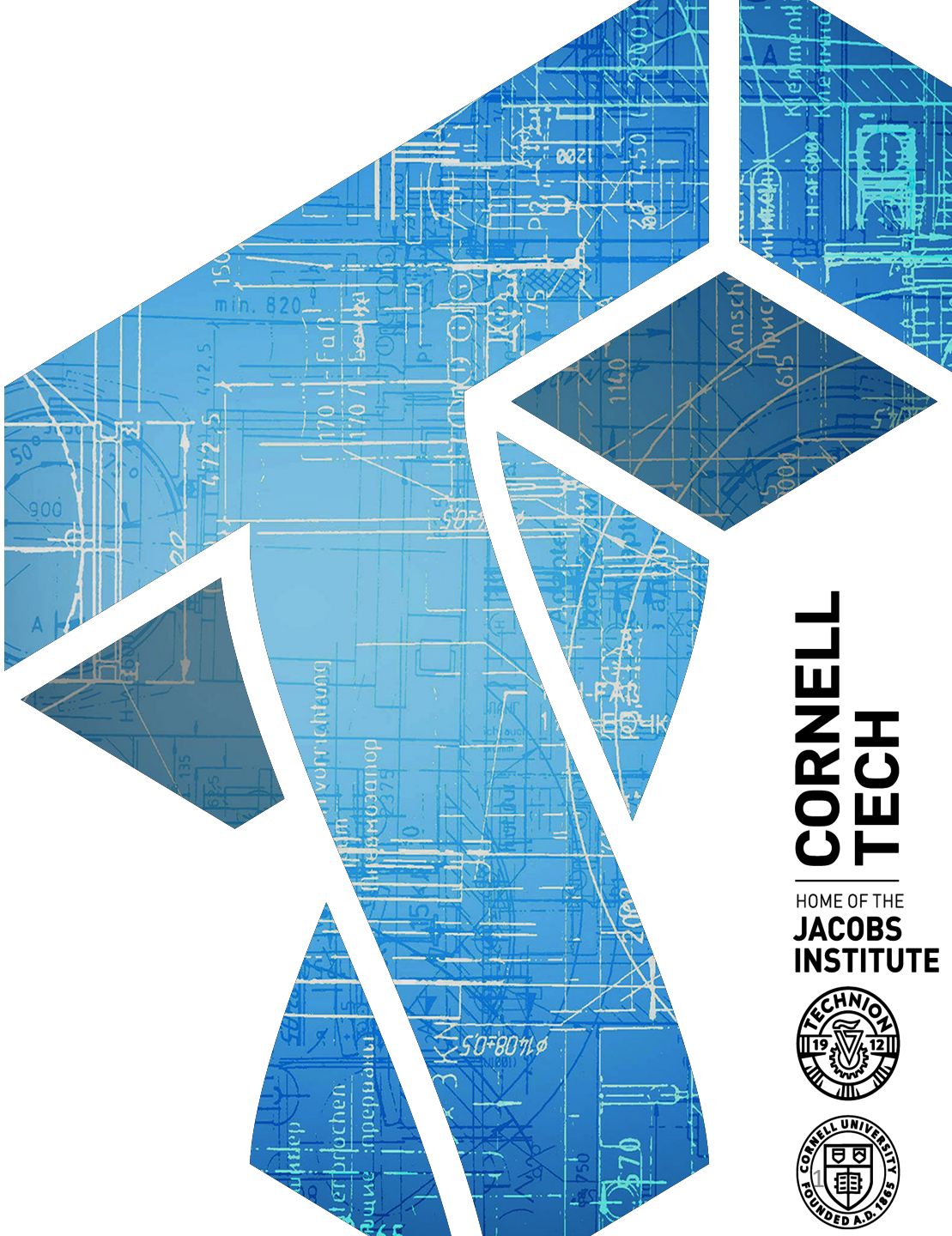
CS 6431: Internet censorship

Instructor: Tom Ristenpart

https://github.com/tomrist/cs6431-fall2021



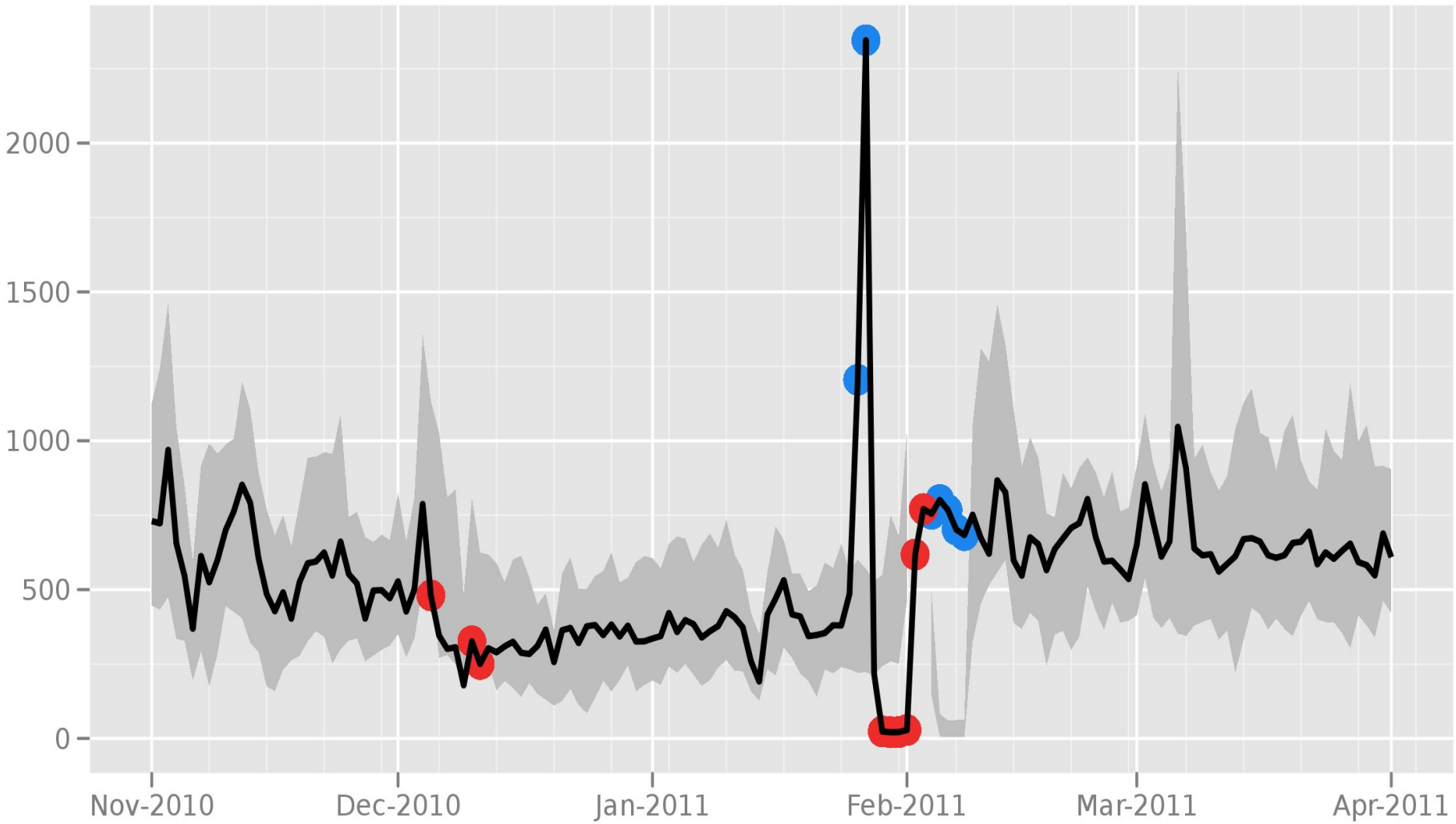
CORNELL TECH
HOME OF THE JACOBS INSTITUTE

Recap: Tor and anonymity online

- Onion routing bounces traffic between different nodes, with data encrypted in multiple layers
  - Hides client IP from server
  - Hides which clients talking to which servers (for some adversaries)
- Hidden services hide server IP address from clients/nodes

