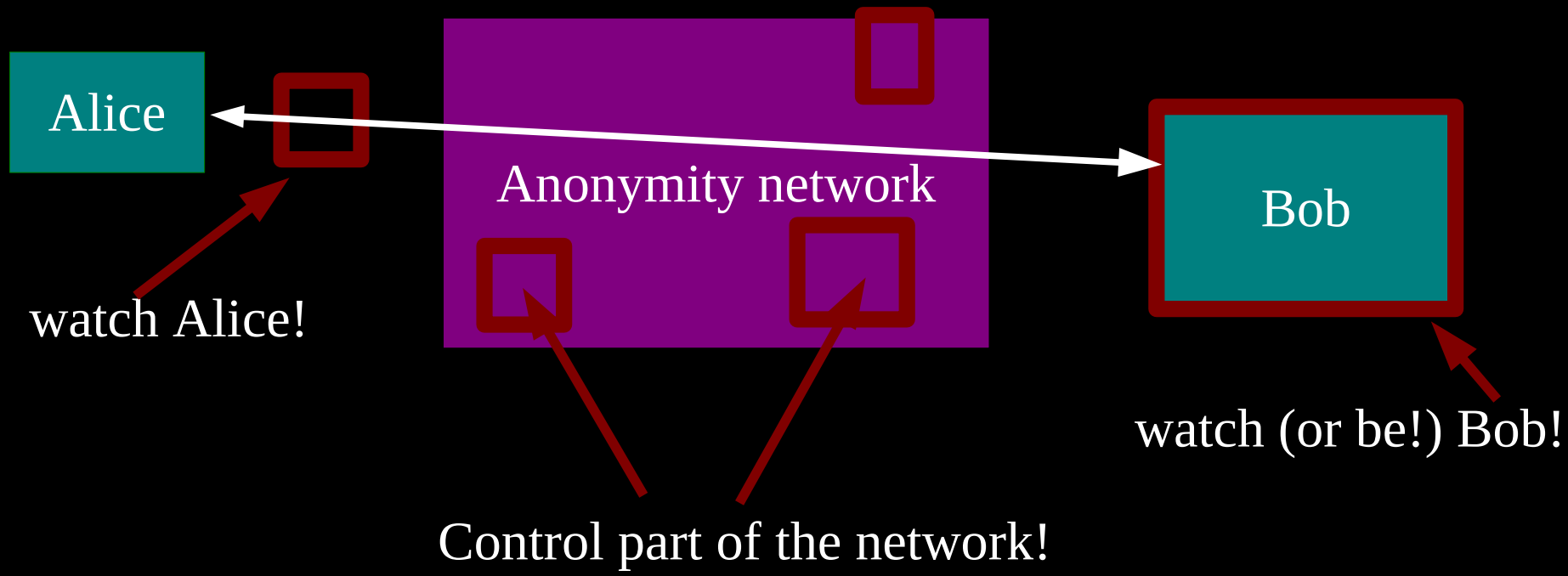
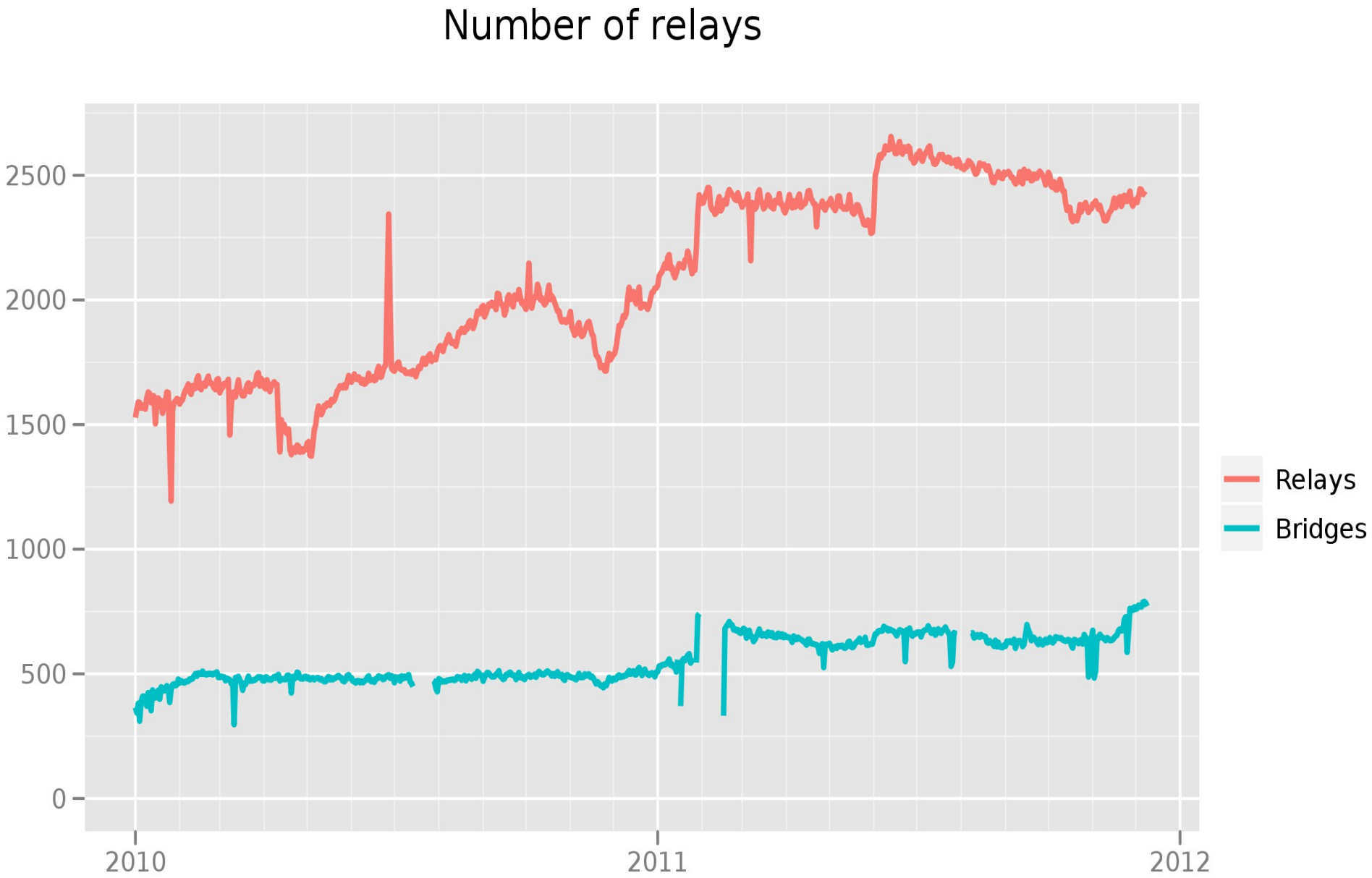
How governments have tried to block Tor

