Internet Censorship

194.144 Privacy-Enhancing Technologies

Dr. Wilfried Mayer

Outline

Internet Censorship

Censorship Concepts & Techniques

Detection & Measurement

Censorship Events Worldwide

Countermeasures & Circumvention

Internet Censorship

Censorship - What?

Control over Information

- Suppression of Content
- Control over Access
- Censorship in an online world?

Internet Censorship

Same concept, but …

- Global network (different jurisdictions)
- Fast developing technology
- Distributed technology

Quotes

- “The Net interprets censorship as damage and routes around it.” - John Gilmore, 1993
- “There is more than one way to burn a book. And the world is full of people running about with lit matches.” - Ray Bradbury, Fahrenheit 451

Why?

- Moral / Military / Political / Religious / Corporate
- Legitimate interest of democratic society
    - Illegal content
    - e.g., Wiederbetätigung
- Political supression
    - Supression of free press
    - Supression of free information
- Who decides?
    - Democratic society, Regimes or Companies
    - Facebook censors breast cancer campaign
    - Related topic: Net Neutrality

Who?

- Scope[1]
  - Individuals
  - Corporations (Service providers, ISPs)
  - State level actors (Legislation)
- Influence & Visibility
- physical, political, economic dynamics

[1] Source: Khattak et al., PETS 2016

Censorship Concepts & Techniques

Example: Tor vs. China

- Tor originally not invented for censorship circumvention
- Used to evade Great Firewall of China (GFW)
- Good example for an arms race[2]

[2] Source: Tschantz et al., S&P 2016

Timeline 1/5

- 2008: Block Tor website (www.torproject.org)
- Response: Website Mirrors, distribution over email

Timeline 2/5

- 2009: Block hardcoded list of Directory Authorities
- Also block all Tor relays
- Response: Introduction of Bridges

Timeline 3/5

- 2009: Enumerating Bridges and blocking them
- Response: Secret unknown Bridges

Timeline 4/5

- 2011: Deep Packet Inspection (DPI)
- e.g., Tor’s TLS client cipher suites
- Response: Pluggable Transports

Timeline 5/5

- 2011: Active Probing against PT
- PT-design against active probing

Other Research

- Ensafi et al. , PETS'15
  Analyzing the Great Firewall of ChinaOver Space and Time
- Winter and Lindskog, FOCI'12
  How the Great Firewall of China is Blocking Tor
- Dunna et al., FOCI'18
  Analyzing China's Blocking of Unpublished Tor Bridges
- Ling et al.
  Extensive Analysis and Large-Scale EmpiricalEvaluation of Tor Bridge Discovery

Tor vs. China

- See complexity: Global / Distributed / Developing
- Tor is often a target[3]
- From simple to complex

[3] Again Source & Good Read: Tschantz et al., S&P 2016

Censorship Theoretical Concepts

Tschantz et al.[4]

- Censor – China
- Monitor – GFW
- Circumventors
  - Users – Chinese citizens / Advocates – e.g. Tor bridge provider
- Approach – Tor meek PT
- Forwarder – Tor network
- Identifier Distribution Mechanism – Tor DirServ

[4] Source: Tschantz et al.

State-of-the-Art Censor

Censors that employ[5]

- website and IP address blocking,
- IDM disruption,
- deep packet inspection,
- and active probing; and

circumvention approaches that use

- secret IP addresses,
- encrypt their payloads, and
- resist active probing.

[5] Source: Tschantz et al.

Censorship Concepts

Fingerprinting & Direct Censorship [6]

- Fingerprinting (What to block)
  - Destination
  - Content
  - Flow Properties
  - Protocol Semantics

[6] Source: Khattak et al.

Censorship Concepts

Fingerprinting & Direct Censorship

- Direct Censorship (How to block)
  - User Side CS
  - Publisher Side CS
  - Degrade Performance
  - Block Destinations
  - Corrupt Routing Information
  - Corrupt Flow Content
  - Corrupt Protocol Semantics

Censorship Techniques

Blocking IPs

- Simple
- Static IPs not reach-/routable
- Blocking subnets or even complete ASes

Censorship Techniques

DNS Filtering

- Blocking DNS: name server does not respond
- Modifiying DNS: name server delivers modified responses
- Redirecting DNS: interception & spoofing of responses

Censorship Techniques

Connection Reset:

- TCP reset
- Injection of spoofing RST packets to disrupt connection
- Requires Deep Packet Inspection (DPI)

Censorship Techniques

Network and Routing:

- DoS attacks
- BGP hijacking
- Network disconnection

Censorship Techniques

Special software: e.g.,

- TomSkype
- GreenDam
- ...

