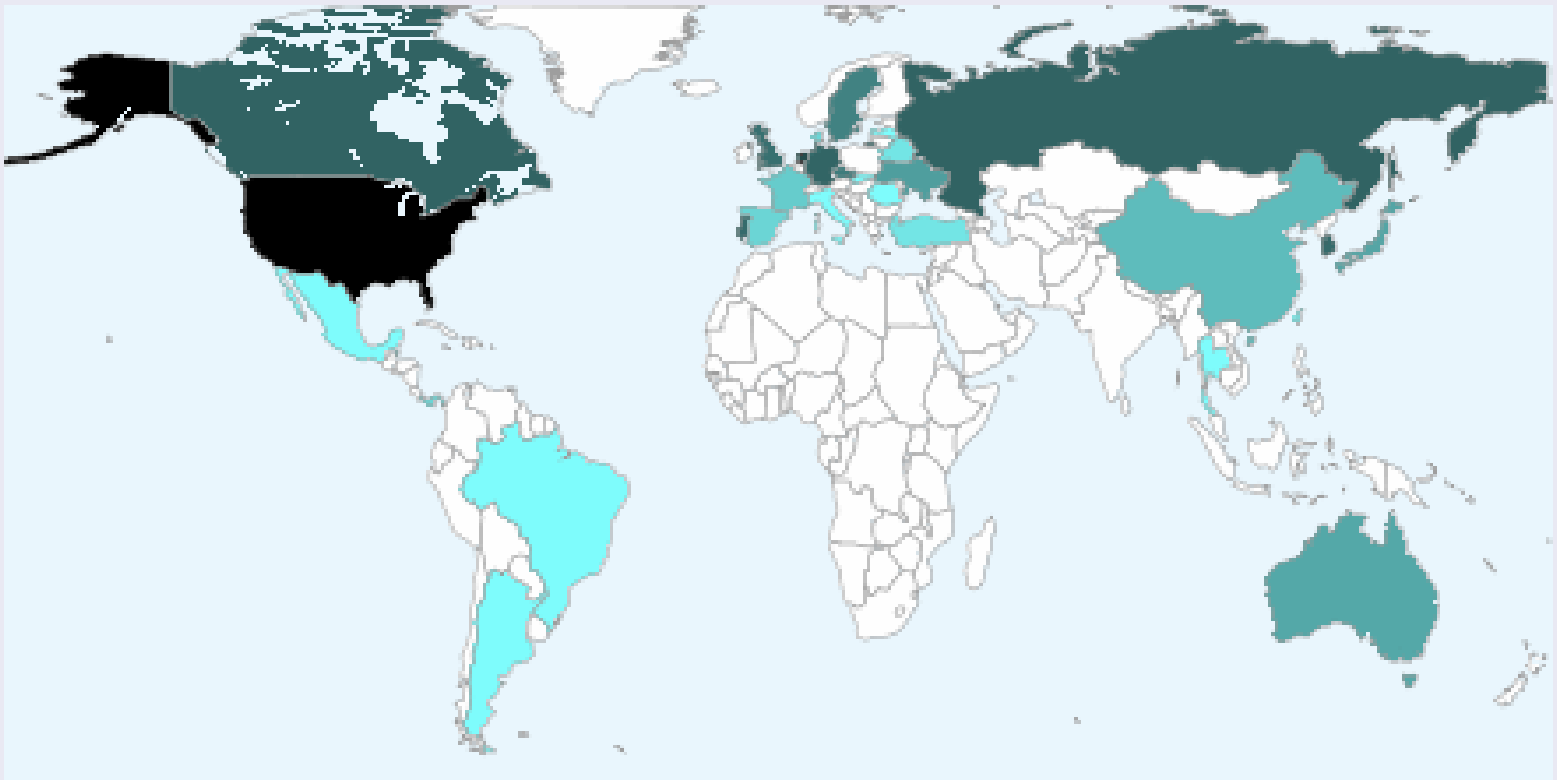


Abbildung: Standorte der Server von der norwegischen Sperrliste

Argumente gegen Sperren #7 – Wo stehen die Server?

