Global Measurement of DNS Manipulation

Paul Pearce

Ben Jones, Frank Li, Roya Ensafi,
Nick Feamster, Nick Weaver, and Vern Paxson
Censorship

China’s scary lesson to the world: Censoring the Internet works

BEHIND THE FIREWALL: How China tamed the Internet | This is part of a series examining the impact of China’s Great Firewall, a mechanism of Internet censorship and surveillance that affects nearly 700 million users.

By Simon Denyer  May 23, 2018

Global Measurement of DNS Manipulation  Paul Pearce
Censorship

China’s scary lesson to the world: Censoring the Internet works

Turkey just banned Wikipedia, labeling it a ‘national security threat’
Censorship

Internet freedom has declined for the sixth consecutive year, with more governments than ever before targeting social media and communication apps as a means of halting the rapid dissemination of information, particularly during anti-government protests.

The increased controls show the importance of social media and online communication for advancing political freedom and social justice. It is no coincidence that the tools at the center of the current crackdown have been widely used to hold governments accountable and facilitate uncensored conversations. Authorities in several countries have even resorted to shutting down all internet access at politically contentious times, solely to prevent users from disseminating information through social media.
Understanding Censorship

• Despite prevalence, existing empirical measurement is sparse across:
  • Time
  • Space
  • Content

• Why? Deployed state of the art: Volunteers

• We argue: Continuous, diverse measurement needed to understand the scope, scale, and evolution of Internet censorship
Our Work

- Censorship techniques vary
  - This work \( \rightarrow \) DNS manipulation

- Measurement Goals:
  - Diverse
  - Longitudinal
  - Does not require participation
  - Ethical

- Design, implement, and deploy Iris, a system to identify DNS manipulation globally

- Global measurement study
  - Identifies pervasiveness of manipulation worldwide
  - Heterogeneity across content, countries, and resolvers
  - Heterogeneity within countries
Approach

• Conceptually simple:
  • Issue DNS queries for sensitive across globally diverse vantage points
  • Look for “wrong” responses

• Challenge 1: Vantage points
  • → Open DNS resolvers

• Challenge 2: Ethics
  • → Identify “Infrastructure” DNS resolvers

• Challenge 3: Repeatable
  • → Design of Iris

• Challenge 4: Identifying “wrong” responses?
  • → Consistency and independent verifiability of structural elements
Ethics

- Guided by ideals laid out by the Menlo Report:
  - Respect for persons
  - Beneficence
  - Respect for law and public

- Only use resolvers *reasonably* attributed to Internet naming infrastructure

- Heavily rate limit queries to resolvers and domains
Finding Infrastructure Resolvers
Finding Infrastructure Resolvers

Internet Scanning

ZMap

DNS Probe Module

The Internet

Global Measurement of DNS Manipulation

Paul Pearce
Finding Infrastructure Resolvers
Finding Infrastructure Resolvers

Internet Scanning
- ZMap
- DNS Probe Module
- The Internet

Filter
- Examine Answers
- Output

Reverse DNS
- ZDNS
- PTR Lookups
- The Internet
Finding Infrastructure Resolvers

Internet Scanning
- ZMap
- DNS Probe Module
- The Internet

Filter
- Examine Answers
- Output

Reverse DNS
- ZDNS
- PTR Lookups
- The Internet

Identify Infrastructure
- Find Nameservers
- Output

Global Measurement of DNS Manipulation

Paul Pearce
What to Measure

• Sensitive
  • All domains from the Citizen Lab sensitive test list

• Popular
  • Random subset of Alexa top 10,000

• Feed these artifacts into the Iris pipeline
  • Output → DNS manipulation
Iris Pipeline
Iris Pipeline

Measurement Artifacts

Input

- Infrastructure Resolvers
- Sensitive and Popular Domains
Iris Pipeline

**Measurement Artifacts**
- Infrastructure Resolvers
- Sensitive and Popular Domains

**Global DNS Resolutions**
- DNS Scanner
  - Internet-wide Lookups
  - Infras. Resolvers
At this point:
We have all DNS responses
Iris Pipeline

Measurement Artifacts
- Input
  - Infrastructure Resolvers
  - Sensitive and Popular Domains

Global DNS Resolutions
- DNS Scanner
  - Internet-wide Lookups
  - Infras. Resolvers

Annotate Results
- Tag IPs
  - Censys
  - Maxmind
Iris Pipeline

Measurement Artifacts
- Input
  - Infrastructure Resolvers
  - Sensitive and Popular Domains