Censorship Techniques

At service provider

- e.g., index from search engines
- Deplatforming

Censorship Techniques

JS Injection: Add or modify JavaScript files

- Tunesia during arab spring 2011[7]
  - JS injection for login credentials
  - Targeting Gmail, Yahoo and Facebook
  - Sent username and password via HTTP GET request
  - Used to delete regime-critical facebook groups and postings
- Comcast, USA, used same method for ads in 2014[8]
  - Xfinity WIFIs, for certain subscribers
  - JS was used to display adds

[7] Source: thetechherald.com

[8] Source: arstechnica.com 2

Censorship Techniques

URL Filter[9]

- Very predominantly used worldwide
- Most of the times at ISP-level
- Also, company networks (incl. TLS interception)

[9] Source: Dalek et al., IMC'13

Censorship Techniques

- New Study 2020[10] - `https://censoredplanet.org/filtermap`
- Clustered Filter Measurements
- 90 Vendors in 103 Countries

[10] Source: Raman et al., NDSS'20

Censorship Techniques

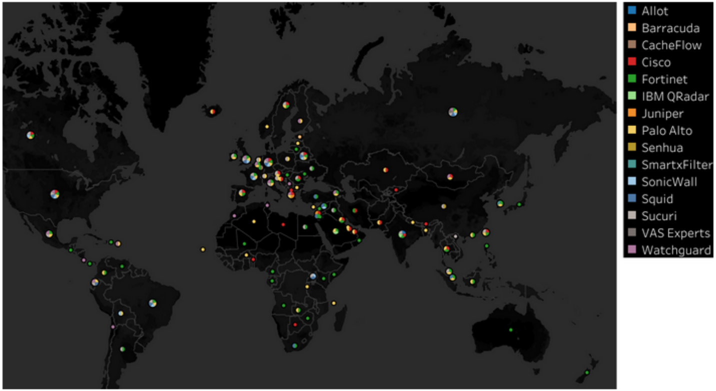


Figure 3: *World Map of commercial filter deployments*

Raman et al., NDSS'20

Censorship Techniques

Active SSL MITM

- Iran and Diginotar 2011
  - Hacked CA
- Kazachstan 2019[11]
  - Forced users to trust Root CA
- … more in TLS lecture …

[11] Source: Raman et al., Investigating Large Scale HTTPS Interception in Kazakhstan, IMC'20

Censorship Techniques

TLS Fingerprinting[12]

- Different TLS Implementations
- Unique characteristics
- CipherSuites, Behaviour, ...
- e.g. Signal, Tor

[12] Source: Frolov and Wustrow, NDSS 2019

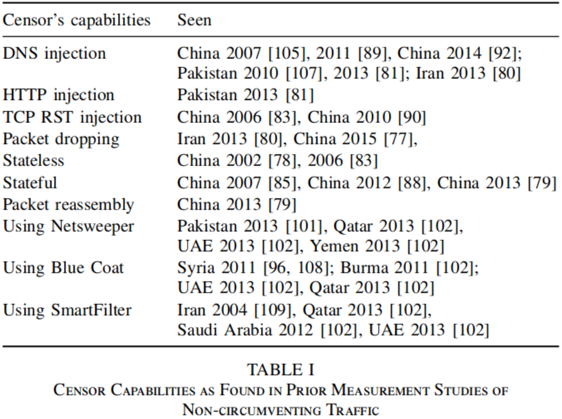
Censorship Techniques

TLS SNI Blocking[13]

- TLS Server Name Indicator (More Hosts on one IP)
- ...cleartext...
- Ommiting SNI
- Encrypted SNI (ESNI) / Encrypted Client Hello (ECH)

[13] Literature: Chai et al., FOCI 2019

Censorship Techniques Measured



Censor's capabilities	Seen
DNS injection	China 2007 [105], 2011 [89], China 2014 [92]; Pakistan 2010 [107], 2013 [81]; Iran 2013 [80]
HTTP injection	Pakistan 2013 [81]
TCP RST injection	China 2006 [83], China 2010 [90]
Packet dropping	Iran 2013 [80], China 2015 [77],
Stateless	China 2002 [78], 2006 [83]
Stateful	China 2007 [85], China 2012 [88], China 2013 [79]
Packet reassembly	China 2013 [79]
Using Netsweeper	Pakistan 2013 [101], Qatar 2013 [102], UAE 2013 [102], Yemen 2013 [102]
Using Blue Coat	Syria 2011 [96, 108]; Burma 2011 [102]; UAE 2013 [102], Qatar 2013 [102]
Using SmartFilter	Iran 2004 [109], Qatar 2013 [102], Saudi Arabia 2012 [102], UAE 2013 [102]

TABLE I
CENSOR CAPABILITIES AS FOUND IN PRIOR MEASUREMENT STUDIES OF NON-CIRCUMVENTING TRAFFIC

Tschantz et al.