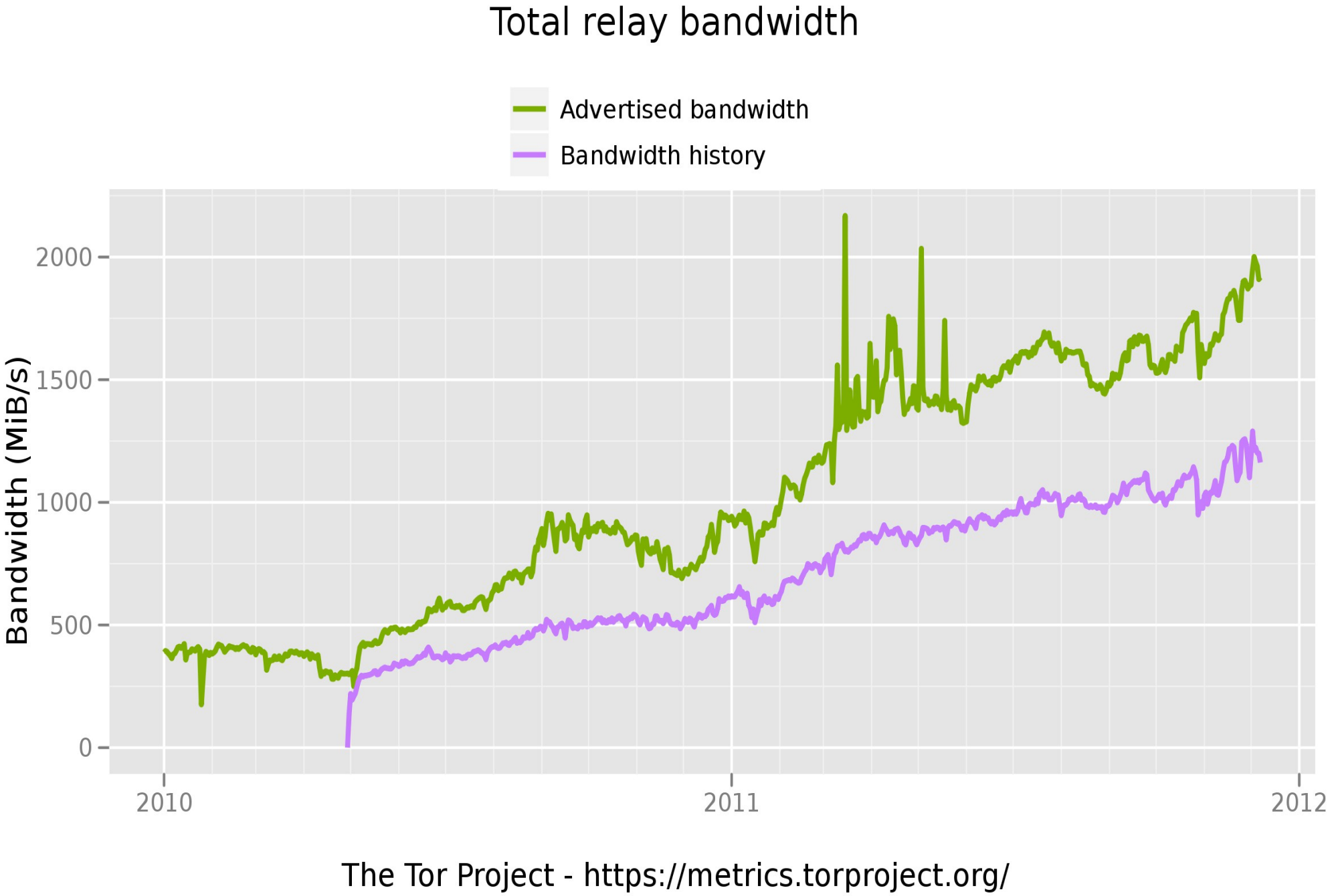
Roger Dingledine
Jacob Appelbaum
The Tor Project
https://torproject.org/


Estimated ~400,000?
daily Tor users

Threat model: what can the attacker do?




Number of relays
2500
2000
1500
1000
500
0
2010
2011
2012
Relays
Bridges
The Tor Project - https://metrics.torproject.org/


Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
2000
1500
1000
500
0
2010
2011
2012
The Tor Project - https://metrics.torproject.org/

Context is everything

This conference is perfectly themed for our subject matter.

Tor's code released (2002)

- Tor's code released in 2002
- Tor's design paper published in 2004
- The clock starts ticking...

Thailand (April 2006)

- DNS filtering of our website
- Only by ISPs that participated in the Cyber Clean program of the Ministry of Information and Communication Technology
- Redirected to block page
  - http://www.mict.go.th/ci/block.html

Smartfilter/Websense (2006)