Herkunft der Einträge auf der Norwegischen Sperrliste

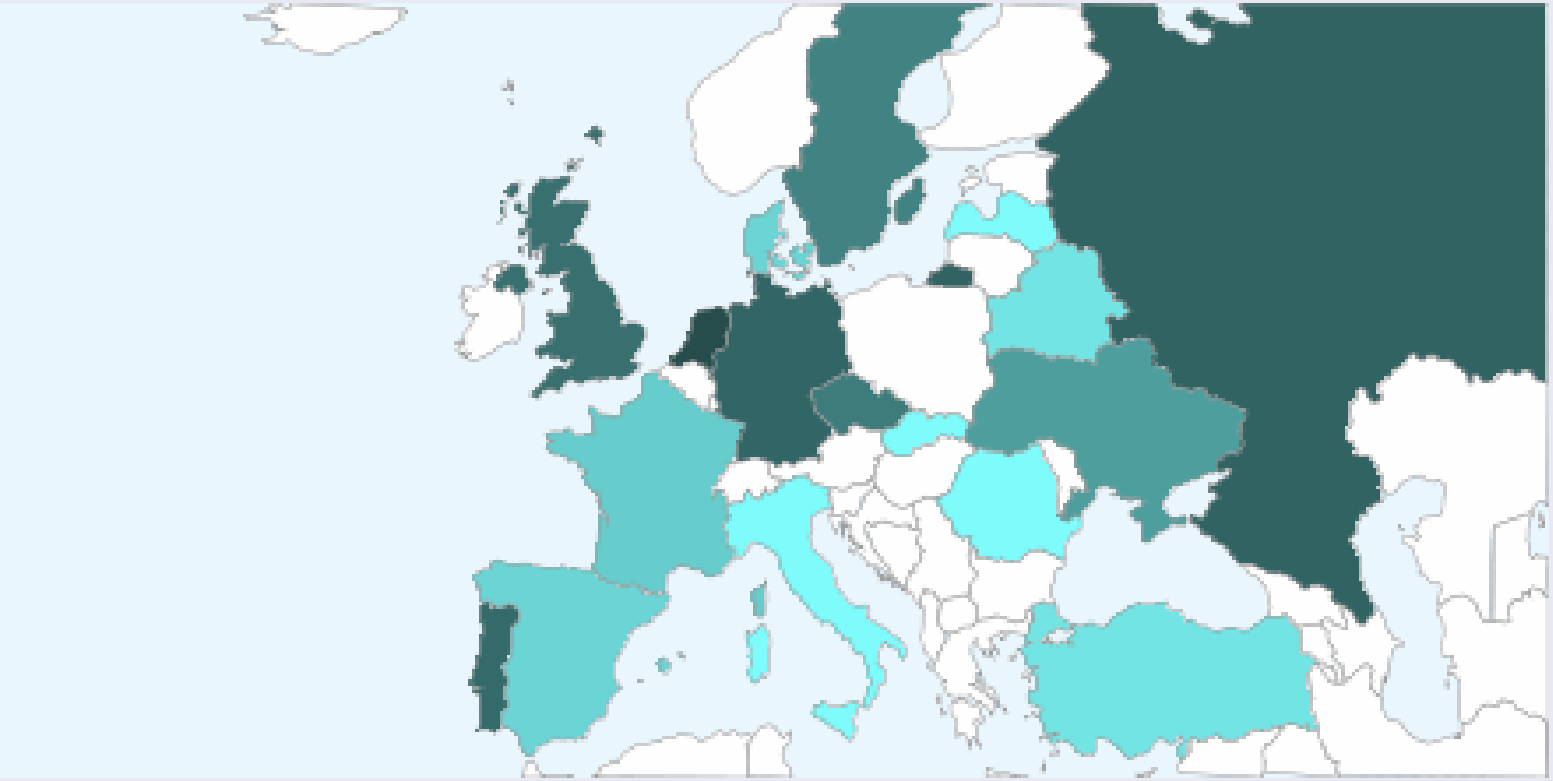


Abbildung: Standorte der Server von der norwegischen Sperrliste

Argumente gegen Sperren #8 – Verfolgung möglich!