Detection & Measurement

Censorship

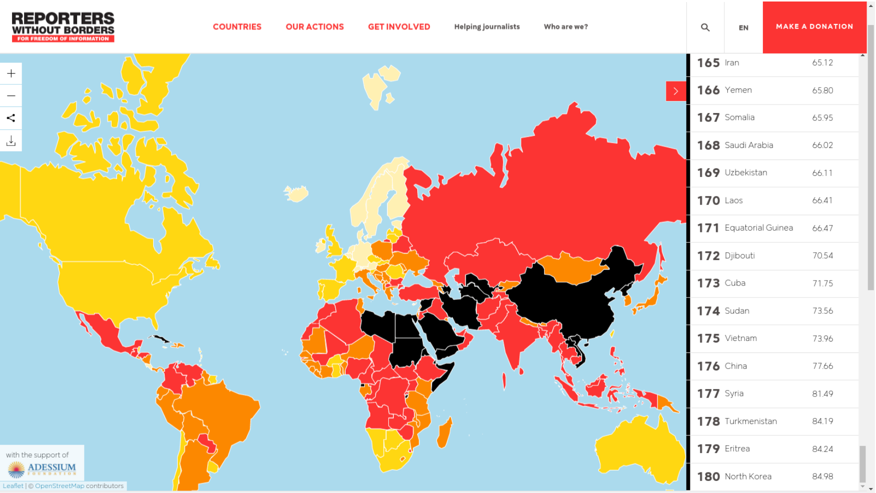
Who monitors censorship:

- Reporters without Borders, RSF - World Press Freedom
- Freedom house

- OpenNet Initiative - `https://opennet.net/`
- Citizen Lab - `https://citizenlab.ca/`
- Censored Planet - `https://censoredplanet.org/`

- OONI
- RIPE Atlas
- Tor
- National regulatory authorities

RSF: World Press Freedom Index



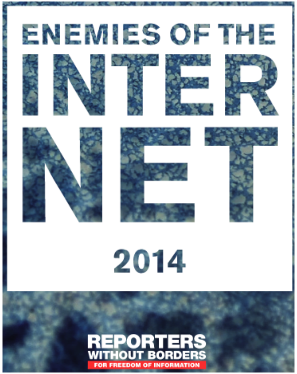
REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

COUNTRIES OUR ACTIONS GET INVOLVED Helping journalists Who are we?

EN MAKE A DONATION

165	Iran	65.12
166	Yemen	65.80
167	Somalia	65.95
168	Saudi Arabia	66.02
169	Uzbekistan	66.11
170	Laos	66.41
171	Equatorial Guinea	66.47
172	Djibouti	70.54
173	Cuba	71.75
174	Sudan	73.56
175	Vietnam	73.96
176	China	77.66
177	Syria	81.49
178	Turkmenistan	84.19
179	Eritrea	84.24
180	North Korea	84.98

RSF: Enemies of the Internet



ENEMIES OF THE INTERNET

2014

REPORTERS WITHOUT BORDERS

FOR FREEDOM OF INFORMATION

Source: Report 2014

Freedom House

Freedom on the Net Evaluated using 3 categories:

- Access restrictions
- Content restrictions
- Users

Findings 2013:

- China, Iran & Saudi Arabia filter the most
- Attacks including DDoS against dissidents Venezuela, Bahrain
- Surveillance against dissidents in many countries

Freedom on the Net

Fast forward to 2015, what has changed:

- Blocking less effective
- Content removal is king
- Surveillance laws
- Undermine anonymity
- Read the report here

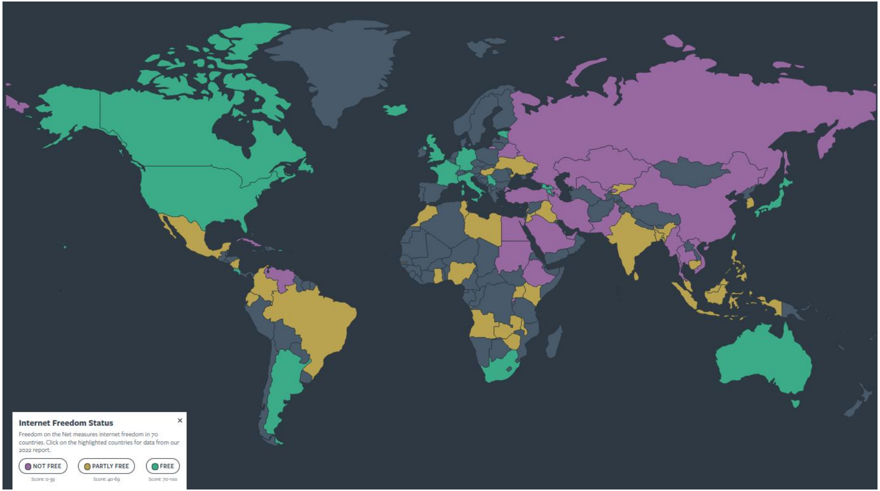
Freedom on the Net

Fast forward to 2018:

- Declines outnumber gains (again)
- China trains the world in digital authoritarianism
- Internet freedom declined in the US
- Citing fake news, governments censor
- Authorities demand control over personal data

Read the 2023 report here

Freedom on the Net 2023



Internet Freedom Status

Freedom on the Net measures internet freedom in 70 countries. Click on the highlighted countries for data from our 2022 report.

OONI

OONI

Open Observatory of Network Interference

A free software, global observation network for detecting censorship, surveillance and traffic manipulation on the internet

https://ooni.torproject.org/

OONI

- Extensible Framework
- HTTP, DNS, Multiprotocol
- Tests: e.g., Web connectivity, WhatsApp, VPNs, Tor[14]
- Run your own OONI probe!
- OONI Explorer for Results

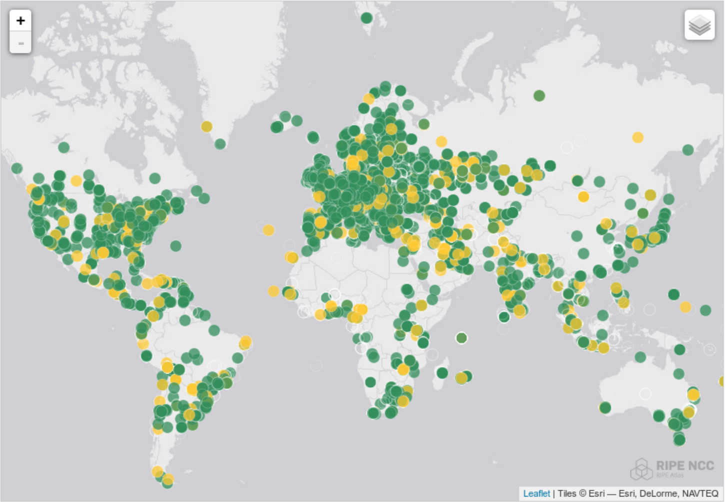
Source: Filasto and Appelbaum, FOCI'12

[14] Source: Winter - FOCI'13

RIPE Atlas

- Global network of probes (10k)
- Open Framework for Measurements
- Simple available commands: e.g., ping, traceroute, …
- Measurements “payed” with credits
- Credits for running probes
- Link

RIPE Atlas



Connected: 10166 Disconnected: 1457 Abandoned: 10763

RIPE Atlas

Censorship Measurement[15]

- Case study: Turkey’s ban of Twitter
- Various commands to measure censorship
- Various Events
    - Block Public DNS
    - Dropped traffic
    - False DNS Answers

[15] Anderson et al., FOCI’14

RIPE Atlas

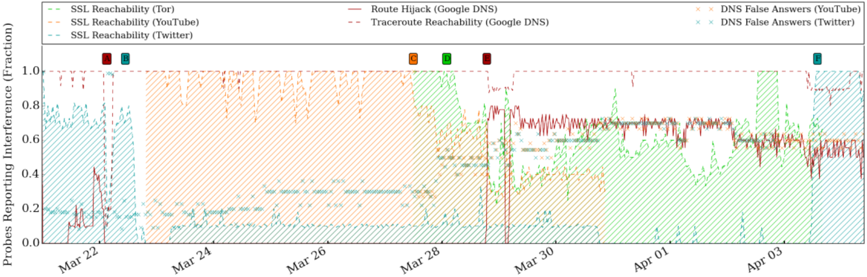


Figure 2: Disruption of Social Media Platforms in Turkey, March – April 2014

RTR Netneutrality report

- Focused on Austria
- Everything for net neutrality: e.g, 0-Rating, …
- Also port blocking, website blocks
- Source