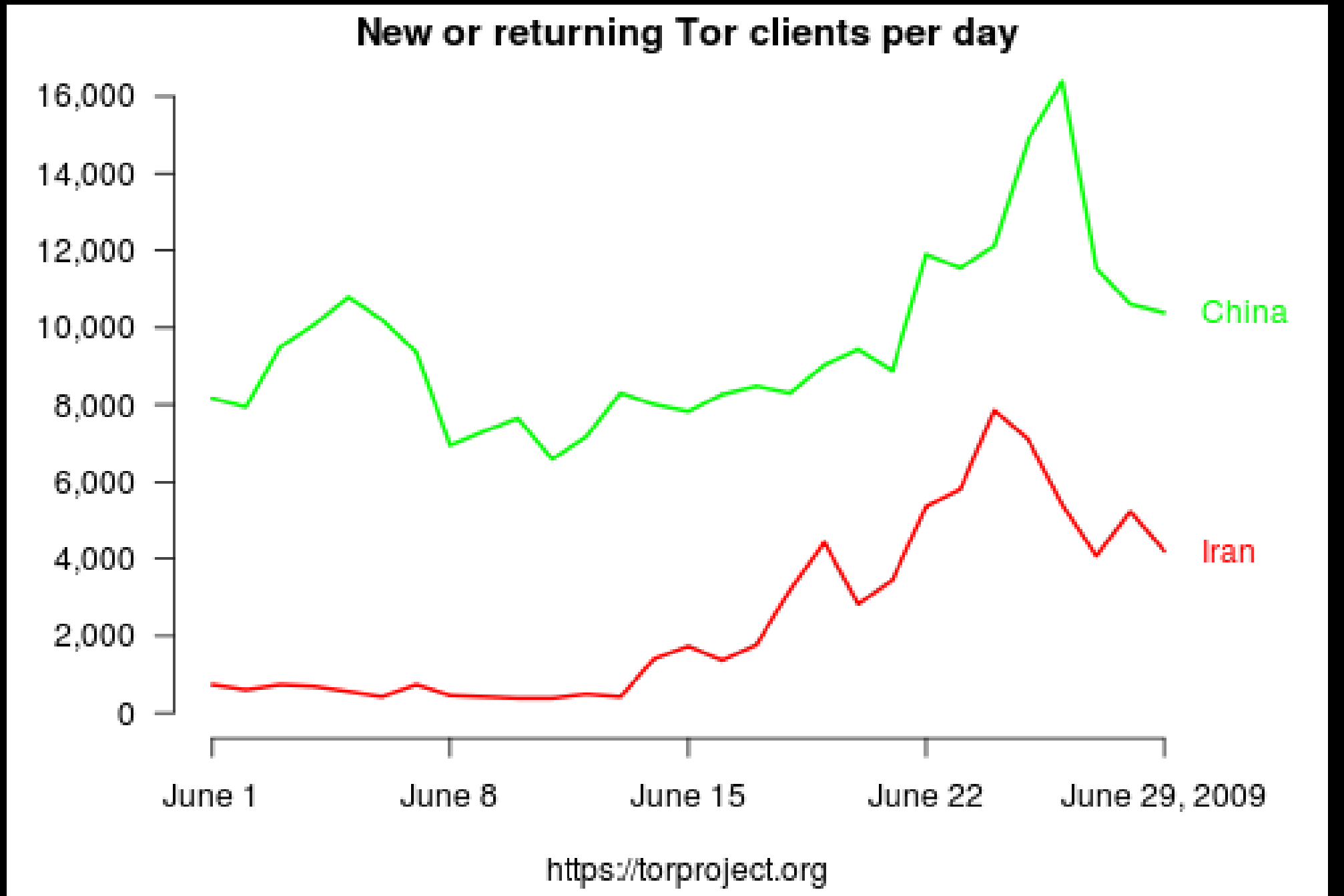
- Tor used TLS for its encrypted connection, and HTTP for fetching directory info.
- Smartfilter just cut all HTTP GET requests for “/tor/...”
  - That is not much of an arms race...
- Websense, Cisco, etc advertised this way of blocking Tor, even when it was obsolete.

Iran/Saudi Arabia/etc (2007)

- Picked up these Smartfilter/Websense rules by pulling an update
- The fix was to tunnel directory fetches inside the encrypted connection
  - When Iran kicked out Smartfilter in early 2009, Tor's old (non-TLS) directory fetches worked again!

Iran throttles SSL (June 2009)

- We made Tor's TLS handshake look like Firefox+Apache.
    - We also now have a dynamic prime option
- So when Iran freaked out and throttled SSL bandwidth by DPI in summer 2009, they got Tor for free


New or returning Tor clients per day
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
China
Iran
June 1
June 8
June 15
June 22
June 29, 2009
https://torproject.org

Tunisia (summer 2009)

- As of the summer of 2009, Tunisia used Smartfilter to filter every port but 80 and 443
- And if they didn't like you, they *would* block 443 just for **you**
- You could use a Tor bridge on port 80, but couldn't bootstrap into the main network
- So we set up a Tor directory authority doing TLS on port 80 (Jacob's authority urras)

China (September 2009)

- China grabbed the list of public relays and blocked them
- They also enumerated one of the three bridge buckets (the ones available via https://bridges.torproject.org/)
- But they missed the other bridge buckets.