Global DNS Resolutions
- DNS Scanner
- Internet-wide Lookups
- Infras. Resolvers

Annotate Results
- Tag IPs
- Censys
- Maxmind

Secondary Scanning
- Tag IPs
- PTR and SNI Certificates
- The Internet
Iris Pipeline

**Measurement Artifacts**
- Input: Infrastructure Resolvers
- Sensitive and Popular Domains

**Global DNS Resolutions**
- DNS Scanner
  - Internet-wide Lookups
  - Infras. Resolvers

**Annotate Results**
- Tag IPs
  - Censys
  - Maxmind

**Secondary Scanning**
- Tag IPs
  - PTR and SNI Certificates
  - The Internet

**Identify Wrong**
- Structural Elements
  - Controls

Global Measurement of DNS Manipulation

Paul Pearce
Iris Pipeline

Challenge 4: Identifying wrong responses

Measurement Artifacts
- Input: Infrastructure Resolvers
- Sensitive and Popular Domains

Global DNS Resolutions
- DNS Scanner: Internet-wide Lookups
- Infras. Resolvers

Annotate Results
- Tag IPs
- Censys
- Maxmind

Secondary Scanning
- Tag IPs: PTR and SNI Certificates
- The Internet

Identify Wrong
- Structural Elements
- Controls

Global Measurement of DNS Manipulation
Paul Pearce
Identifying Wrong Responses

• Intuition: Shared structural elements, even in global deployments

• Approach: structure consistency and independent verifiability

• Consistency
  • 4, uncensored, geographically diverse controls
  • Compare each answer with the control set

• Independent Verifiability
  • Valid HTTPS certificate, with and without SNI

• If any metric consistent/verifiable, response is correct
Iris Pipeline

Measurement Artifacts
- Input
  - Infrastructure Resolvers
  - Sensitive and Popular Domains

Global DNS Resolutions
- DNS Scanner
  - Internet-wide Lookups
  - Infras. Resolvers

Annotate Results
- Tag IPs
  - Censys
  - Maxmind

Secondary Scanning
- Tag IPs
  - PTR and SNI Certificates
  - The Internet

Identify Wrong
- Structural Elements
- Controls

Challenge 4: Identifying wrong responses
Iris Pipeline

Measurement Artifacts
- Input
  - Infrastructure Resolvers
  - Sensitive and Popular Domains

Global DNS Resolutions
- DNS Scanner
  - Internet-wide Lookups
  - Infras. Resolvers

Annotate Results
- Tag IPs
  - Censys
  - Maxmind
  - The Internet

Secondary Scanning
- Tag IPs
  - PTR and SNI Certificates

Identify Wrong
- Structural Elements
- Controls

Global Measurement of DNS Manipulation
Paul Pearce
Global Measurement of DNS Manipulation

Iris Pipeline

Measurement Artifacts
- Input: Infrastructure Resolvers
- Input: Sensitive and Popular Domains

Global DNS Resolutions
- DNS Scanner: Internet-wide Lookups
- Infras. Resolvers

Annotate Results
- Tag IPs
- Censys
- Maxmind

Secondary Scanning
- Tag IPs
- PTR and SNI Certificates
- The Internet

Identify Wrong
- Structural Elements
- Controls

Results
- Output: Correct Answers
- Output: Incorrect Answers
Measurement Study and Dataset

• What is the open resolver population?

• How much does our ethical framework reduce coverage?

• What is the total set of DNS responses we examine?

• What does our dataset reveal?

<table>
<thead>
<tr>
<th>Resolver Dataset</th>
<th>Number Resolvers</th>
<th>Number Countries</th>
<th>Median / Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Open</td>
<td>4.2M</td>
<td>232</td>
<td>660</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number Resolvers</th>
<th>Number Domains</th>
<th>Total Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>6,564</td>
<td>2,330</td>
<td>14.5M</td>
</tr>
</tbody>
</table>
Manipulation By Country

• What countries experience the most manipulation?
Manipulation By Country

- What **countries** experience the most manipulation?
  - Qualitatively consistent with prior work

<table>
<thead>
<tr>
<th>Country</th>
<th>Median Manipulated</th>
<th>Number Resolvers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iran</td>
<td>6.02%</td>
<td>122</td>
</tr>
<tr>
<td>China</td>
<td>5.22%</td>
<td>62</td>
</tr>
<tr>
<td>Indonesia</td>
<td>0.63%</td>
<td>80</td>
</tr>
<tr>
<td>Greece</td>
<td>0.28%</td>
<td>62</td>
</tr>
<tr>
<td>Mongolia</td>
<td>0.17%</td>
<td>6</td>
</tr>
<tr>
<td>Iraq</td>
<td>0.09%</td>
<td>7</td>
</tr>
<tr>
<td>Bermuda</td>
<td>0.04%</td>
<td>2</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>0.04%</td>
<td>14</td>
</tr>
<tr>
<td>Belarus</td>
<td>0.04%</td>
<td>18</td>
</tr>
</tbody>
</table>
Manipulation By Country

- What **countries** experience the most manipulation?
  - Qualitatively consistent with prior work

- Are there outliers within countries?