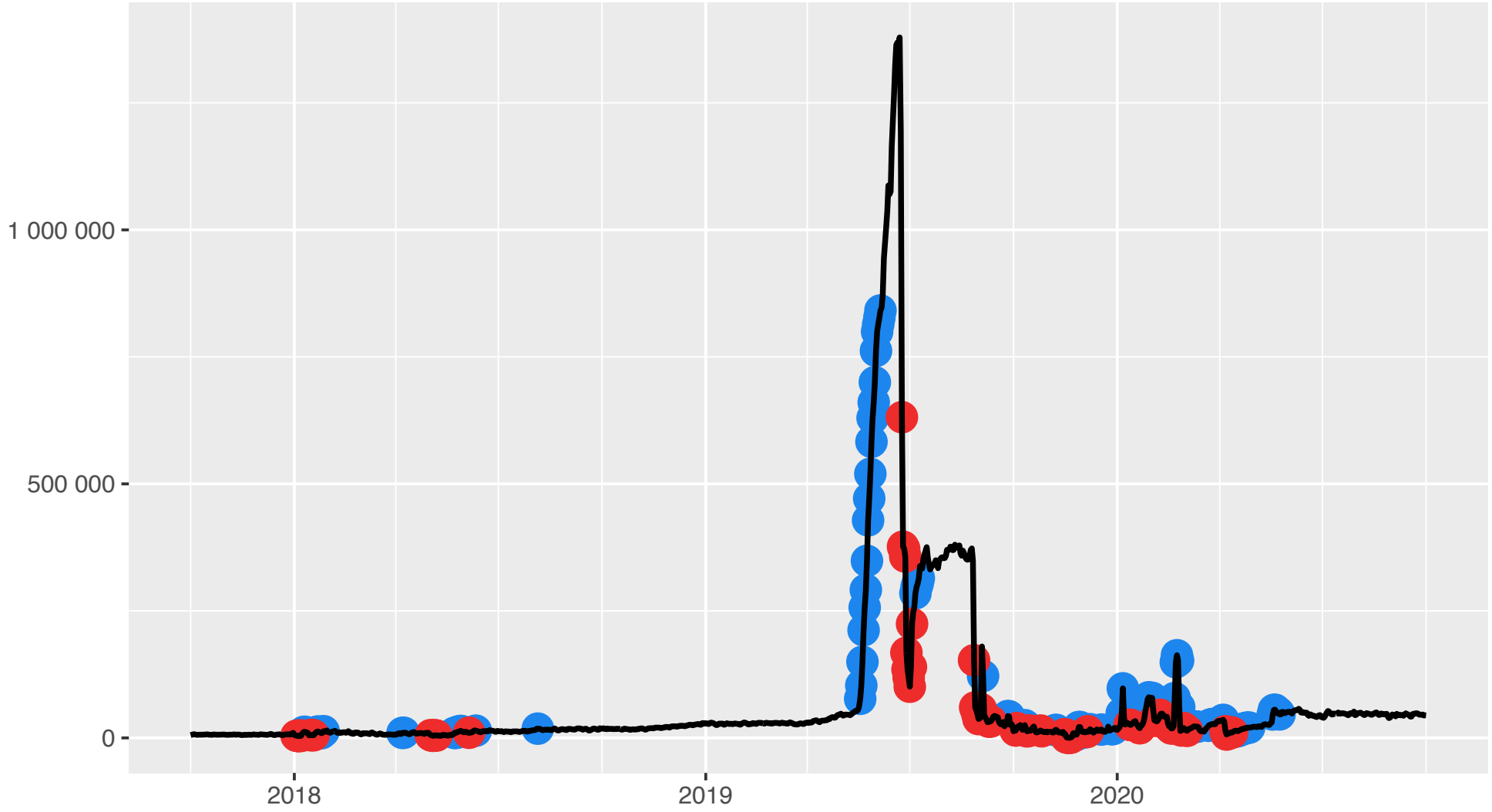
- High impact paper and system
- Tor has seen a lot of use for censorship circumvention

Directly connecting users from Egypt



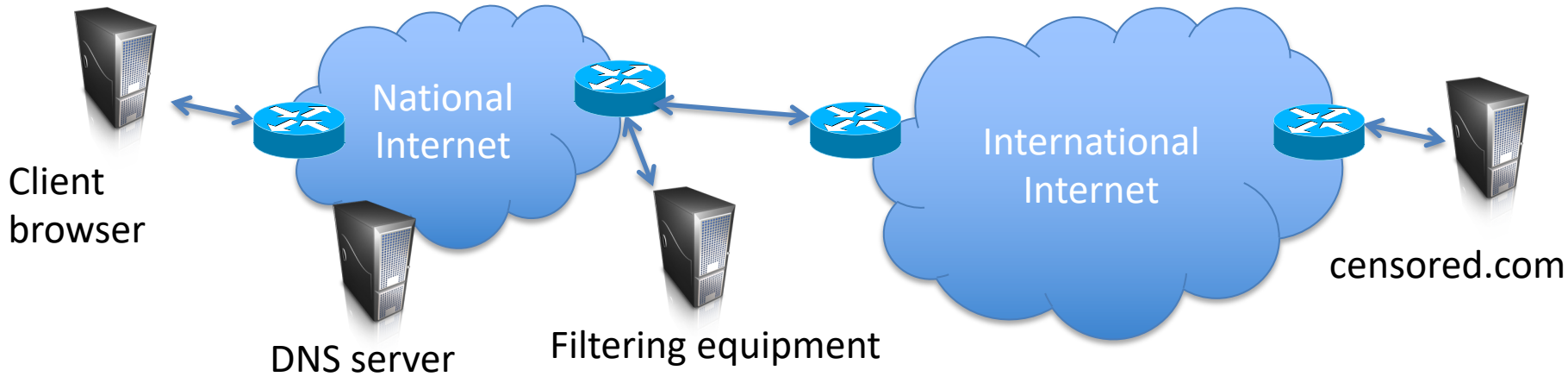
The Tor Project - https://metrics.torproject.org/

Directly connecting users from Iran



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

How would you censor web requests?



- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering (search keywords in TCP packets)
- Protocol filtering (detect Tor protocol)

Golden Shield Project

> “If you open the window for fresh air, you have to expect some flies to blow in” – Deng Xiaoping in 1980s

Started in 1997s. Most well-known aspect is “Great Firewall” of China:

- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering (search keywords in TCP packets)
- Protocol filtering
- Active probing of suspect destination IP addresses

Islamic Republic of Iran

- Every ISP must run “content-control software”
  - SmartFilter (up until 2009) made by USA company
  - Nokia Siemens deep-packet inspection (DPI) systems
- According to wikipedia: 50% of top 500 most popular websites blocked in Iran
- Occasional widespread filtering of Tor, TLS, other encrypted protcols
- Once in a while complete international Internet shutdown
  - 2019 Iranian protests

Censorship as two-step process

1. *Sensitive content identification*
   - DNS and IP blocklists
   - Keyword blocklists with DPI
   - Protocol identification (e.g., TLS)
   - Tool identification (e.g., Tor)