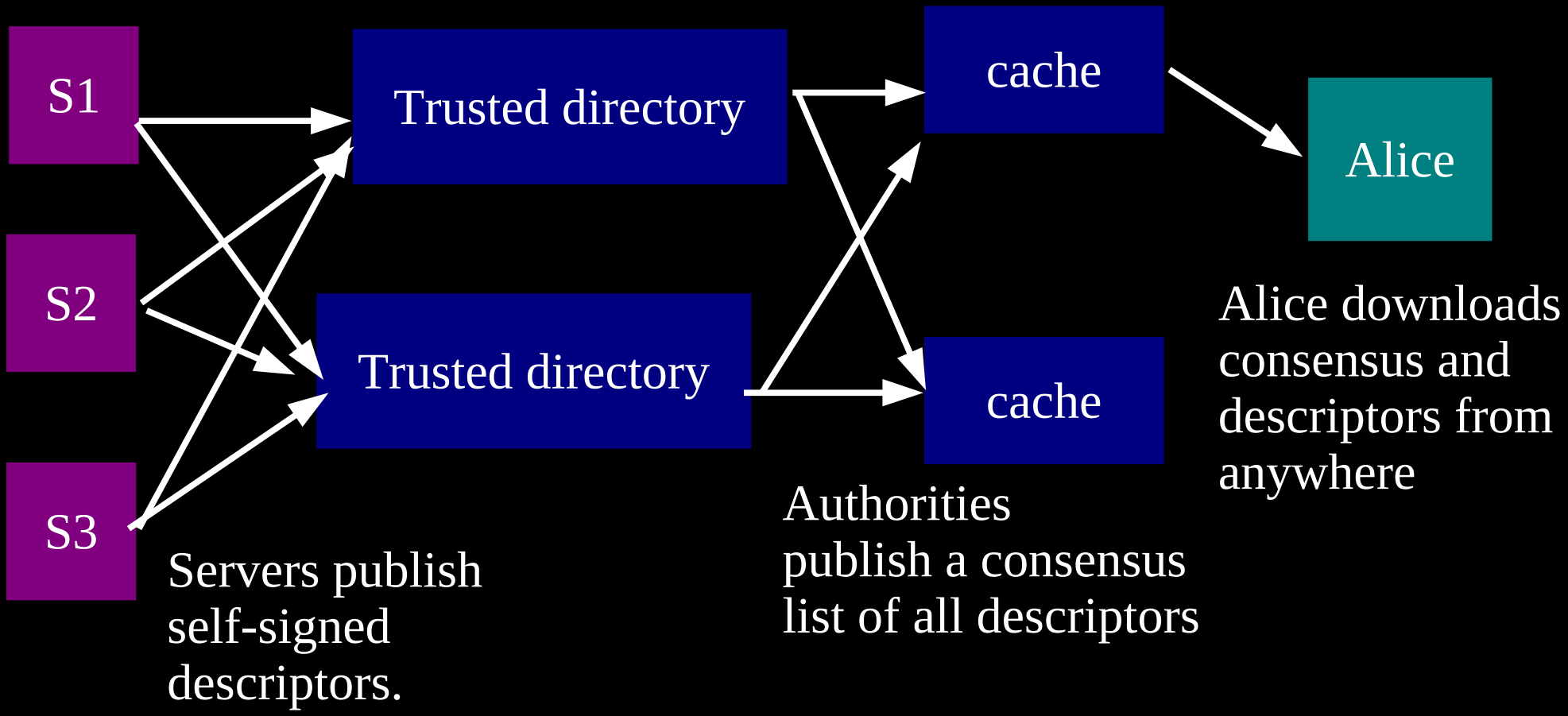
Relay versus Discovery

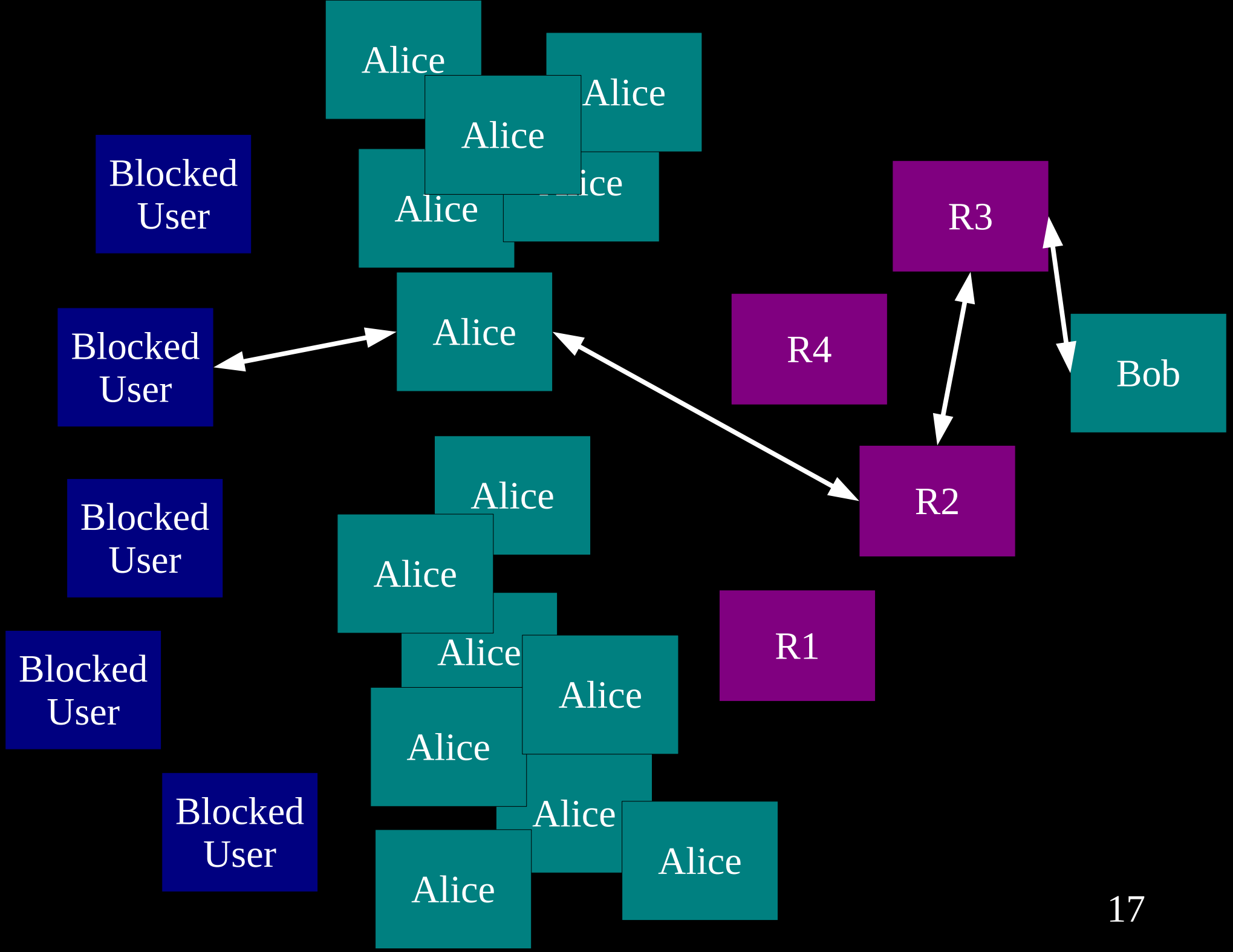
There are two pieces to all these “proxying” schemes:

a **relay** component: building circuits, sending traffic over them, getting the crypto right

a **discovery** component: learning what relays are available

The basic Tor design uses a simple centralized directory protocol.




Alice
Alice
Alice
Alice
Alice
Blocked User
Blocked User
Blocked User
Blocked User
Blocked User
Alice
Alice
Alice
Alice
Alice
Alice
Alice
R3
R4
R2
R1
Bob

How do you find a bridge?

1) **https://bridges.torproject.org/** will tell you a few based on time and your IP address

2) Mail bridges@torproject.org from a gmail address and we'll send you a few

3) I mail some to a friend in Shanghai who distributes them via his social network

4) You can set up your own private bridge and tell your target users directly

Attackers can block users from connecting to the Tor network

1) By blocking the directory authorities

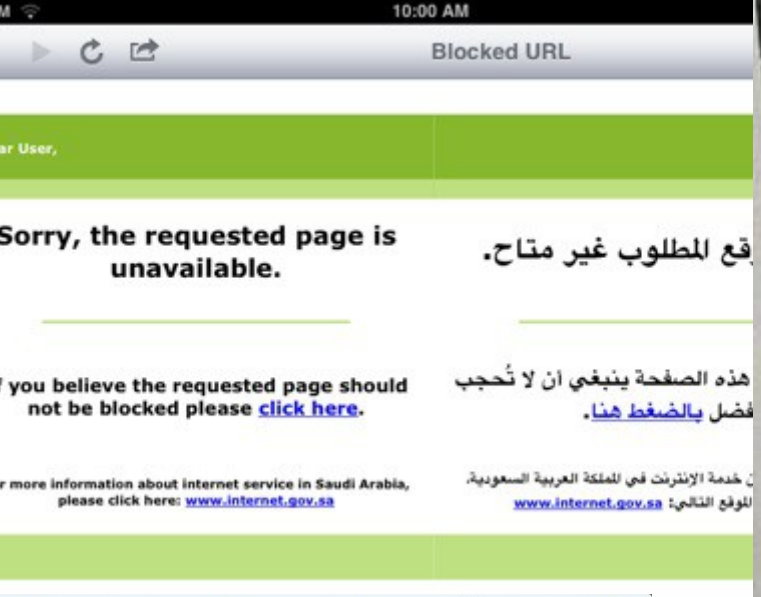
2) By blocking all the relay IP addresses in the directory, or the addresses of other Tor services