Staaten mit adäquater Gesetzgebung

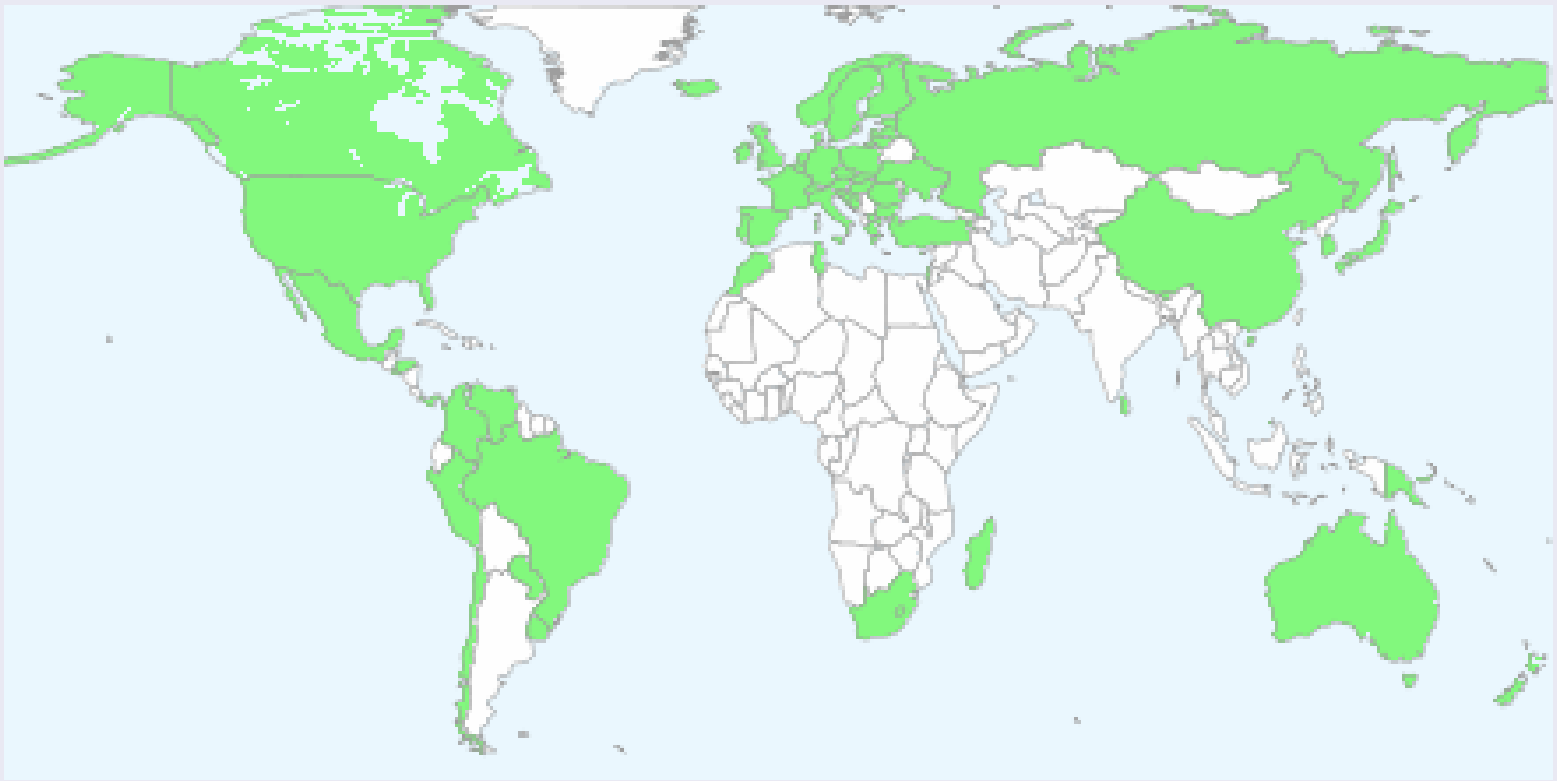


Abbildung: Staaten mit adäquater Gesetzgebung

(Viele moslemische Länder ächten jegliche Form von Pornographie)

Argumente gegen Sperren #8 – Verfolgung möglich!

Staaten mit adäquater Gesetzgebung

Abbildung: Staaten mit adäquater Gesetzgebung

(Viele moslemische Länder ächten jegliche Form von Pornographie)