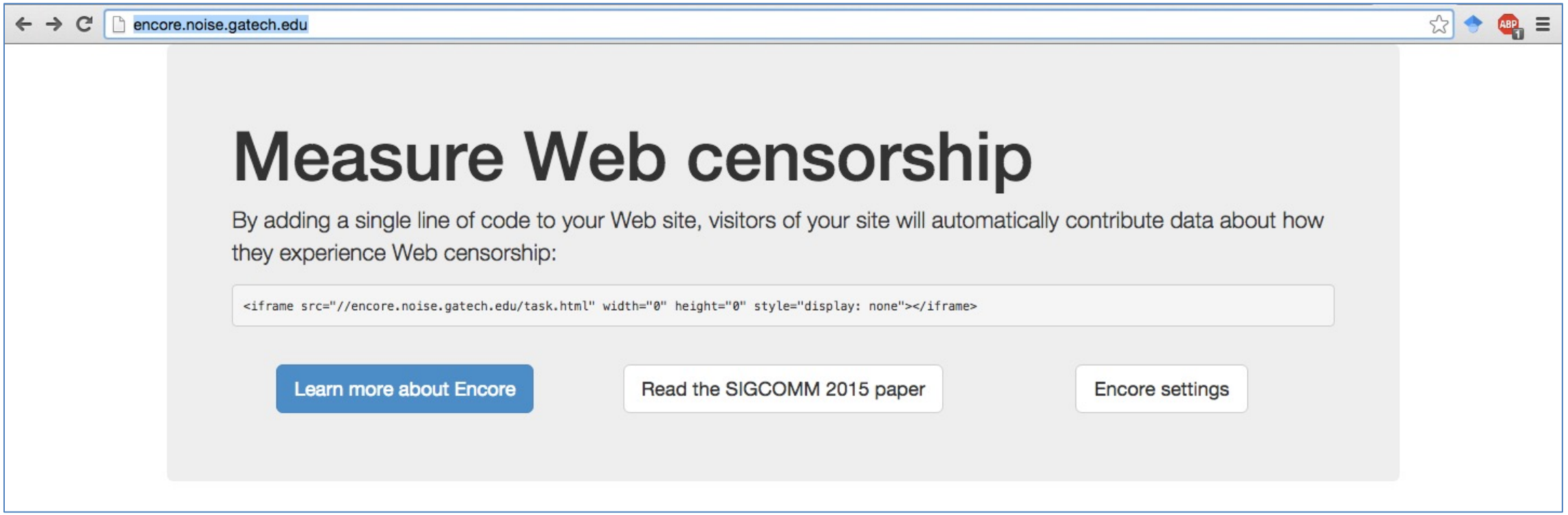
2. *Censoring action*
   - DNS poisoning
   - HTTP man-in-the-middle
   - TCP resets
   - Dropping packets

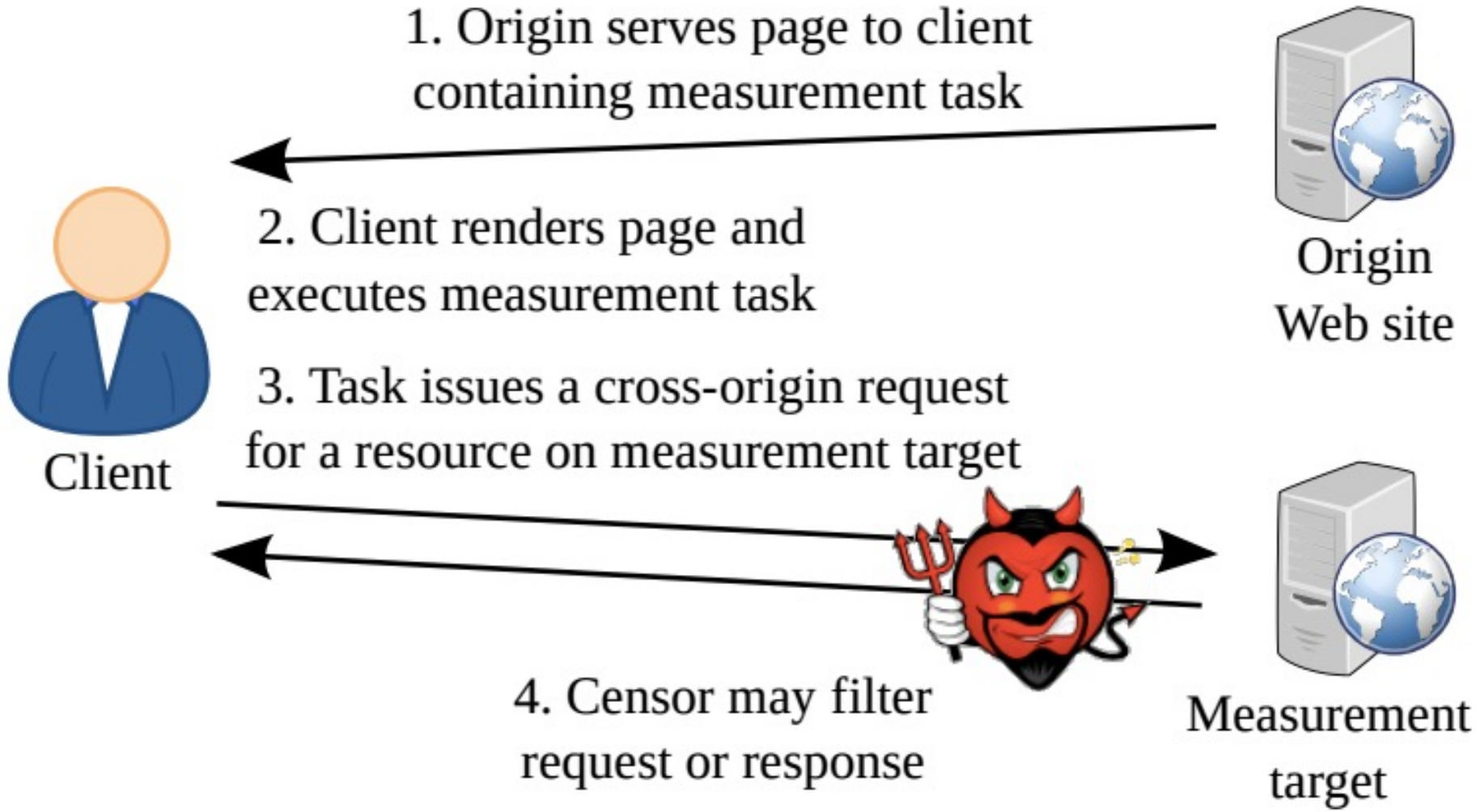
How would you measure censorship?

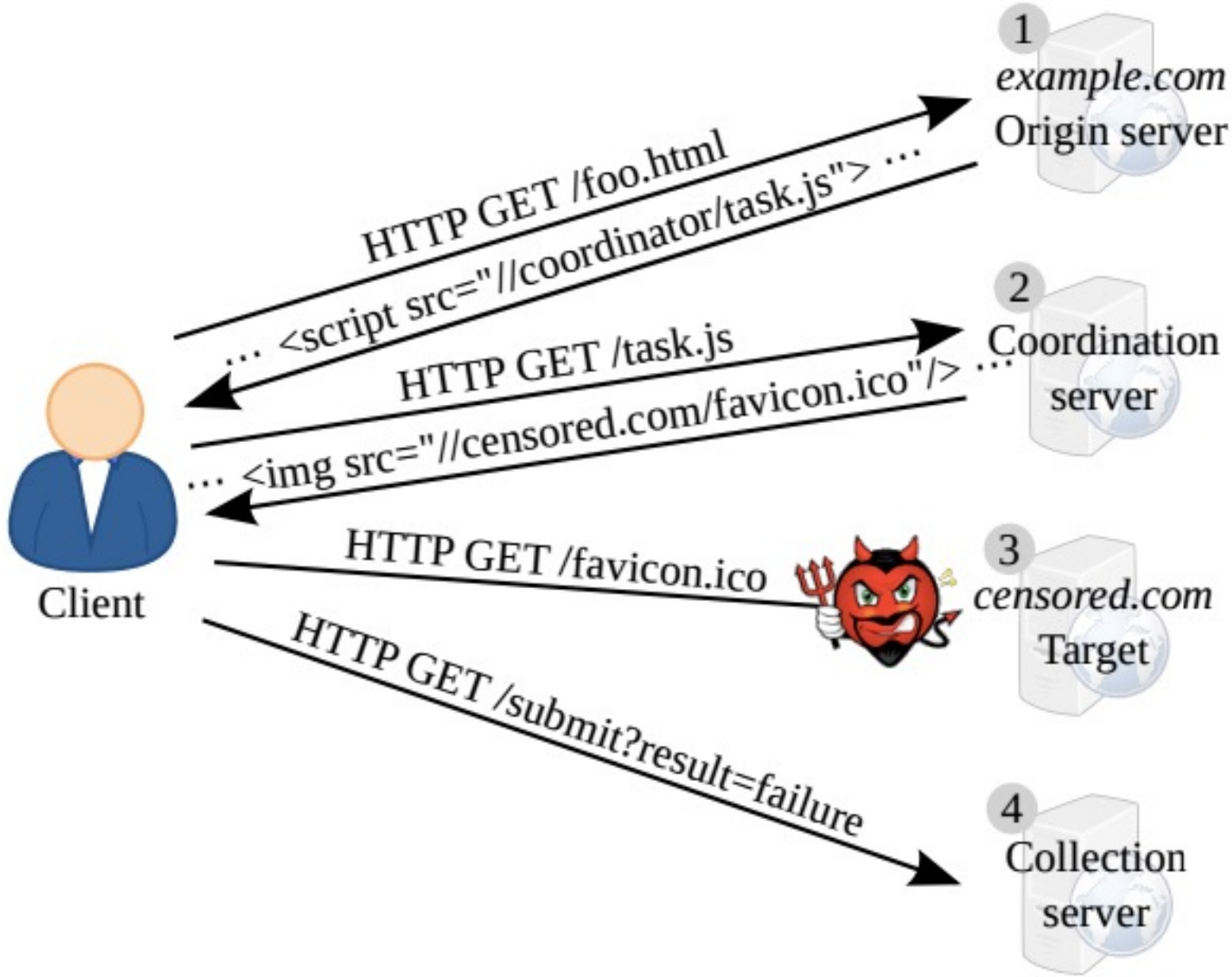
How do we know about censorship?