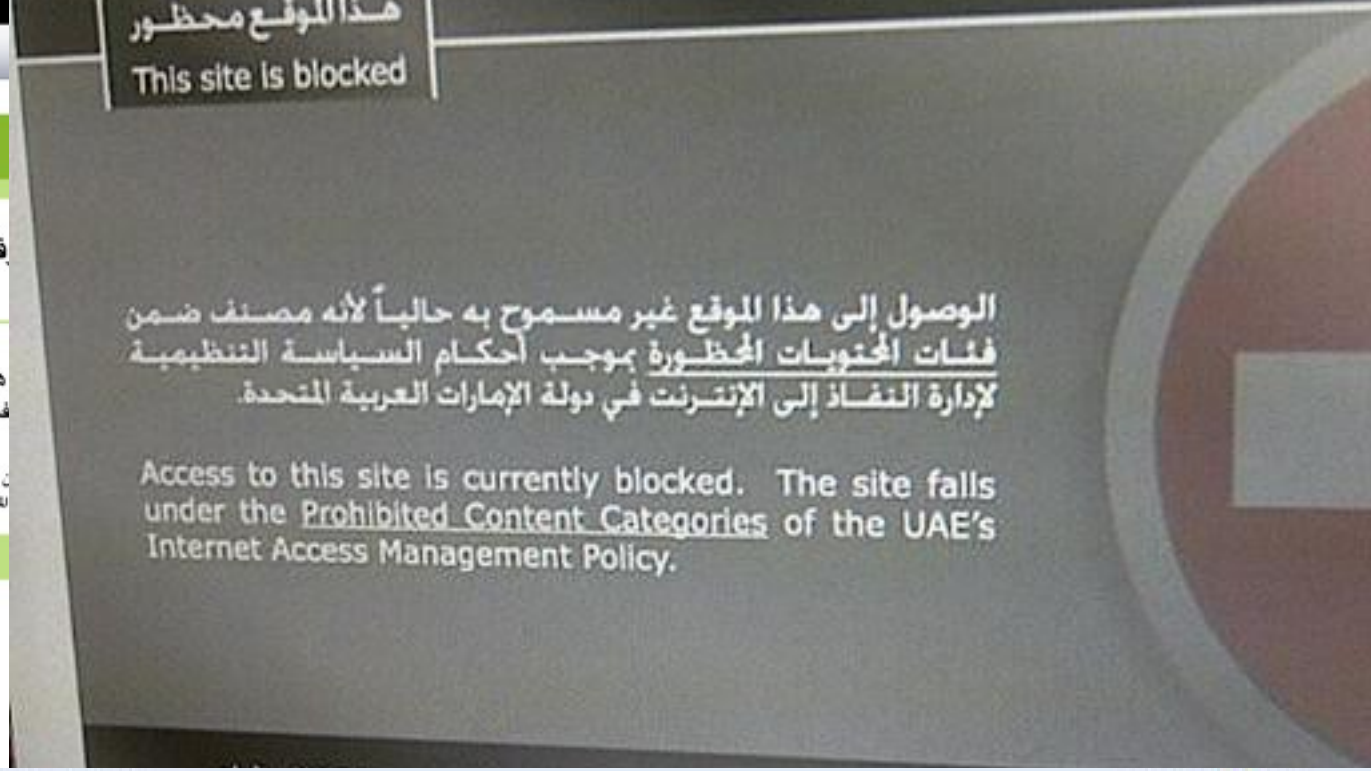
3) By filtering based on Tor's network fingerprint

4) By preventing users from finding the Tor software (usually by blocking website)