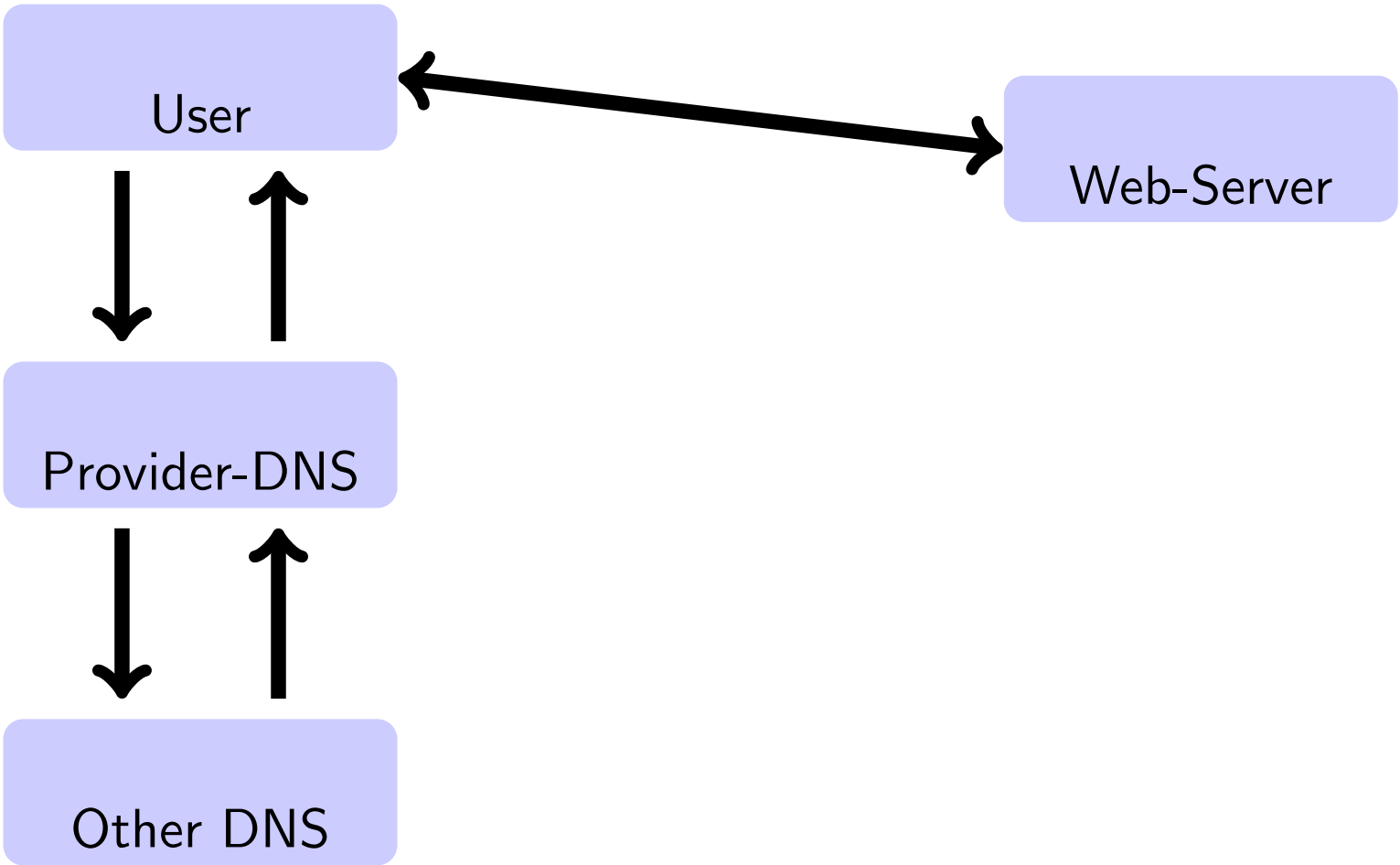
Argumente gegen Sperren #9 – Sinkende Fallzahlen!

- Mit Erscheinen der vollständigen PKS des Jahres 2008 (in 08.2009) ist klar, dass die PKS 2007 sehr stark durch die Operation Himmel beeinflusst war:
- Fallzahlen Besitz und Besitzverschaffung (1433) von 8832 Fällen im Jahr 2007 auf 6707 Fälle im Jahr 2008 reduziert.
- Anzahl der Ermittlungsverfahren von banden- oder gewerbsmäßiger Verbreitung (1432) auf etwa ein Drittel gesunken (-64%, $347 \rightarrow 123$ Fälle)
- Aufklärungsquote für Verbreitung in bandenmäßigen Strukturen (1432) von $82,7\%$ auf $55,3\%$ gesunken
- Kinderpornographie wird also spätestens seit der Operation Himmel verstärkt in geschlossenen Netzwerken (auch Telefon & Post) (zum großen Teil weitgehend kostenfrei) getauscht.