- Anecdotes from people within censored regions
- More formal surveys
- Network measurements:
  - Web sites aggregating info such as GreatFire
  - Herdict tool (browser plugin to manually report blockage)
  - Open Observatory of Network Interference (opt-in measurements of network connections)
  - Encore measurement paper [Burnett, Feamster 2015]

Encore measurement paper




1. Origin serves page to client
containing measurement task
Origin
Web site
2. Client renders page and
executes measurement task
3. Task issues a cross-origin request
for a resource on measurement target
Client
4. Censor may filter
request or response
Measurement
target


1
example.com
Origin server
HTTP GET /foo.html
… <script src="//coordinator/task.js"> …
2
Coordination server
HTTP GET /task.js
… …
Client
HTTP GET /favicon.ico
3
censored.com
Target
HTTP GET /submit?result=failure
4
Collection server

Encore measurement paper

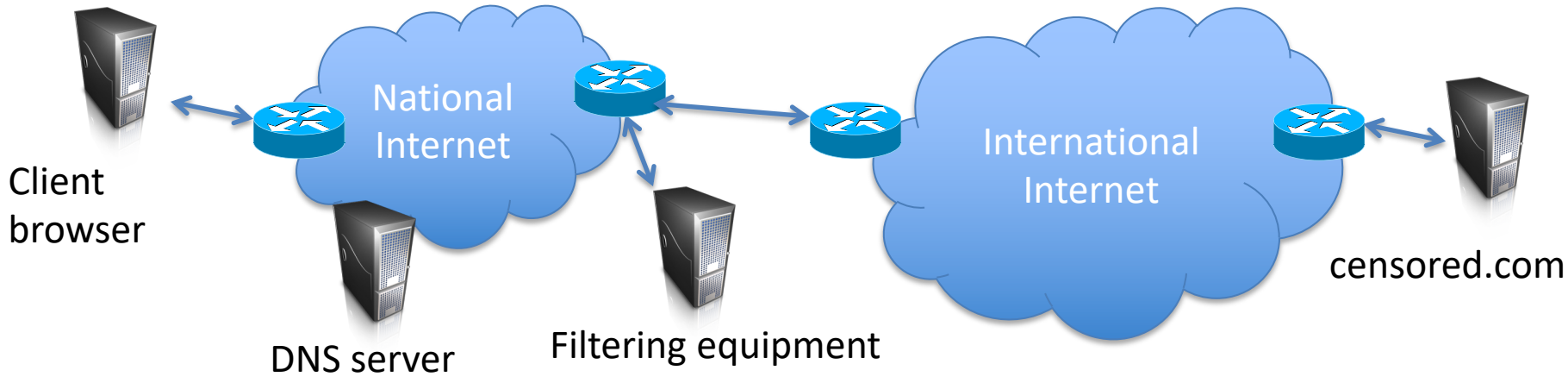
- Loads measurement task in iframe on other sites
- Automatically (try to) fetch content that may be censored

Deployed with >= 17 websites to obtain ~140k measurements. Confirmed blocking of:

- youtube.com in Pakistan, Iran, China
- Twitter.com, facebook.com in China, Iran

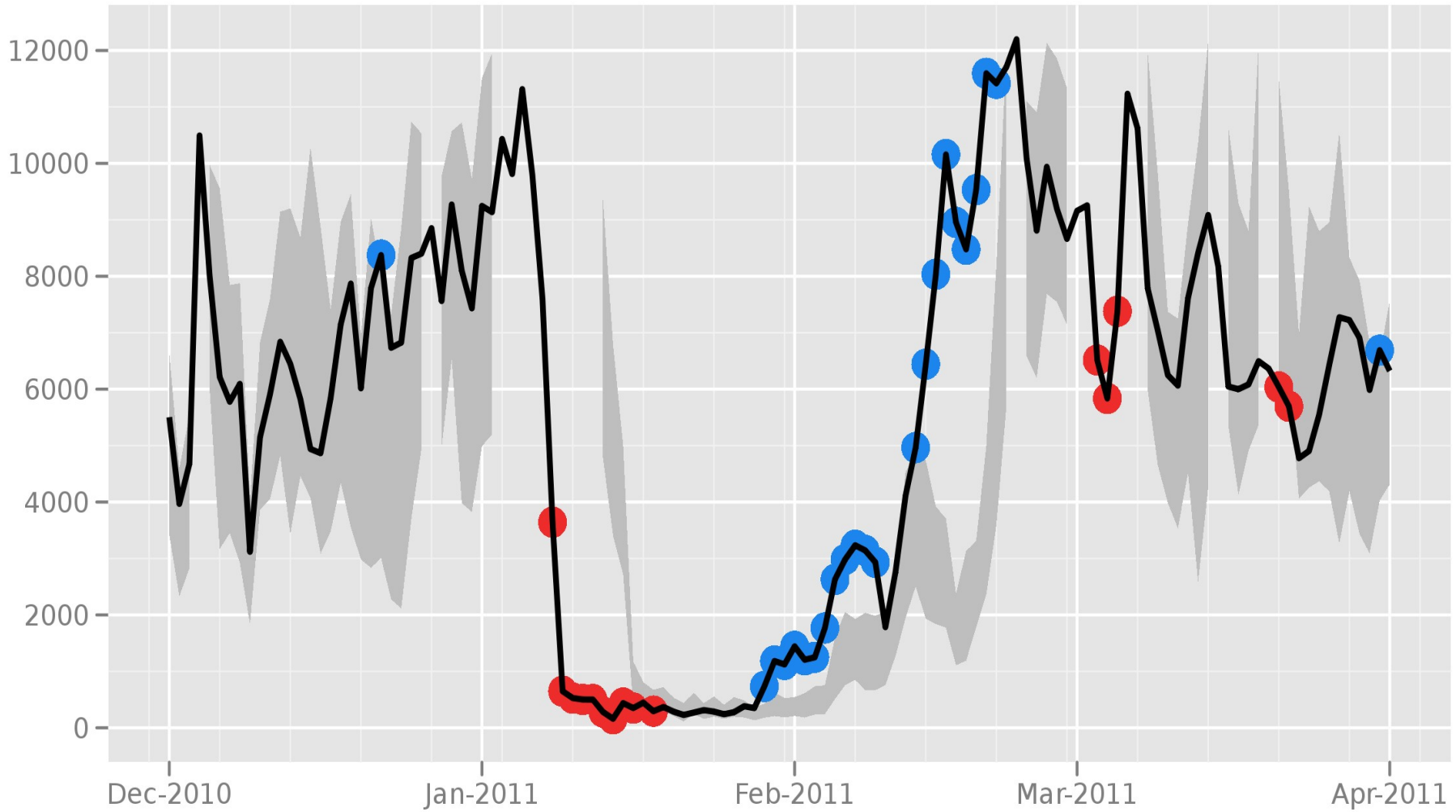
Statement from the SIGCOMM 2015 Program Committee: The SIGCOMM 2015 PC appreciated the technical contributions made in this paper, but found the paper controversial because some of the experiments the authors conducted raise ethical concerns. The controversy arose in large part because the networking research community does not yet have widely accepted guidelines or rules for the ethics of experiments that measure online censorship. In accordance with the published submission guidelines for SIGCOMM 2015, had the authors not engaged with their Institutional Review Boards (IRBs) or had their IRBs determined that their research was unethical, the PC would have rejected the paper without review. But the authors did engage with their IRBs, which did not flag the research as unethical. The PC hopes that discussion of the ethical concerns these experiments raise will advance the development of ethical guidelines in this area. It is the PC's view that future guidelines should include as a core principle that researchers should not engage in experiments that subject users to an appreciable risk of substantial harm absent informed consent. The PC endorses neither the use of the experimental techniques this paper describes nor the experiments the authors conducted.