Your request was denied because of its conte

ء على اللوائح والقوانين
مع unblock.kw@kw.zain

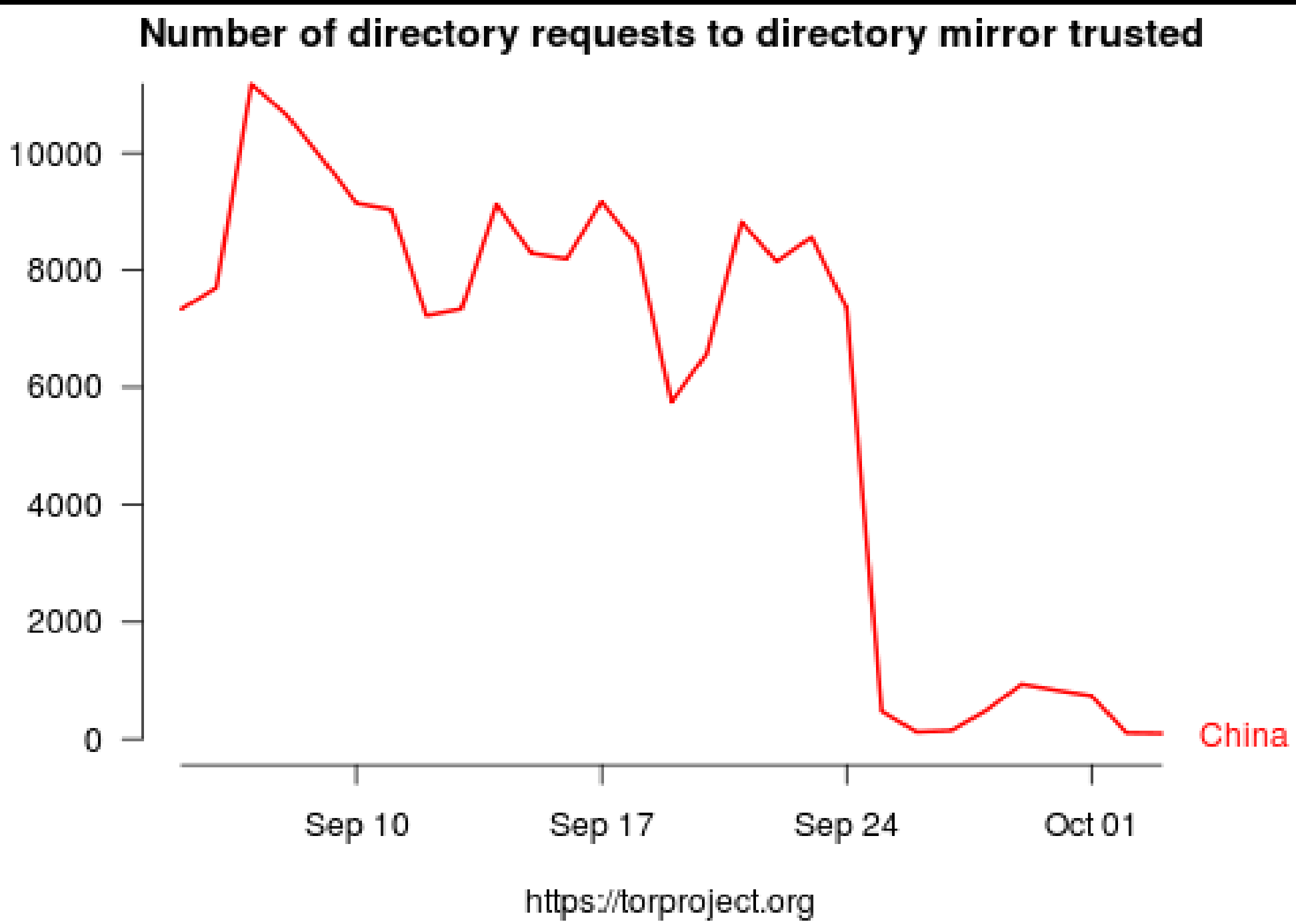

10:00 AM
Blocked URL
ar User,
Sorry, the requested page is unavailable.
قع المطلوب غير متاح.
you believe the requested page should not be blocked please click here.
هذه الصفحة ينبغي أن لا تُحجب
فضل بالضغط هنا.
r more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa
www.internet.gov.sa

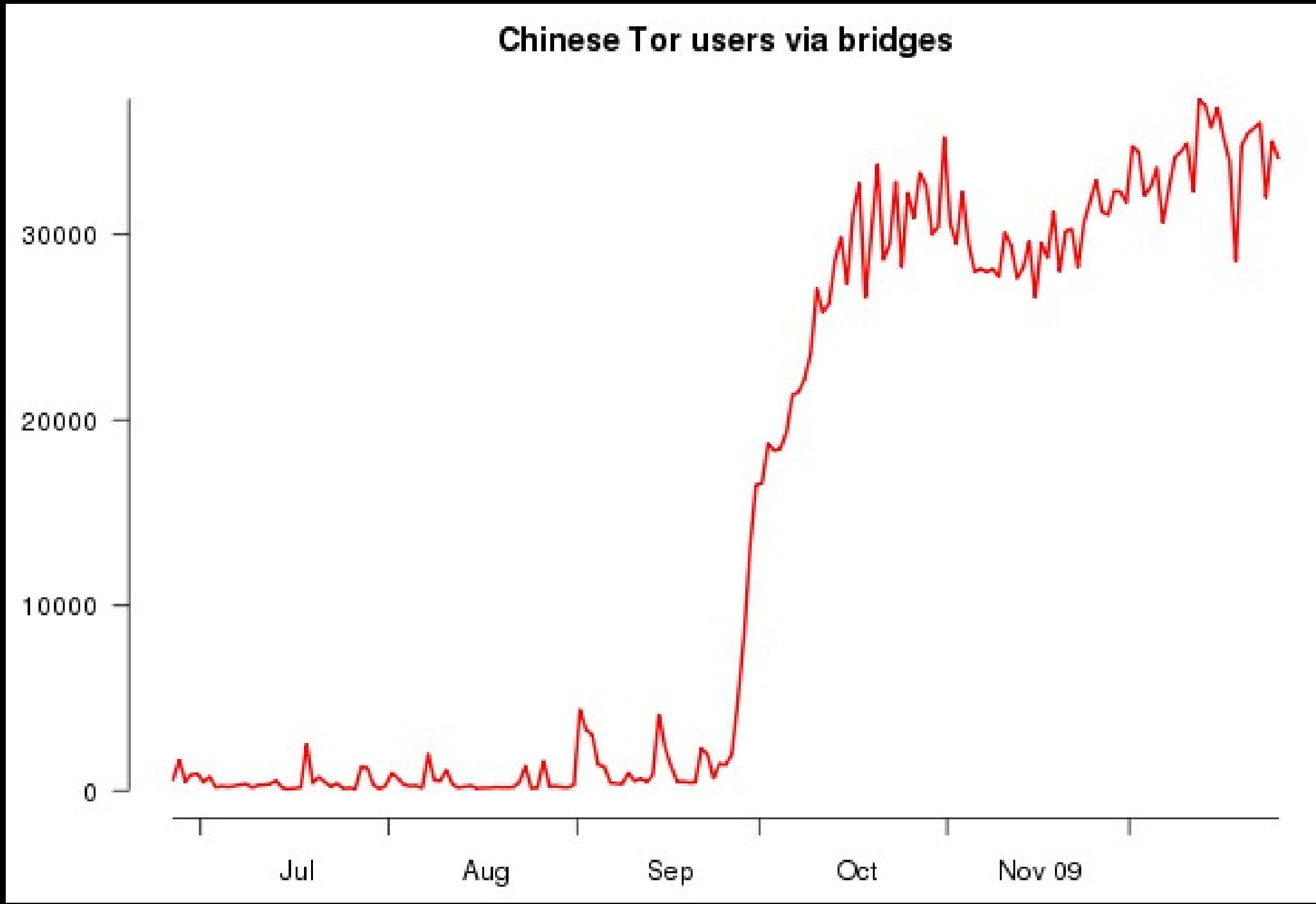

This site is blocked
الوصول إلى هذا الموقع غير مسموح به حالياً لأنه مصنف ضمن فئات المحتويات المحظورة بموجب أحكام السياسة التنظيمية لإدارة النفاذ إلى الإنترنت في دولة الإمارات العربية المتحدة.
Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's Internet Access Management Policy.


KT WATA...
٩:٢١ ص
87%
Tweet
Blocked by Mada Com...