<table>
<thead>
<tr>
<th>Country</th>
<th>Median Manipulated</th>
<th>Number Resolvers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iran</td>
<td>6.02%</td>
<td>122</td>
</tr>
<tr>
<td>China</td>
<td>5.22%</td>
<td>62</td>
</tr>
<tr>
<td>Indonesia</td>
<td>0.63%</td>
<td>80</td>
</tr>
<tr>
<td>Greece</td>
<td>0.28%</td>
<td>62</td>
</tr>
<tr>
<td>Mongolia</td>
<td>0.17%</td>
<td>6</td>
</tr>
<tr>
<td>Iraq</td>
<td>0.09%</td>
<td>7</td>
</tr>
<tr>
<td>Bermuda</td>
<td>0.04%</td>
<td>2</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>0.04%</td>
<td>14</td>
</tr>
<tr>
<td>Belarus</td>
<td>0.04%</td>
<td>18</td>
</tr>
</tbody>
</table>
## Manipulation By Country

- **What countries** experience the most manipulation?
  - Qualitatively consistent with prior work

- **Are there outliers within countries?**
  - High outliers
    - → localized manipulation

<table>
<thead>
<tr>
<th>Country</th>
<th>Median Manipulated</th>
<th>Number Resolvers</th>
<th>Max Manipulated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iran</td>
<td>6.02%</td>
<td>122</td>
<td>22.41%</td>
</tr>
<tr>
<td>China</td>
<td>5.22%</td>
<td>62</td>
<td>8.40%</td>
</tr>
<tr>
<td>Indonesia</td>
<td>0.63%</td>
<td>80</td>
<td>9.95%</td>
</tr>
<tr>
<td>Greece</td>
<td>0.28%</td>
<td>62</td>
<td>0.83%</td>
</tr>
<tr>
<td>Mongolia</td>
<td>0.17%</td>
<td>6</td>
<td>0.36%</td>
</tr>
<tr>
<td>Iraq</td>
<td>0.09%</td>
<td>7</td>
<td>5.79%</td>
</tr>
<tr>
<td>Bermuda</td>
<td>0.04%</td>
<td>2</td>
<td>0.09%</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>0.04%</td>
<td>14</td>
<td>3.90%</td>
</tr>
<tr>
<td>Belarus</td>
<td>0.04%</td>
<td>18</td>
<td>0.30%</td>
</tr>
</tbody>
</table>
Manipulation By Country

• What **countries** experience the most manipulation?
  • Qualitatively consistent with prior work

• Are there outliers within countries?
  • High outliers
    • → localized manipulation
  • Low outliers
    • → geolocation error

<table>
<thead>
<tr>
<th>Country</th>
<th>Median Manipulated</th>
<th>Number Resolvers</th>
<th>Max Manipulated</th>
<th>Min Manipulated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iran</td>
<td>6.02%</td>
<td>122</td>
<td>22.41%</td>
<td>0%</td>
</tr>
<tr>
<td>China</td>
<td>5.22%</td>
<td>62</td>
<td>8.40%</td>
<td>0%</td>
</tr>
<tr>
<td>Indonesia</td>
<td>0.63%</td>
<td>80</td>
<td>9.95%</td>
<td>0%</td>
</tr>
<tr>
<td>Greece</td>
<td>0.28%</td>
<td>62</td>
<td>0.83%</td>
<td>0%</td>
</tr>
<tr>
<td>Mongolia</td>
<td>0.17%</td>
<td>6</td>
<td>0.36%</td>
<td>0%</td>
</tr>
<tr>
<td>Iraq</td>
<td>0.09%</td>
<td>7</td>
<td>5.79%</td>
<td>0%</td>
</tr>
<tr>
<td>Bermuda</td>
<td>0.04%</td>
<td>2</td>
<td>0.09%</td>
<td>0%</td>
</tr>
<tr>
<td>Kazakhstan</td>
<td>0.04%</td>
<td>14</td>
<td>3.90%</td>
<td>0%</td>
</tr>
<tr>
<td>Belarus</td>
<td>0.04%</td>
<td>18</td>
<td>0.30%</td>
<td>0%</td>
</tr>
</tbody>
</table>
Manipulation By Domain