How would you *avoid* censorship?



- IP filtering
- DNS filtering / redirection
- URL filtering
- Packet filtering (search keywords in TCP packets)
- Protocol filtering (detect Tor protocol)

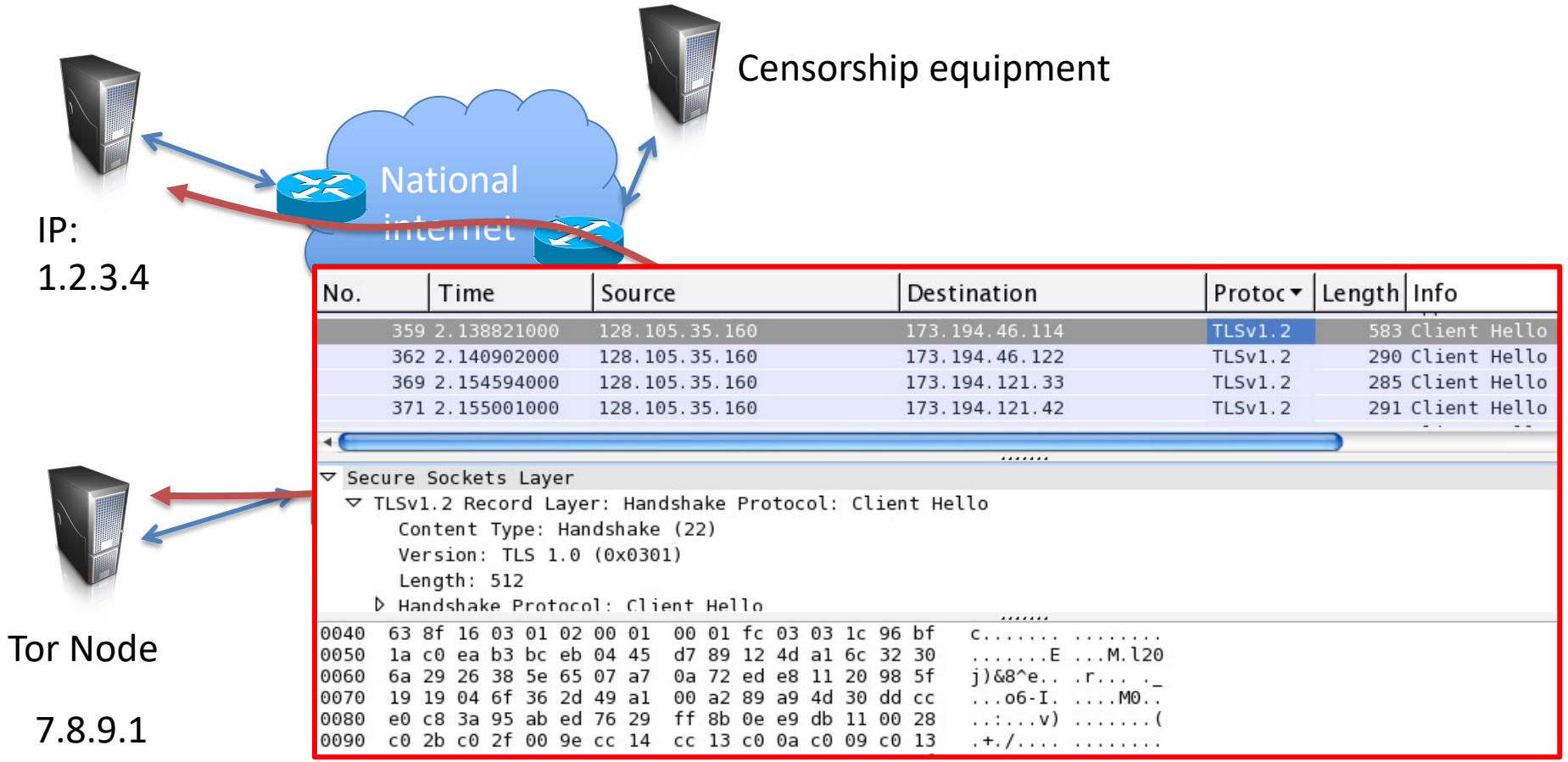
Directly connecting users from the Islamic Republic of Iran



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

Iran DPI blocking of Tor

- Tor point-to-point connections use TLS



TLS Handshake

Client

Server

Pick random Nc

ClientHello, MaxVer, Nc, Ciphers/CompMethods

Pick random Ns

ServerHello, Ver, Ns, SessionID, Cipher/CompMethod

Check CERT using CA public verification key

CERT = (pk of server, signature over it)

C

Pick random PMS
C <- E(pk,PMS)

PMS <- D(sk,C)

