

Gefahren der Vernetzung

Andreas Jaekle

Das Internet ist gefährlich

”Eines der größten Missverständnisse im Cyberspace ist die Gefahr durch jugendliche Hacker. Die geraten in die Schlagzeilen, weil sie gefasst werden. Aber die Profis werden nicht geschnappt.”

– Richard Hancock (Computer Security Institutes)

Übersicht

- Internet ist in amerikanischer Hand
- Wie funktioniert das Internet
 - Transportschicht
 - Vermittlungsschicht
 - Zensur in Deutschland
 - Anwendungen
 - Ziele dieser Programme
 - Persönliche Daten
- Andere Aspekte
 - Militärisch Risiken
 - Wirtschaftlich Risiken
 - Politisch Risiken

Das Internet ist in amerikanischer Hand

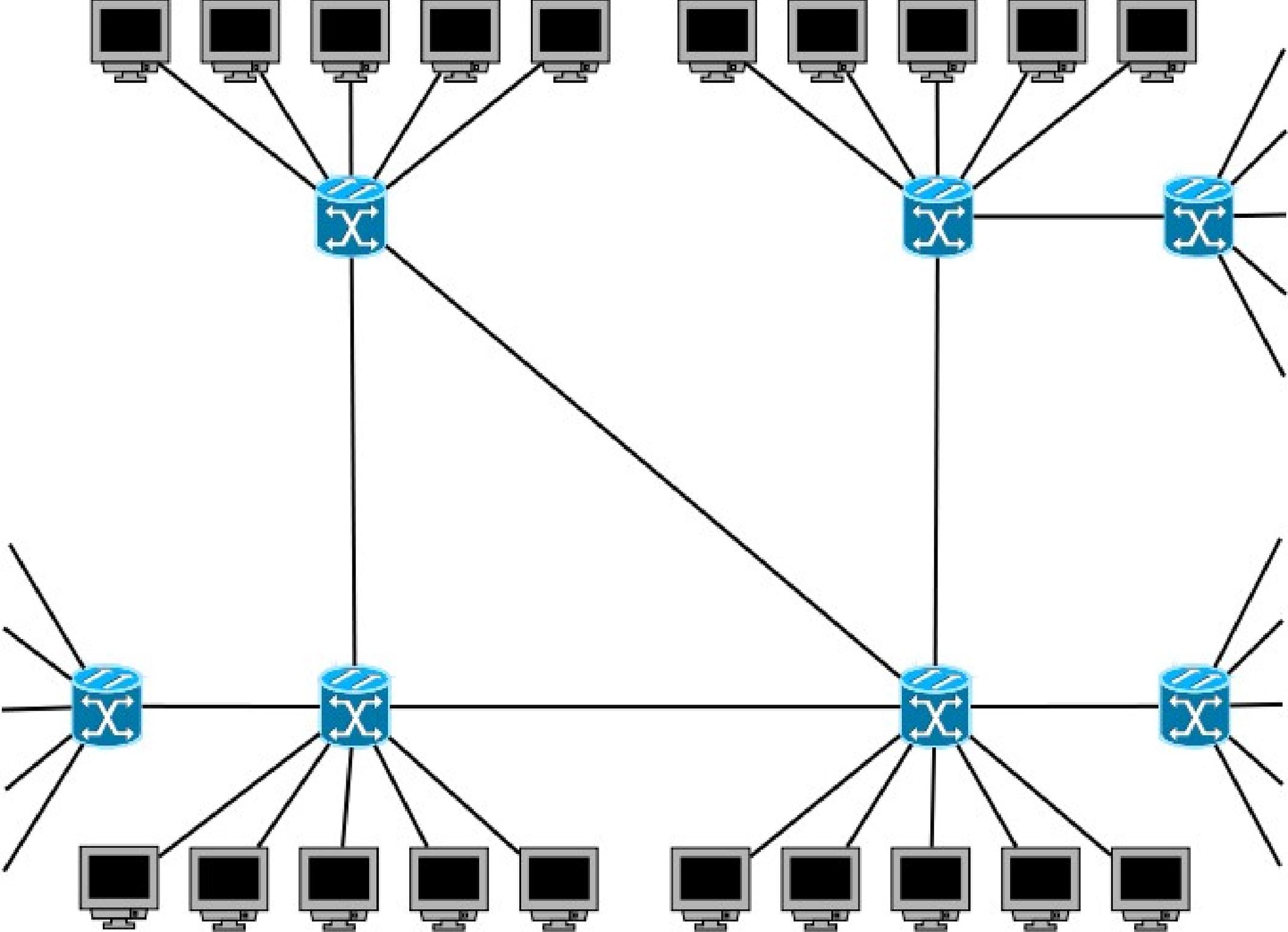
- Die Internet Corporation for Assigned Names and Numbers (ICANN)
 - Vergibt IP-Adressen
 - Koordiniert das DNS-System