مـــدى للإتصـــالات
mada Mada Communications
ان الموقع الذي تحاول زيارته محجوب
Access to this website is prohibited
This site is blocked according to the goverment filtering policy.
If you feel this page has been blocked in errors, kindly fill out the form and we will investigate.
Thank You.
Required fields are denoted by (*)
Full Name *
الإسم
Email *
العنوان البريدي
Blocked URL *
www.
.com
اسم المخالف
Comments
استفسارك
Submit

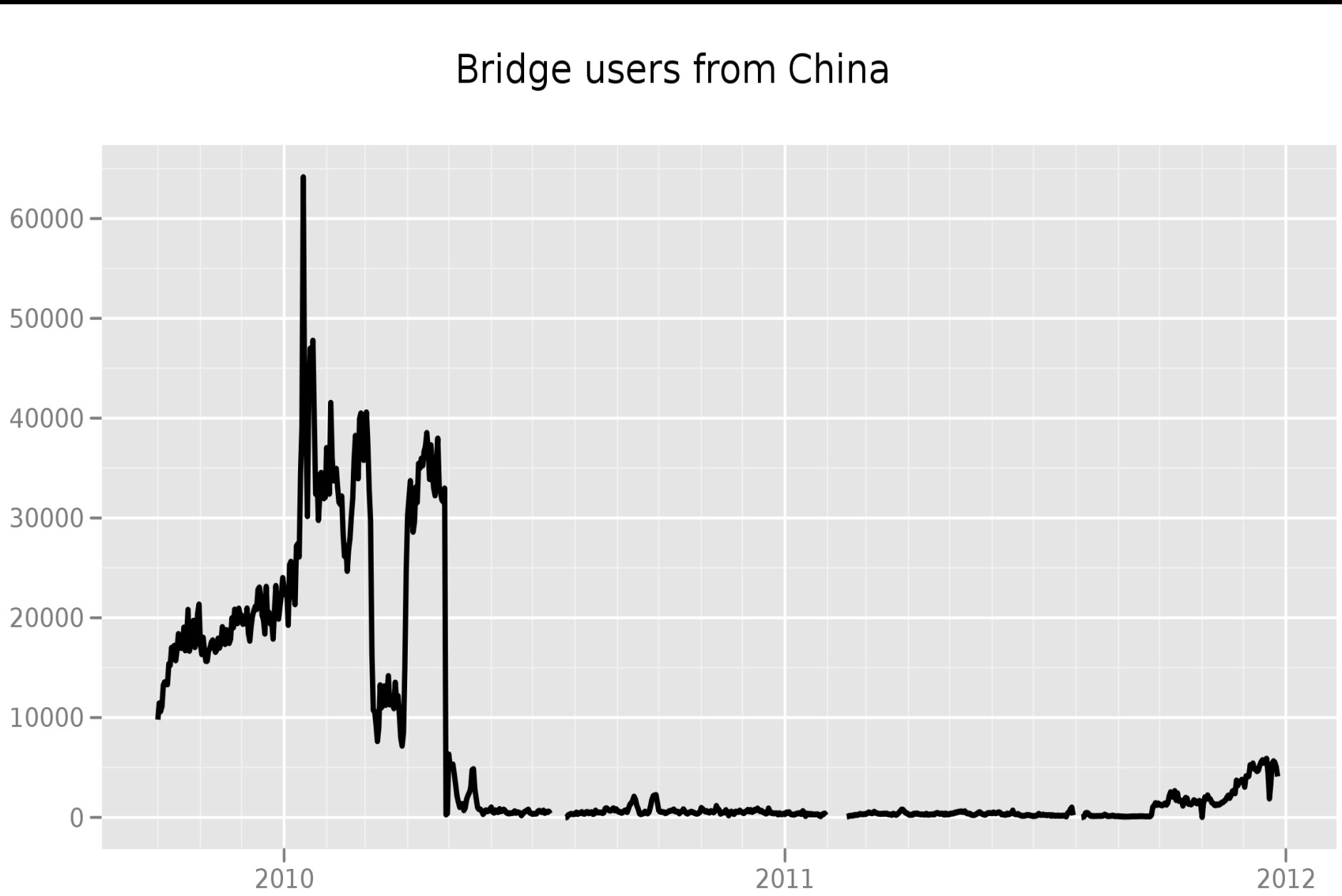

أفا oops
لقد تم منع الدخول إلى هذا الموقع
This site has been blocked
تم إيقاف عملية الدخول الى الموقع الذي تحاول زيارته نظراً لاحتوائه على محتويات محظورة
The web page you are trying to access has been blocked as the content contains prohibited materials
إذا كنت ترى أن هناك خطأ في ذلك - يرجى إرسال رسالة بريد إلكتروني إلى helpdesp.qa
If you feel this is an error then please send


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


Chinese Tor users via bridges
30000
20000
10000
0
Jul
Aug
Sep
Oct
Nov 09

China (March 2010)

- China enumerated the second of our three bridge buckets (the ones available at bridges@torproject.org via Gmail)
- We were down to the social network distribution strategy, and the private bridges


Bridge users from China
60000
50000
40000
30000
20000
10000
0
2010
2011
2012
The Tor Project - https://metrics.torproject.org/