• What **domains** are most frequently manipulated?
Manipulation By Domain

- **What domains** are most frequently manipulated?
  - Gambling and Pornography
  - → 8 of top 10

<table>
<thead>
<tr>
<th>Rank</th>
<th>Domain</th>
<th>Category</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="http://www.pokerstars.com">www.pokerstars.com</a></td>
<td>Gambling</td>
<td>19</td>
</tr>
<tr>
<td>2</td>
<td>betway.com</td>
<td>Gambling</td>
<td>19</td>
</tr>
<tr>
<td>3</td>
<td>pornhub.com</td>
<td>Pornography</td>
<td>19</td>
</tr>
<tr>
<td>4</td>
<td>youporn.com</td>
<td>Pornography</td>
<td>19</td>
</tr>
<tr>
<td>5</td>
<td>xvideos.com</td>
<td>Pornography</td>
<td>19</td>
</tr>
<tr>
<td>6</td>
<td>thepiratebay.org</td>
<td>P2P File Sharing</td>
<td>18</td>
</tr>
<tr>
<td>7</td>
<td>thepiratebay.se</td>
<td>P2P File Sharing</td>
<td>18</td>
</tr>
<tr>
<td>8</td>
<td>xhamster.com</td>
<td>Pornography</td>
<td>18</td>
</tr>
<tr>
<td>9</td>
<td><a href="http://www.partypoker.com">www.partypoker.com</a></td>
<td>Gambling</td>
<td>17</td>
</tr>
<tr>
<td>10</td>
<td>beeg.com</td>
<td>Pornography</td>
<td>17</td>
</tr>
</tbody>
</table>
Manipulation By Domain

• What **domains** are most frequently manipulated?
  • Gambling and Pornography
  • → 8 of top 10

• Are commonly measured sites the most frequent targets?
  (Anonymity tools, Twitter, Google)
  • No. They experience significantly less manipulation globally
  • → diversity in measured domains

<table>
<thead>
<tr>
<th>Rank</th>
<th>Domain</th>
<th>Category</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="http://www.pokerstars.com">www.pokerstars.com</a></td>
<td>Gambling</td>
<td>19</td>
</tr>
<tr>
<td>2</td>
<td>betway.com</td>
<td>Gambling</td>
<td>19</td>
</tr>
<tr>
<td>3</td>
<td>pornhub.com</td>
<td>Pornography</td>
<td>19</td>
</tr>
<tr>
<td>4</td>
<td>youporn.com</td>
<td>Pornography</td>
<td>19</td>
</tr>
<tr>
<td>5</td>
<td>xvideos.com</td>
<td>Pornography</td>
<td>19</td>
</tr>
<tr>
<td>6</td>
<td>thepiratebay.org</td>
<td>P2P File Sharing</td>
<td>18</td>
</tr>
<tr>
<td>7</td>
<td>thepiratebay.se</td>
<td>P2P File Sharing</td>
<td>18</td>
</tr>
<tr>
<td>8</td>
<td>xhamster.com</td>
<td>Pornography</td>
<td>18</td>
</tr>
<tr>
<td>9</td>
<td><a href="http://www.partypoker.com">www.partypoker.com</a></td>
<td>Gambling</td>
<td>17</td>
</tr>
<tr>
<td>10</td>
<td>beeg.com</td>
<td>Pornography</td>
<td>17</td>
</tr>
<tr>
<td>80</td>
<td>torproject.org</td>
<td>Anonymity &amp; Censorship</td>
<td>12</td>
</tr>
<tr>
<td>181</td>
<td>twitter.com</td>
<td>Twitter</td>
<td>9</td>
</tr>
<tr>
<td>250</td>
<td><a href="http://www.youtube.com">www.youtube.com</a></td>
<td>Google Video</td>
<td>8</td>
</tr>
<tr>
<td>495</td>
<td><a href="http://www.citizenlab.org">www.citizenlab.org</a></td>
<td>Freedom of Expression</td>
<td>4</td>
</tr>
<tr>
<td>606</td>
<td><a href="http://www.google.com">www.google.com</a></td>
<td>Google</td>
<td>3</td>
</tr>
</tbody>
</table>
Manipulation By Category

• What **categories** are most frequently manipulated?
Manipulation By Category

• What **categories** are most frequently manipulated?
  • Sites from the Alexa sampling experience widespread manipulation

  • While Gambling and Pornography individual domains were most common, they are not the most common categories