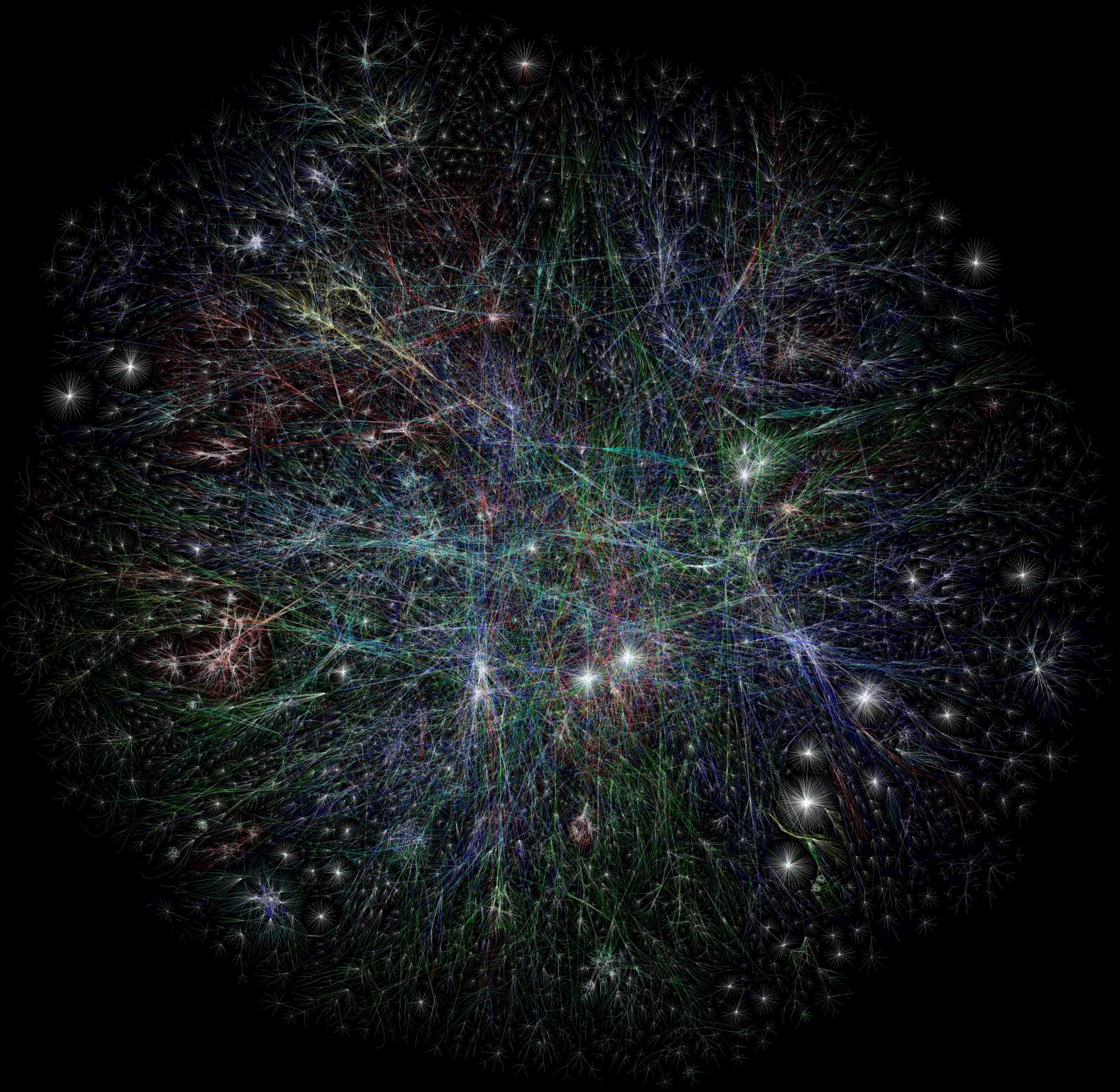
Wie funktioniert das Internet ?