ChangeCipherSpec,
{ Finished, PRF(MS, “Client finished” || H(transcript)) }

ChangeCipherSpec,
{ Finished, PRF(MS, “Server finished” || H(transcript’)) }

Bracket notation means contents encrypted

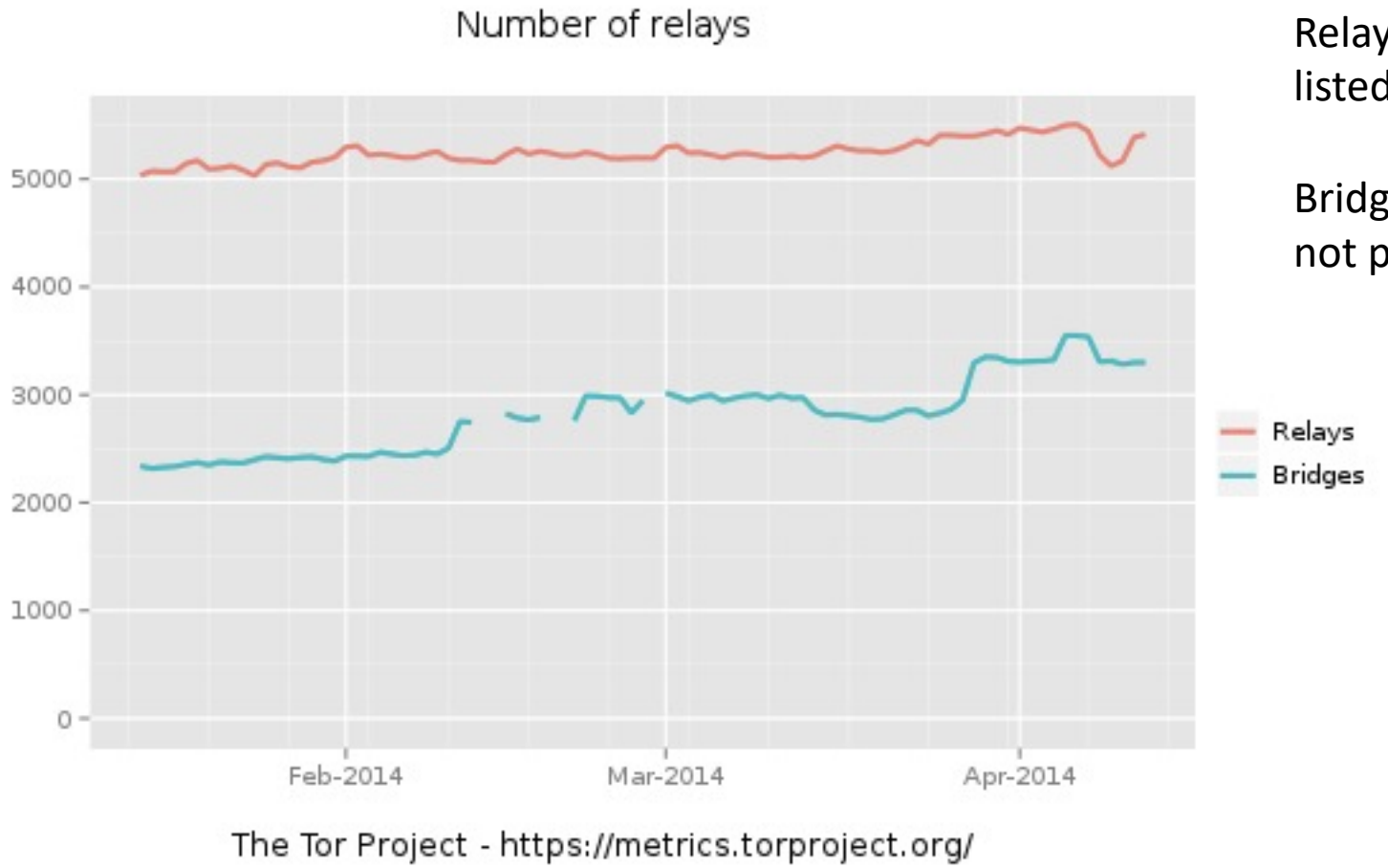
MS <- PRF(PMS, “master secret” || Nc || Ns)

Iran DPI blocking of Tor

- Tor point-to-point connections use TLS
- Use DPI to filter Tor connections:
  - Tor certificates have short expiration date
  - Most websites have long expiration date
  - Shut down those connections with short expiration dates
  - https://blog.torproject.org/blog/update-internet-censorship-iran
- Tor fixed via longer expiration dates
- Later in 2012: blocking/degrading all TLS connections

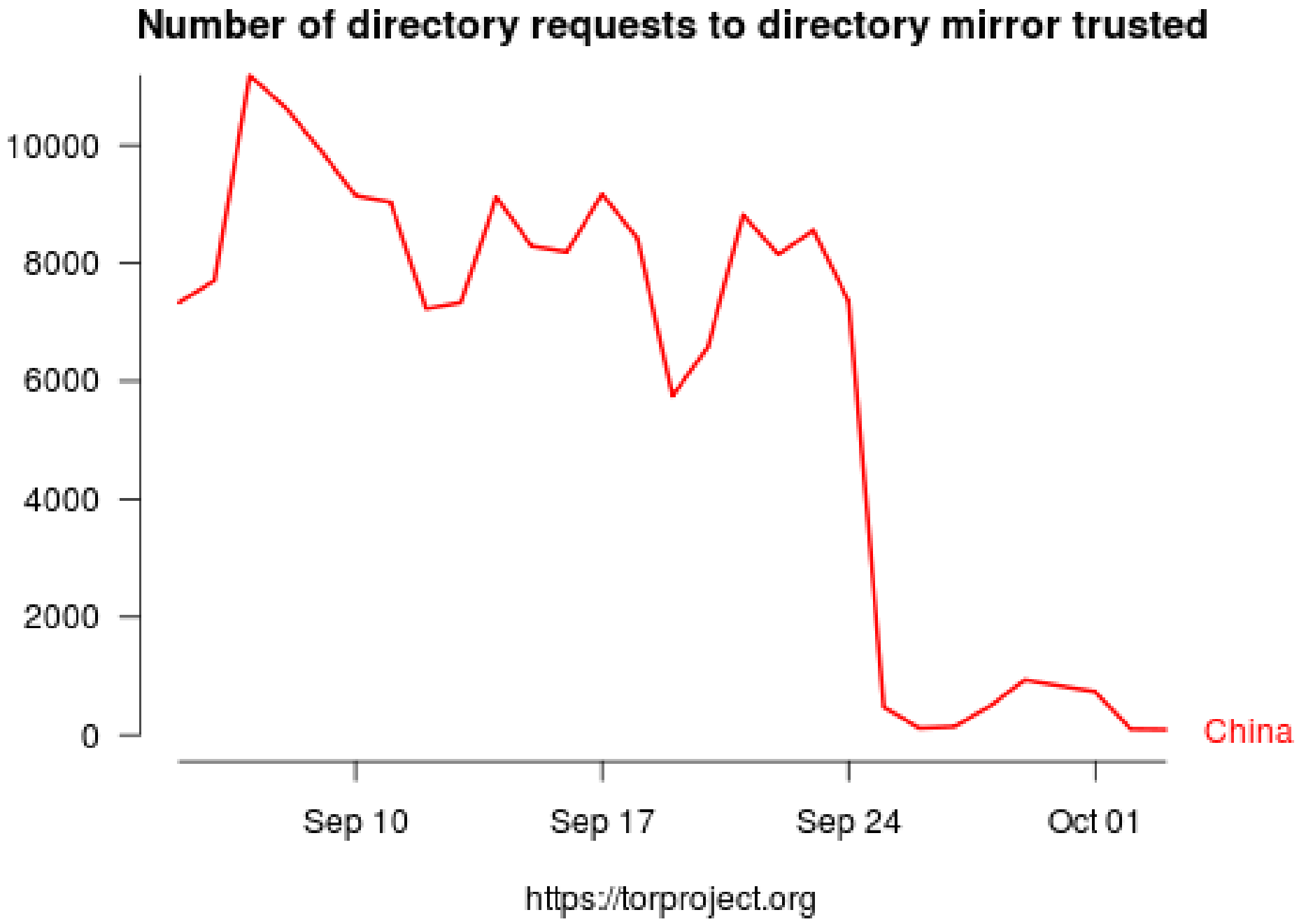
Great Firewall targeting of Tor (circa 2011 and before)