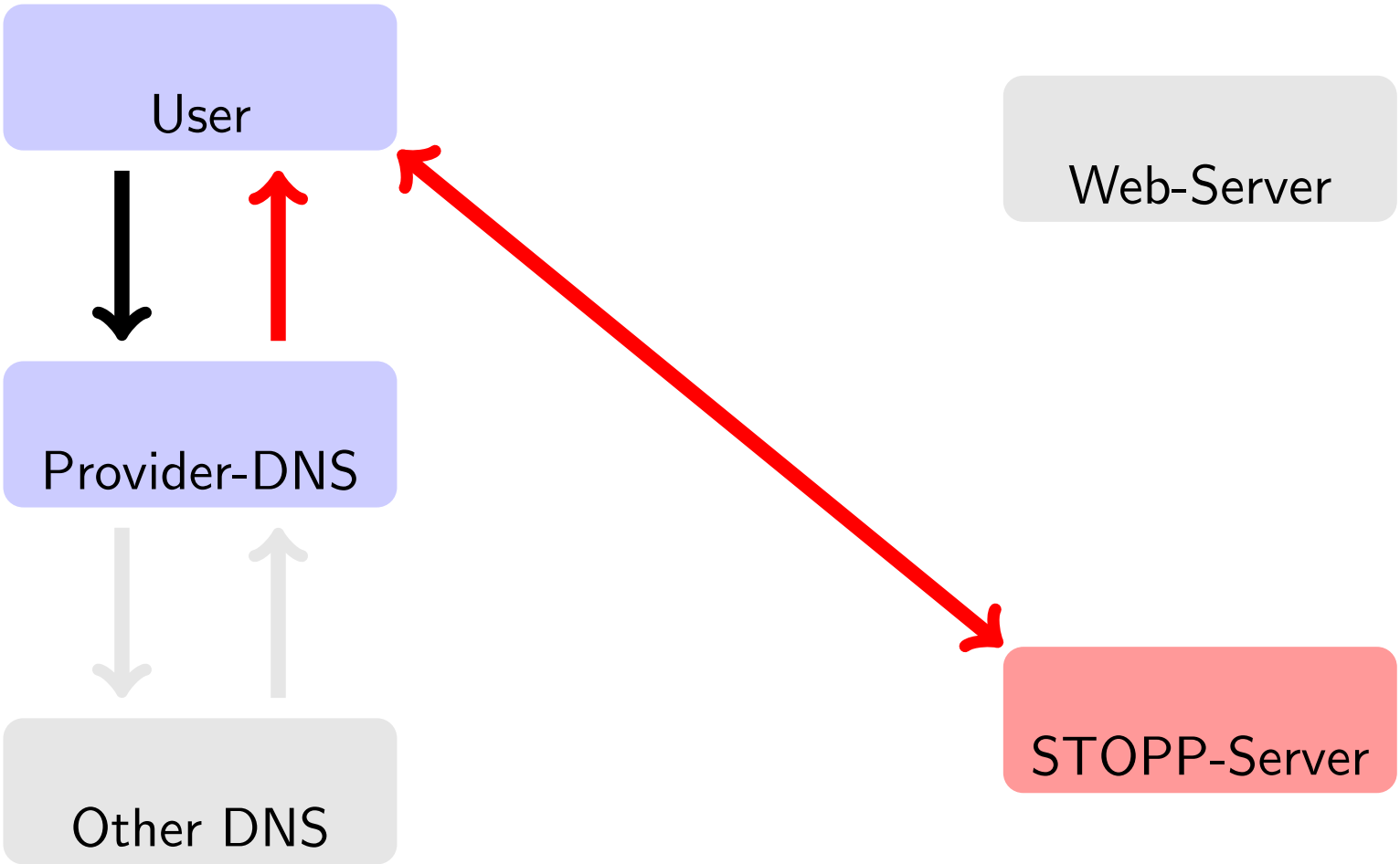
Wie die Sperren funktionieren sollen

- Die Sperren beruhen auf der Umleitung auf Stopp-Seiten
- Diese Umleitung erfolgt durch die Fälschung von Antworten der Provider-eigenen Namensauflösung (DNS).
- Die Adressumleitung wird voraussichtlich durch die Manipulation ganzer Zones realisiert. (nicht nur A-Record)
- Die Provider-eigenen Nameserver liefern dann für bestimmte Einträge gefälschte Antworten.
- Folgt ein Browser einem solchen falsche Eintrag, so wird er auf einen spezielle Webserver umgeleitet, welcher dann zu jeder Anfrage ein Stopp-Schild ausliefert.
- Dieser Stopp-Server wird jeden Zugriff aufzeichnen.
- Über alle Dienste außer HTTP wurde wohl nicht nachgedacht. (insbesondere SMTP/E-Mail und DNSSEC)

Ablauf einer korrekten Namensabfrage



Ablauf einer gefälschten Namensabfrage



Lösung? – Rekursive Namensabfrage selber durchführen!