- Das Internet besteht aus mehreren Ebenen
 - Transport-Schicht (Daten)
 - Vermittlungs-Schicht (DNS-Adressen)
 - Anwendungen
 - WWW
 - Mail
 - Chat
 - Würmer
 - usw.

Transportschicht

- Dezentrales Netzwerk aus tausenden von Knotenpunkten (2005 ca. 26.000)
 - Bei Ausfall einzelner Knoten wird ein anderer Weg automatisch gesucht
 - Alle Knoten wissen von allen anderen großen Knoten (ca. 170.000)
- Angriffe
 - Router (Manipulation, Fehlkonfiguration)
 - Physikalisches Trennen der Verbindungen
- Zensur über Manipulation der Router möglich





Beispiel godaddy.com

```
$ traceroute godaddy.com
traceroute to godaddy.com (97.74.104.201), 30 hops max, 60 byte packets
 1          .dyndns.org (192.168.100          0.183 ms  0.140 ms  0.134 ms
 2          .hsi5.kabel-badenwuerttemberg.de          7.870 ms  13.529 ms  13.510 ms
 3 172.30.9.101 (172.30.9.101) 12.347 ms 12.362 ms 12.324 ms
 4 HSI-KBW-078-042-040-241.hsi3.kabel-badenwuerttemberg.de (78.42.40.241) 12.253 ms 12.227 ms 12.211 ms
 5 ae1.FRA-M1.ip-bb.kabel-badenwuerttemberg.de (78.42.40.17) 38.317 ms 38.300 ms 38.273 ms
 6 9-3-0.edge5-frankfurt.eu.level3.net (195.16.160.13) 15.582 ms 15.127 ms 15.100 ms
 7 vlan79.csw2.Frankfurt1.Level3.net (4.68.23.126) 25.407 ms vlan99.csw4.Frankfurt1.Level3.net (4.68.23.254) 28.515 ms vlan69.csw1.Fra
 8 ae-82-82.ebr2.Frankfurt1.Level3.net (4.69.140.25) 24.364 ms ae-72-72.ebr2.Frankfurt1.Level3.net (4.69.140.21) 24.254 ms ae-82-82.eb
241 ms
 9 ae-41-41.ebr2.Washington1.Level3.net (4.69.137.50) 112.965 ms ae-43-43.ebr2.Washington1.Level3.net (4.69.137.58) 112.938 ms 124.40
10 ae-92-92.csw4.Washington1.Level3.net (4.69.134.158) 131.408 ms ae-62-62.csw1.Washington1.Level3.net (4.69.134.146) 110.314 ms ae-82
54) 113.496 ms
11 ae-91-91.ebr1.Washington1.Level3.net (4.69.134.141) 112.611 ms 112.597 ms ae-81-81.ebr1.Washington1.Level3.net (4.69.134.137) 109.
12 ae-2-2.ebr3.Atlanta2.Level3.net (4.69.132.85) 130.134 ms 130.044 ms 130.054 ms
13 ae-7.ebr3.Dallas1.Level3.net (4.69.134.21) 149.864 ms 149.815 ms 149.769 ms
14 ae-91-98.ebr1.Dallas1.Level3.net (4.69.146.90) 137.139 ms ae-81-88.ebr1.Dallas1.Level3.net (4.69.146.82) 138.807 ms ae-71-78.ebr1.D
15 ae-8-8.car1.Phoenix1.Level3.net (4.69.133.29) 163.784 ms 164.536 ms 160.838 ms
16 ae-11-11.car2.Phoenix1.Level3.net (4.69.133.34) 189.155 ms 173.630 ms 176.521 ms
17 THE-GO-DADD.car2.Phoenix1.Level3.net (4.53.106.2) 178.679 ms 178.986 ms 178.952 ms
18 ip-208-109-112-142.ip.secureserver.net (208.109.112.142) 166.684 ms 166.661 ms 167.915 ms
19 ip-216-69-188-74.ip.secureserver.net (216.69.188.74) 178.458 ms 178.412 ms 178.404 ms
20 ip-208-109-112-150.ip.secureserver.net (208.109.112.150) 166.170 ms 162.258 ms 177.195 ms
21 ip-208-109-112-185.ip.secureserver.net (208.109.112.185) 185.601 ms 185.563 ms 172.915 ms
```