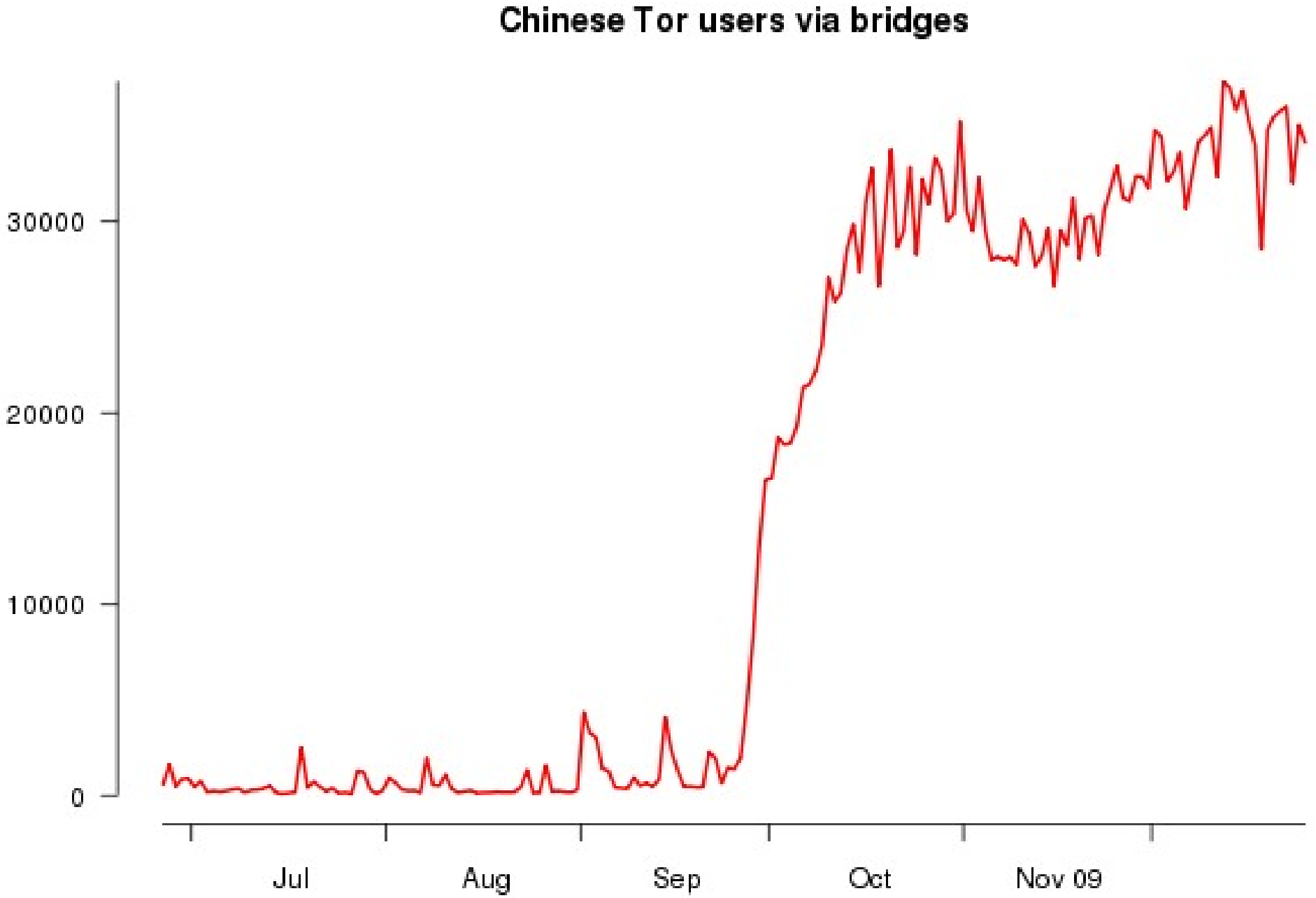
- Enumerate Tor relays and filter them



Relay is publicly listed Tor node

Bridge is Tor node not publicly listed


Number of directory requests to directory mirror trusted
10000
8000
6000
4000
2000
0
Sep 10
Sep 17
Sep 24
Oct 01
China
https://torproject.org



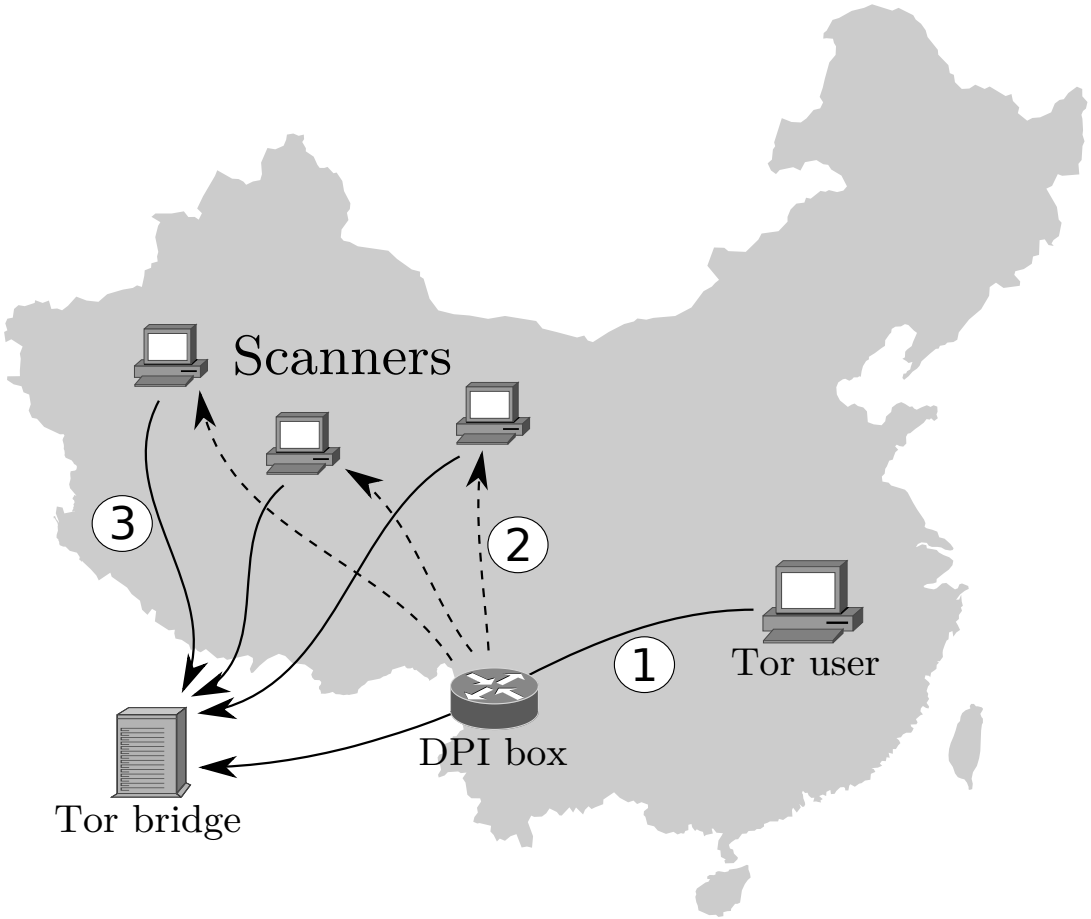
Tor project -- www.torproject.org

Great Firewall targeting of Tor (circa 2011 – today)

Admin noticed weird connections from China 2011

TLS connections with particular ciphersuites flagged for active probing

If remote server speaks Tor then add its IP address to blacklist



From [Winter, Lindskog 2012]

https://gist.github.com/da3c7a9af01d74cd7de7

TLS Handshake

Client

Server

SNI google.com

Pick random Nc

ClientHello, MaxVer, Nc, Ciphers/CompMethods

Pick random Ns

ServerHello, Ver, Ns, SessionID, Cipher/CompMethod

Check CERT
using CA public
verification key

CERT = (pk of server, signature over it)

C

Pick random PMS
C <- E(pk,PMS)

PMS <- D(sk,C)