Tor Censorship

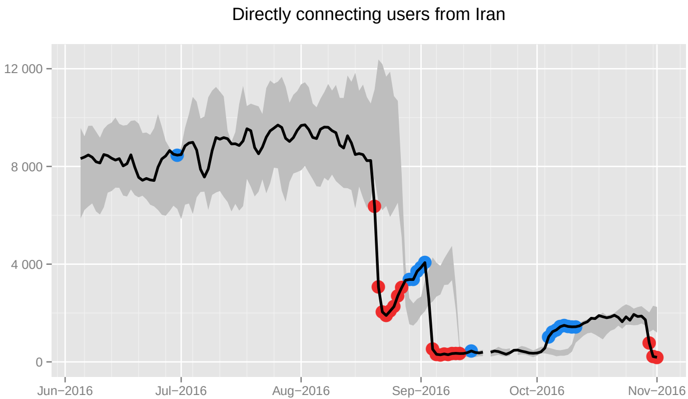
Tor often target of censorship:

- Website and downloads
- Directory servers, or all Tor relays
- DPI

Censorship event detection:

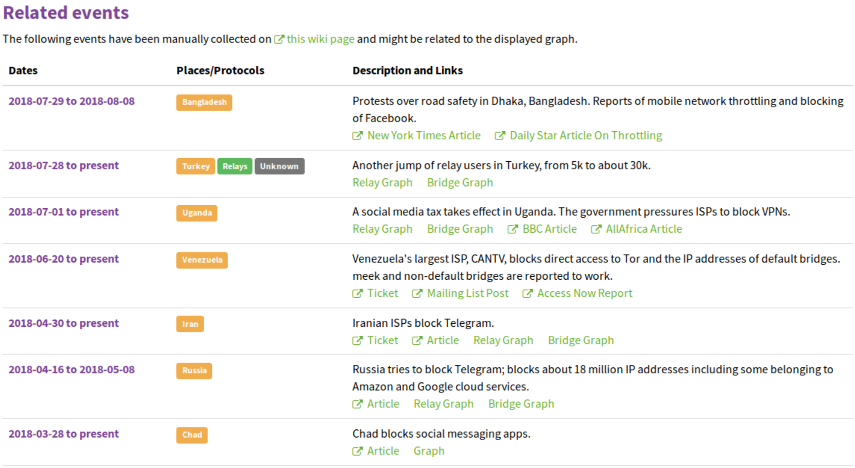
- Some directory servers collect information on user location
- Detects unusual changes (many more/less users)

Tor Metrics



The Tor Project − https://metrics.torproject.org/

Tor Metrics



Related events

The following events have been manually collected on this wiki page and might be related to the displayed graph.

Dates	Places/Protocols	Description and Links
2018-07-29 to 2018-08-08	Bangladesh	Protests over road safety in Dhaka, Bangladesh. Reports of mobile network throttling and blocking of Facebook. New York Times Article Daily Star Article On Throttling
2018-07-28 to present	Turkey Relays Unknown	Another jump of relay users in Turkey, from 5k to about 30k. Relay Graph Bridge Graph
2018-07-01 to present	Uganda	A social media tax takes effect in Uganda. The government pressures ISPs to block VPNs. Relay Graph Bridge Graph BBC Article AllAfrica Article
2018-06-20 to present	Venezuela	Venezuela's largest ISP, CANTV, blocks direct access to Tor and the IP addresses of default bridges. meek and non-default bridges are reported to work. Ticket Mailing List Post Access Now Report
2018-04-30 to present	Iran	Iranian ISPs block Telegram. Ticket Article Relay Graph Bridge Graph
2018-04-16 to 2018-05-08	Russia	Russia tries to block Telegram; blocks about 18 million IP addresses including some belonging to Amazon and Google cloud services. Article Relay Graph Bridge Graph
2018-03-28 to present	Chad	Chad blocks social messaging apps. Article Graph

Tor Blog & Tor Bugtracker

- Many censorship events not automatically measured
- Tor advocates, developers, users report inconsistency
- `https://blog.torproject.org/`
- `https://gitlab.torproject.org/`

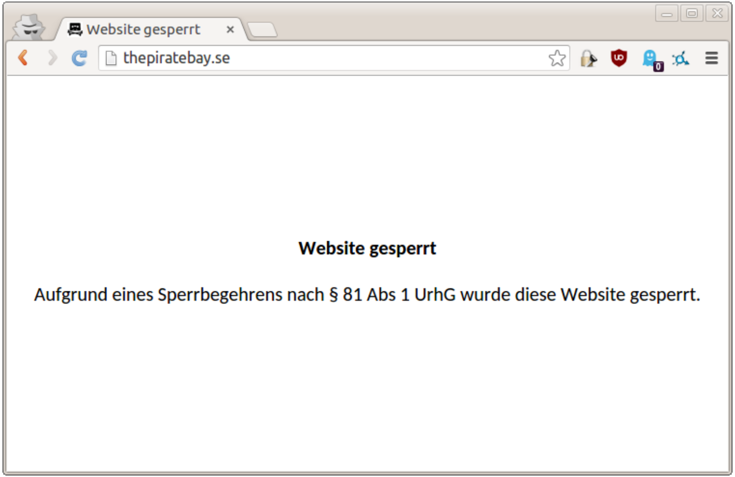
Censorship Events Worldwide

Austria

Piratebay in Austria:

- Court ordered to block access to thepiratebay.se, isohunt.to, 1337x.to and h33t.to in summer 2015
- DNS-based filter
- Slightly different behavior
- First case of its kind in .at

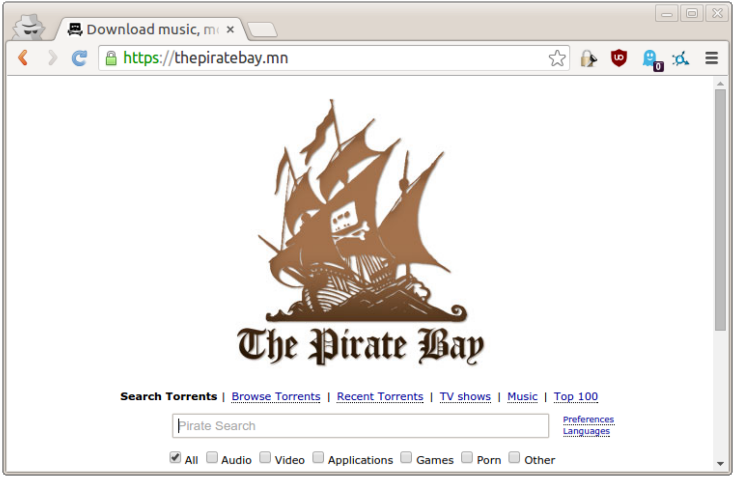
Austria



Website gesperrt

Aufgrund eines Sperrbegehrens nach § 81 Abs 1 UrhG wurde diese Website gesperrt.

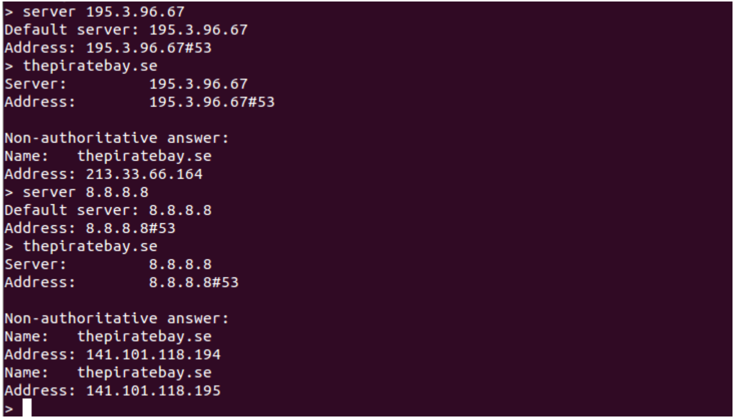
Austria



Search Torrents | Browse Torrents | Recent Torrents | TV shows | Music | Top 100

☑ All □ Audio □ Video □ Applications □ Games □ Porn □ Other

Austria

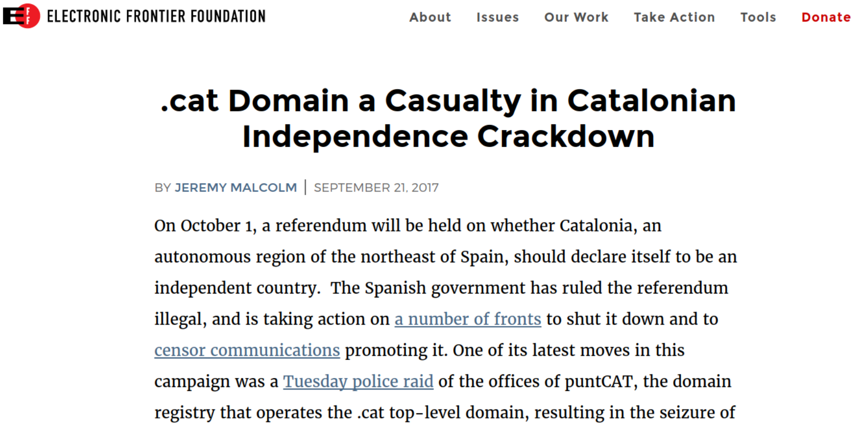


```
> server 195.3.96.67
Default server: 195.3.96.67
Address: 195.3.96.67#53
> thepiratebay.se
Server:         195.3.96.67
Address:        195.3.96.67#53

Non-authoritative answer:
Name:   thepiratebay.se
Address: 213.33.66.164
> server 8.8.8.8
Default server: 8.8.8.8
Address: 8.8.8.8#53
> thepiratebay.se
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   thepiratebay.se
Address: 141.101.118.194
Name:   thepiratebay.se
Address: 141.101.118.195
> 
```