Vermittlungs-Schicht

- `www.irgendwas.de` → 11.22.33.44
- DNS: es gibt nur ca. 200 DNS-Haupt-Server
- Bis 2003 gab es bloß 13
- Kein Schutz vor falschen Antworten
- Zensur über Manipulation der DNS-Server möglich

Heute sind es ca. 200

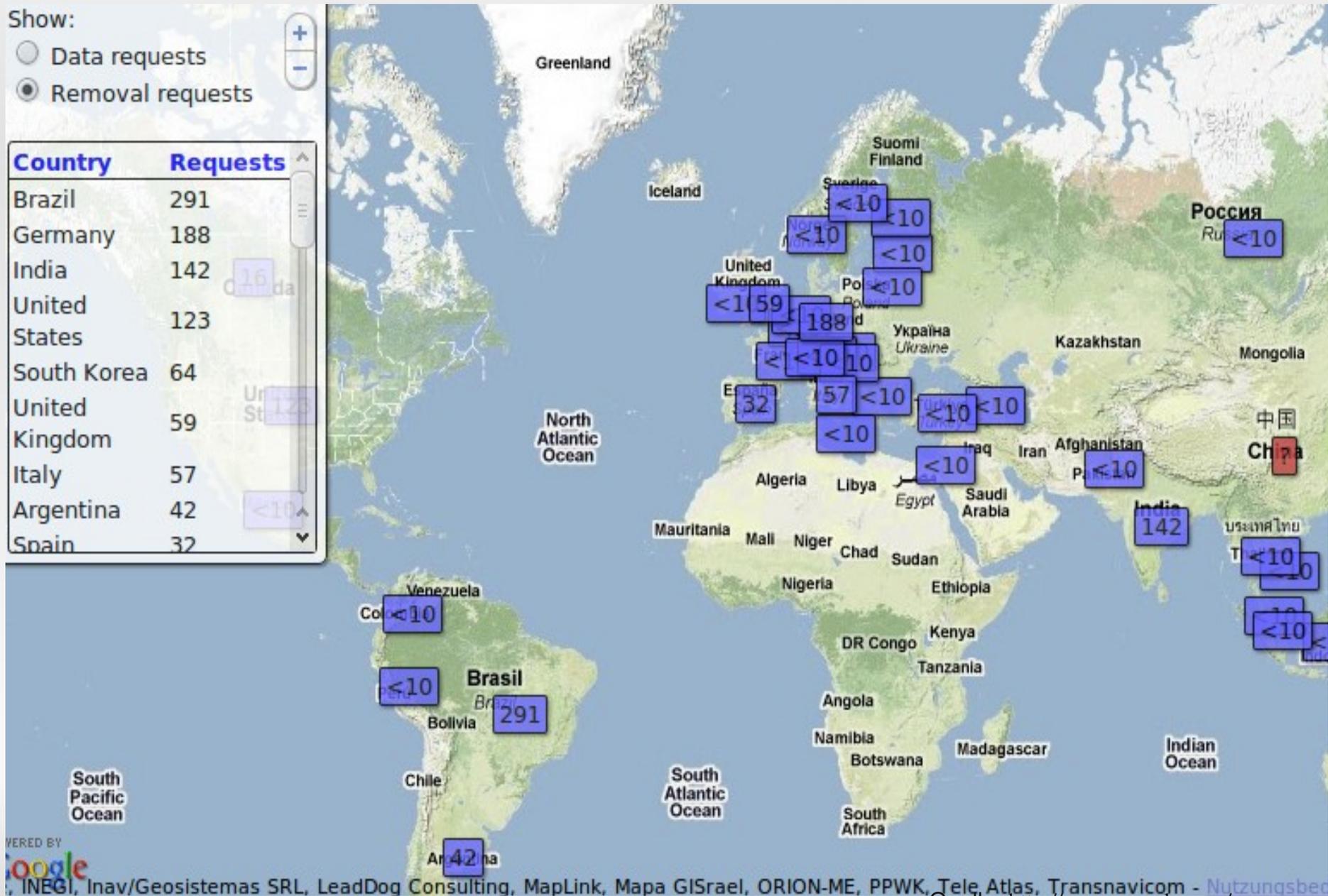


Quelle: <http://www.root-servers.org/>

Zensur in Deutschland

- Seiten werden in Deutschland dadurch zensiert, dass sie nicht gefunden werden
 - "Aus Rechtsgründen hat Google 1 Ergebnis(se) von dieser Seite entfernt. Weitere Informationen über diese Rechtsgründe finden Sie unter ChillingEffects.org."
- Sachen, die in Deutschland zensiert werden:
 - Unmenschliche Gewaltdarstellung
 - Nazipropaganda
 - Pornographie

Eingriffe der Regierungen



Anwendungen

- Manipulierte Webseiten
 - Auslesen von Daten zur Nutzeridentifizierung
- Viren
 - Programme, die vorhandene Programme modifizieren
 - Verbreiten sich über Mails und Webseiten
- Würmer
 - Programme, die sich selbst über das Netzwerk verteilen
- Trojaner
 - Scheinbar nützliches Programm
 - Verbreitung vor allem über Webseiten

Ziele dieser Programme

- Ego des Authors
- Persönliche Daten ermitteln
- Botnetzwerke aufbauen
- Zerstörung von Daten
- Dialer
- Werbung einblenden
- Phishing durch Manipulieren von Webseiten
- Spionage

Persönliche Daten

- Werbung mit persönlichen Daten