ChangeCipherSpec,
{ Finished, PRF(MS, “Client finished” || H(transcript)) }

ChangeCipherSpec,
{ Finished, PRF(MS, “Server finished” || H(transcript’)) }

Bracket notation
means contents
encrypted

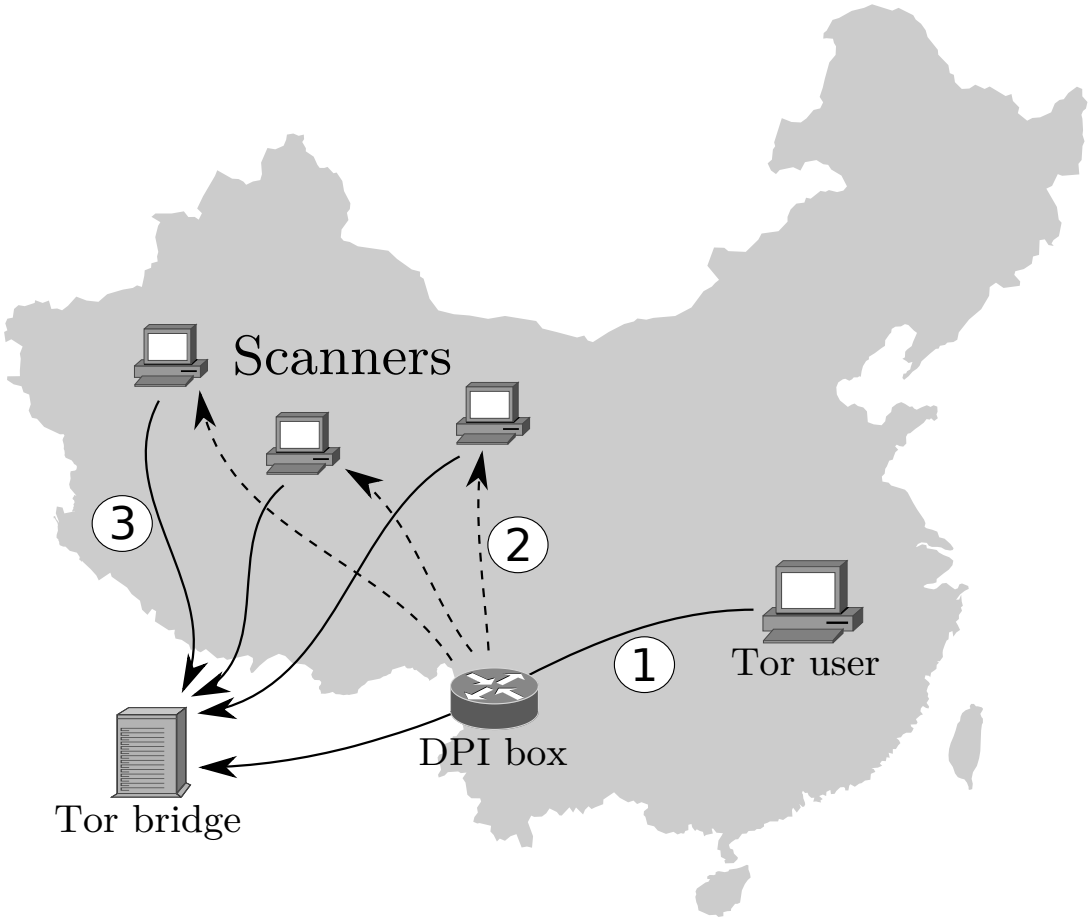
MS <- PRF(PMS, “master secret” || Nc || Ns)

Great Firewall targeting of Tor (circa 2011 – today)

Admin noticed weird connections from China 2011

TLS connections with particular ciphersuites flagged for active probing

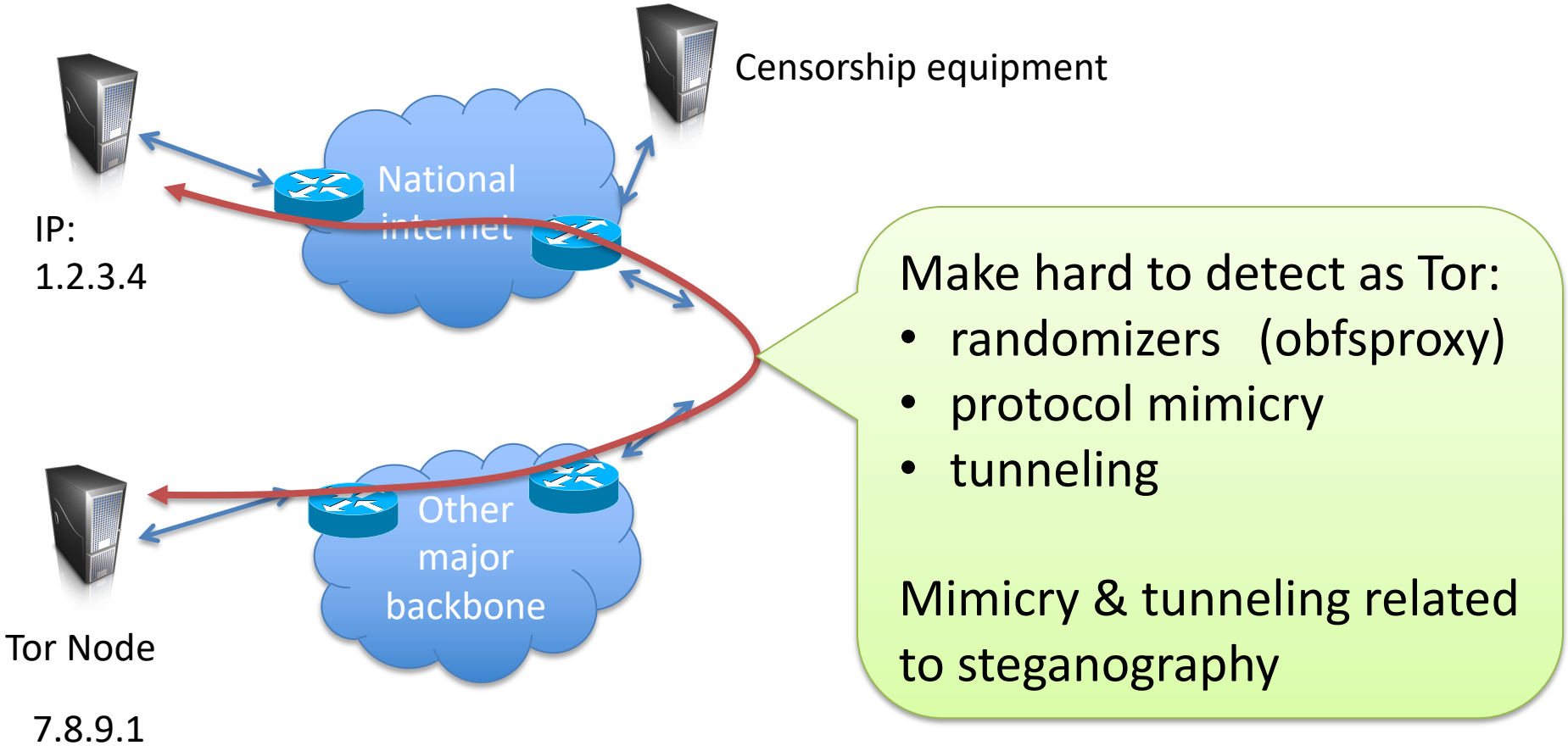
If remote server speaks Tor then add its IP address to blacklist



From [Winter, Lindskog 2012]

https://gist.github.com/da3c7a9af01d74cd7de7

How to circumvent DPI-based protocol/tool identification?



Research on traffic obfuscation

- obfsproxy
  - CTR-mode encryption with per-bridge key
- Flashproxy [Fifield et al. 2012], Snowflake follow-up
  - Use browser extensions as short-lived bridges
- Stegotorus mimicry [Weinberg et al. 2012], format-transforming encryption [Dyer et al. 2013]
  - Make traffic “look” like plaintext traffic
- Meek domain fronting [Fifield et al. 2015]
  - Bounce off HTTPS layer 7 load balancers of cloud services
  - Fake server name indicator
- Decoy routing [Wustro et al., Karlin et al., Houmansadr et al. 2011]
  - Use router to covertly reroute traffic

Research showing inefficacy of obfuscation

- Parrot is dead paper [Houmansadr et al. 2013]
  - Observe that mimicry doesn't provide full fidelity, show attacks against mimicry implementations
  - Don't really measure false positive rates
  - Widely cited as indicating mimicry doesn't work
- [Wang et al. 2015]
  - Use real network traffic from University of Wisconsin to evaluate false positive rates, gather network traces for true positive rates

Obfuscator	Type	Attack	TPR	FPR
obfsproxy3	Randomizer	entropy + length	1.0	0.002
obfsproxy4	Randomizer	entropy + length	1.0	0.002
FTE	Mimicry	URI entropy/length	1.0	0.00003
meek-amazon	Tunneling	decision tree	0.98	0.0002
meek-google	Tunneling	decision tree	0.98	0.00006

Great Firewall targeting of Tor (circa 2011 – today)

Ensafi et al. IMC 2015 follow-up study

- Active measurements, log file analysis, etc.
- China is checking obfsproxy3 bridges
- Hijack IP addresses to perform active probing
- DPI is stateful but does not reconstruct TCP streams

Censorship summary

- Nation-state censorship apparatuses are technologically sophisticated
- Arms race between circumvention community (activists, academics, USG)
- Lots of research and development:
  - New circumvention tools
  - Understanding detection tools
  - Active development community (Tor, Ultrasurf, Psyphon, etc.)