Catalonia

- Region of Spain, wants autonomy
- Referendum October 1st 2017
- Internet Censorship
- 34C3 Talk
- OONI Report

Catalonia



.cat Domain a Casualty in Catalonian Independence Crackdown

BY JEREMY MALCOLM | SEPTEMBER 21, 2017

On October 1, a referendum will be held on whether Catalonia, an autonomous region of the northeast of Spain, should declare itself to be an independent country. The Spanish government has ruled the referendum illegal, and is taking action on a number of fronts to shut it down and to censor communications promoting it. One of its latest moves in this campaign was a Tuesday police raid of the offices of puntCAT, the domain registry that operates the .cat top-level domain, resulting in the seizure of

Source: EFF, 2017

Catalonia

- Website(s) shutdown: referendum.cat, …
- Website blocks (… any kind of information about the referendum)
- OONI: 25 website blocked (other numbers up to 140)
- Shutdown of Fundacio .cat (Arrested director)
- DNS tampering
- HTTP blocking
- DPI

Catalonia

- First mirrors installed: censored
- Massive amounts of mirrors (100+) / Onion Services
- DPI filter bypassing/ state bypassing (Sleep 10)
- Polling station blocked: Cell phones, New IP per phone
- Circumvention: Use of Tor, Signal, VPN, …

Turkey

Turkey vs. Google:

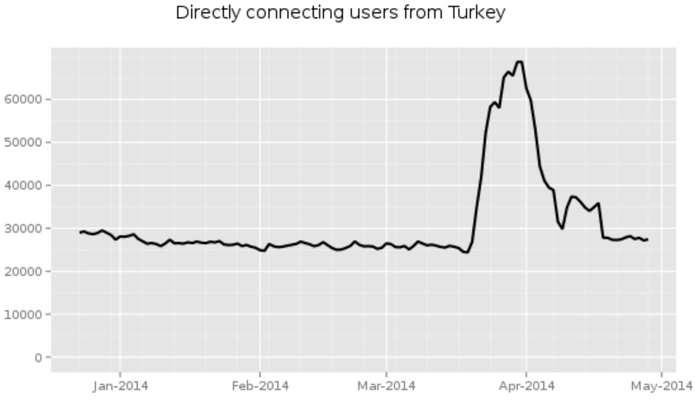
- Youtube filtered 2007-2010
- direct IP or alternative DNS servers possible
- even though blocked it was in the Top 10, according to Alexa
- after that again and again blocked for a short time

Turkey

March 2014:

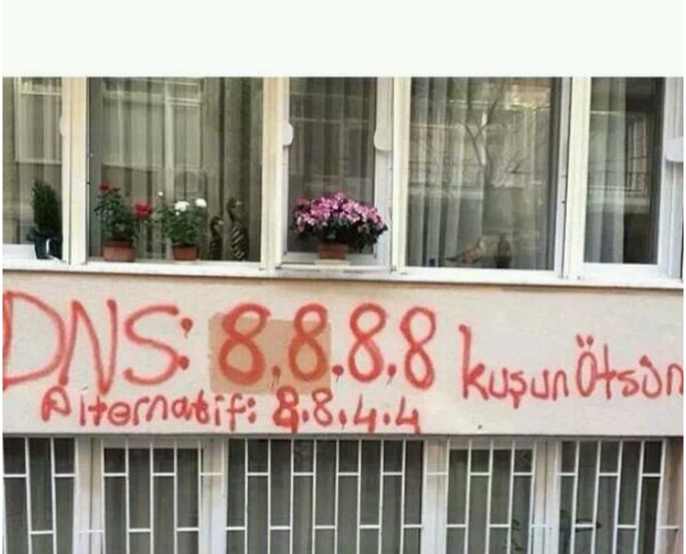
- recorded phone conversation spreads via social media
- president Erdogan wants to “eradicate Twitter”
- additionally Google DNS hijacking (8.8.8.8) & redirection
- VPN and Tor were used to bypass censorship

Turkey



The Tor Project - https://metrics.torproject.org/

Turkey



Great Firewall of China

Project “Golden shield”

- For censorship and surveillance
- “Chinas intranet”
- First with large-scale use of TCP RST
- Triggered by URL, keywords, Tor connections, TLS, …

Great Firewall of China

Towards a Comprehensive Picture of the Great Firewall's DNS Censorship[16]:

- Located at the network border to China
- Prevents open resolvers like 8.8.8.8
- Word list contains approx. 15.000 words
- One cluster sends approx. 2.800 responses per second
- Has about 350 processes

[16] Source: Anonymous, FOCI'14

Great Firewall of China

“GreenDam”:

- Filter software for Windows,
- First Mandatory then voluntarily, in particular schools and Internet cafes
- URL filter & text filter

“Dam Burst”

- Jon Obereide, Defcon 18
- Injected Dam Burst & removed Green Dam
- Without admin permissions!