- Zielgruppenspezifische Werbung
- Phishing (Zugangsdaten erschleichen)
- Erpressung
- Social Engineering

Militärische Aspekte

- Militärspionage
- Sabotage
- Propaganda
- Stören, manipulieren, unterbinden der Landes internen Kommunikation

Wirtschaftliche Aspekte

- Wirtschaftsspionage
 - Stehlen von Technologien
 - Bessere Verhandlungsposition
 - Veröffentlichungstermine
- Konkurrenz schädigen
 - Webshop angreifen
 - Kostenpflichtige Werbung
- Meinungsmanipulation
 - Wikipedia, Blogs, Suchergebnisse, Nachrichten

Politische Aspekte

- Staatsgeheimnisse
 - Verhandlungsstrategien
- Öffentliche Meinung manipulieren
- Lobbyarbeit
- Meinungsmanipulation
 - Wikipedia, Blogs, Nachrichten

Dank für Ihre Aufmerksamkeit

Fragen ?

Quellen

- http://www.zdnet.de/news/wirtschaft_telekommunikation_wirtschaftsspionage_blueht_dank_internet_story-39001023-2053395-1.htm
- <http://dejure.org/gesetze/StGB/131.html>
- <http://www.root-servers.org/>
- <http://de.wikipedia.org/wiki/Root-Nameserver>
- <http://www.heise.de/newsticker/meldung/Chinesischer-Provider-entfuehrt-kurzzeitig-Teile-des-Internets-975137.html>
- <http://www.google.com/governmentrequests/>
- <http://www.opte.org/maps/>
- http://de.wikipedia.org/wiki/Social_Engineering_%28Sicherheit%29
- <http://www.de-cix.net/content/network.html>