<table>
<thead>
<tr>
<th>Rank</th>
<th>Category</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alexa Top 10,000</td>
<td>36</td>
</tr>
<tr>
<td>2</td>
<td>Freedom of Expression</td>
<td>35</td>
</tr>
<tr>
<td>3</td>
<td>P2P File Sharing</td>
<td>34</td>
</tr>
<tr>
<td>4</td>
<td>Human Rights</td>
<td>31</td>
</tr>
<tr>
<td>5</td>
<td>Gambling</td>
<td>29</td>
</tr>
<tr>
<td>6</td>
<td>Pornography</td>
<td>29</td>
</tr>
<tr>
<td>7</td>
<td>Alcohol and Drugs</td>
<td>28</td>
</tr>
<tr>
<td>8</td>
<td>Anonymity &amp; Censorship</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>Hate Speech</td>
<td>22</td>
</tr>
<tr>
<td>10</td>
<td>Multimedia Sharing</td>
<td>21</td>
</tr>
</tbody>
</table>
Manipulation By Category

• What **categories** are most frequently manipulated?
  • Sites from the Alexa sampling experience widespread manipulation

• While Gambling and Pornography individual domains were most common, they are not the most common categories

• Are commonly measured sites the most frequent targets?
  • No

<table>
<thead>
<tr>
<th>Rank</th>
<th>Category</th>
<th>Countries</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alexa Top 10,000</td>
<td>36</td>
</tr>
<tr>
<td>2</td>
<td>Freedom of Expression</td>
<td>35</td>
</tr>
<tr>
<td>3</td>
<td>P2P File Sharing</td>
<td>34</td>
</tr>
<tr>
<td>4</td>
<td>Human Rights</td>
<td>31</td>
</tr>
<tr>
<td>5</td>
<td>Gambling</td>
<td>29</td>
</tr>
<tr>
<td>6</td>
<td>Pornography</td>
<td>29</td>
</tr>
<tr>
<td>7</td>
<td>Alcohol and Drugs</td>
<td>28</td>
</tr>
<tr>
<td>8</td>
<td>Anonymity &amp; Censorship</td>
<td>24</td>
</tr>
<tr>
<td>9</td>
<td>Hate Speech</td>
<td>22</td>
</tr>
<tr>
<td>10</td>
<td>Multimedia Sharing</td>
<td>21</td>
</tr>
<tr>
<td>20</td>
<td>Google (All)</td>
<td>16</td>
</tr>
<tr>
<td>34</td>
<td>Facebook (All)</td>
<td>10</td>
</tr>
<tr>
<td>38</td>
<td>Twitter (All)</td>
<td>9</td>
</tr>
</tbody>
</table>
Consistency Within Countries

• Is there heterogeneity within countries?
Consistency Within Countries

• Is there heterogeneity within countries?
Consistency Within Countries

- Is there heterogeneity within countries?
  - Yes: Modal effects $\rightarrow$ multiple systems, localized manipulation
Consistency Within Countries

• Is there heterogeneity within countries?
  • Yes: Modal effects $\rightarrow$ multiple systems, localized manipulation

• Is there non-determinism?
  • Yes: Smearing effects
Consistency Within Countries

• Is there heterogeneity within countries?
  • Yes: Modal effects $\rightarrow$ multiple systems, localized manipulation

• Is there non-determinism?
  • Yes: Smearing effects

• Is there ISP-level filtering?
  • Yes: Low-but-incomplete countries
Consistency Within Countries

• Is there heterogeneity within countries?
  • Yes: Modal effects → multiple systems, localized manipulation

• Is there non-determinism?
  • Yes: Smearing effects

• Is there ISP-level filtering?
  • Yes: Low-but-incomplete countries

• Is there geolocation error?
  • Yes: High-but-incomplete countries
Methodological Takeaways

- Domain selection is critical for comparative studies
  - List biases will influence ranking, comparisons

- Measurement of non-sensitive content is important
  - Lists at inherently limited

- How data is grouped influences results
  - Domain vs Category

- In-country diversity is necessary to accurately depict manipulation
  - Outliers both high and low
  - Heterogeneous manipulation
Conclusion and Next Steps

• Internet Censorship is prevalent and heterogeneous

• Iris is a ethical system to identify DNS manipulation Internet-wide

• We identified heterogeneity of censorship across multiple dimensions, including variance within countries, highlighting the need for tools such as Iris

• Next Steps: Use of Iris and other Internet-wide techniques for continuous longitudinal measurement
Thank You

@paul_pearce
pearce@berkeley.edu
https://cs.berkeley.edu/~pearce/