Great Firewall of China

Evading not so easy anymore:

- DPI on encryption (HTTPS, SSL, SSH, VPN, ...)
- Tor Bridges semi-blocked
- *meek*

Countermeasures & Circumvention

Simple: Alternative DNS servers

- Google: 8.8.8.8, 8.8.4.4
- Cloudflare: 1.1.1.1, 1.0.0.1
- OpenDNS: 208.67.222.222, 208.67.220.220
- Or just use the IP!
- DoH & DoT!

VPN

- Often sufficient
- Usage is not hidden
- Popular VPN endpoints will get blocked eventually
- Encrypted data can be blocked using DPI

Circumvention concepts

- Overblocking
- Underblocking
- Too much collateral damage?
- Many circumvention approaches utilize this
- Or: many false positive

Domain Fronting

- Communicate with forbidden host[17]
- Hide remote endpoint in HTTP Host
- Appears to be allowed host in TLS SNI
- User -(TLS)- Allowed CDN -(HTTP)- Forbidden Host
- Blocking of CDN is expensive collateral damage
- Used in Tor, Telegram, Signal, ...

[17] Source: Fifield et al., PETS 2015

Domain Fronting cont.

- April 2018, Domain Fronting Disabled
- Google and Amazon
- ”now largely non-viable”[18]
- Domain Fronting/Hiding with TLS1.3

[18] Moxie Marlinspike

Tor

- Perfect against (DPI-)filter and IP-based blocks
- Often easier and simpler to use compared to VPNs
- (Private) bridges on the network
- Pluggable transports against DPI

Pluggable Transports

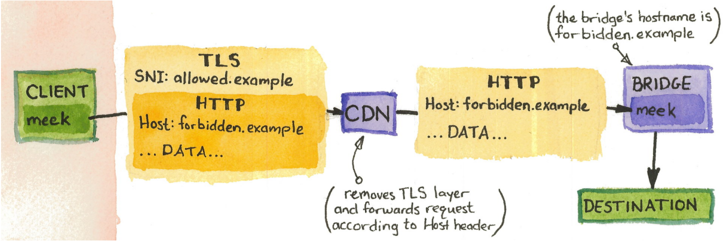
obfsproxy

- Mimics communication to other protocols
- Between Tor client & bridge

Problems

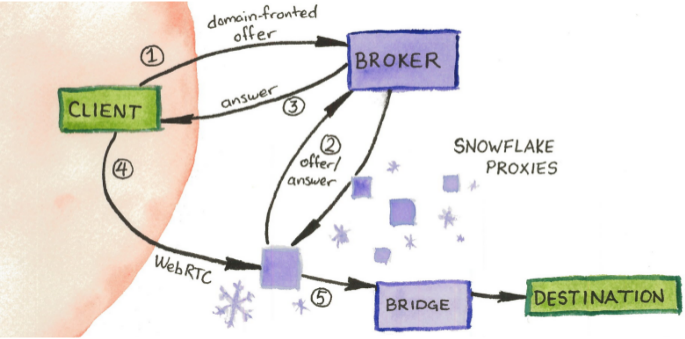
- Mimiced protocols are easy to discover
- Easy to find specific distinguish features

Meek



Source: https://www.bamsoftware.com/papers/thesis/

Snowflake



Source: https://trac.torproject.org/projects/tor/attachment/wiki/doc/Snowflake/snowflake-schematic.png

Censorship Circumvention

Just tip of the iceberg:

- Telex
- Message in a Bottle
- Flashproxy
- Facet
- TapDance
- CovertCast
- Paper: Tschantz et al. SoK: Towards Grounding Censorship Circumvention in Empiricism, S&P 2016

Censorship Circumvention

However:

- Costs of maintaining the systems
- Usability of systems
- Pace of arms race not analyzed

Censorship Literature

Complete (academic) overview:

- Censorbib by Philipp Winter

Free and Open Communications on the Internet

- up to FOCI'20
- FOCI'24

Questions?