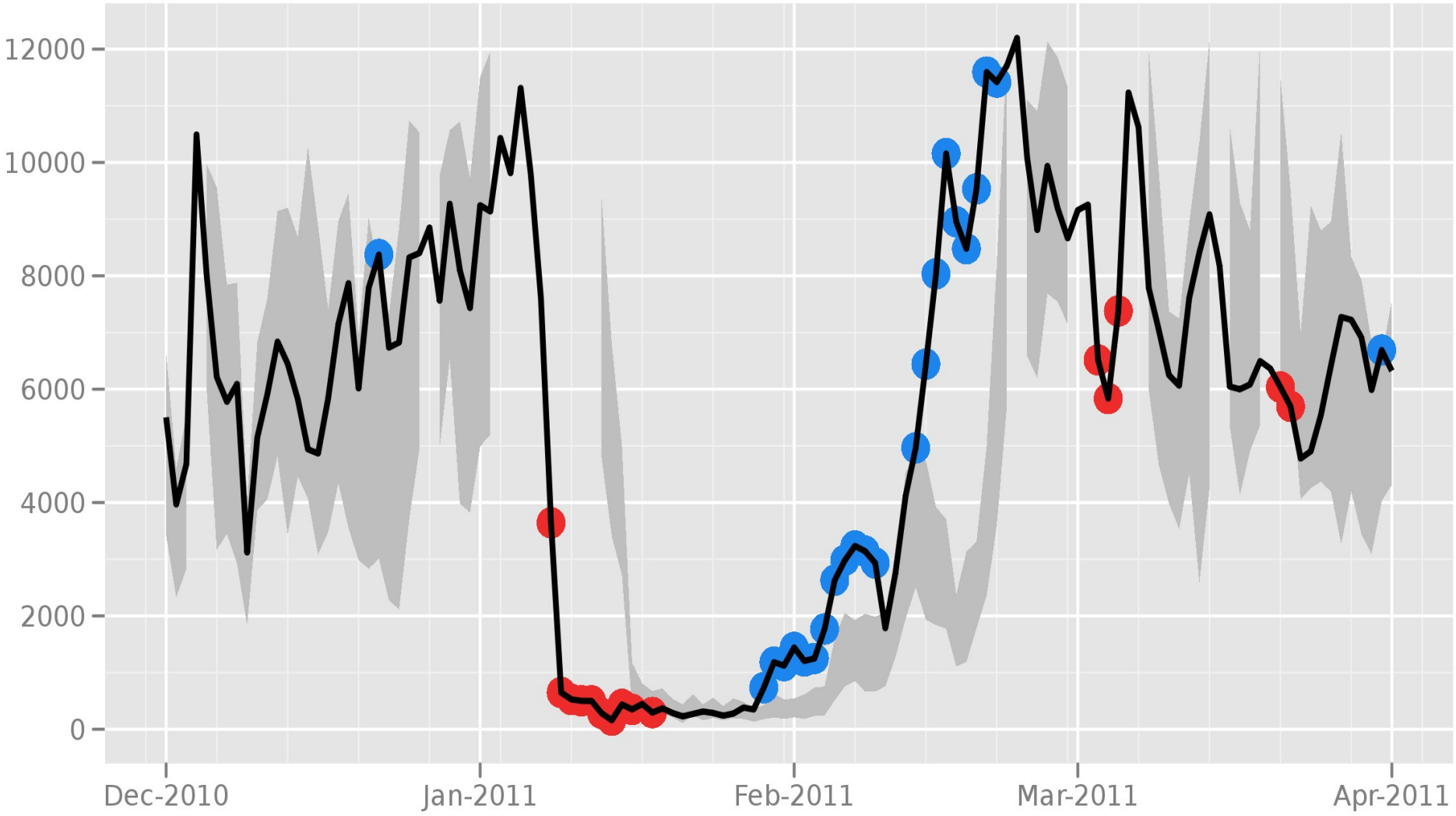
Greece (~5th century BC)

- Jumping back in time...
  - Hippasus is drowned for showing a new class of numbers...
    - “Proof of the irrationality of √2”

Iran (January 2011)

- Iran blocked Tor by DPI for SSL and filtering our Diffie-Hellman parameter.
    - Our prime p is part of a banned class of numbers; not irrational, liberating?
- Socks proxy worked fine the whole time (the DPI didn't pick it up)
- DH p is a server-side parameter, so the relays and bridges had to upgrade, but not the clients

Directly connecting users from the Islamic Republic of Iran

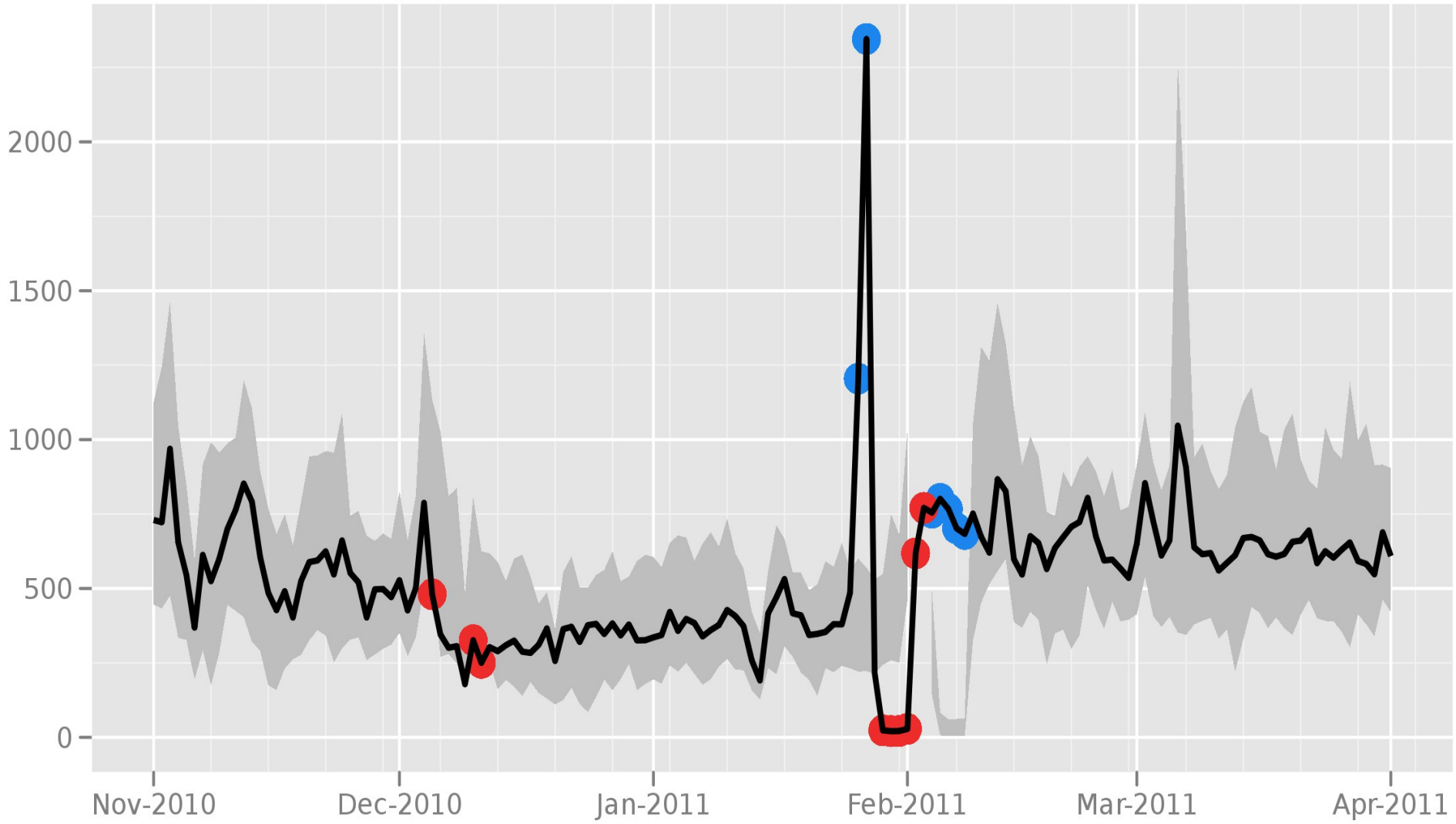


The Tor Project - https://metrics.torproject.org/

Egypt (January 2011)

- Egypt selected and targeted sites for blocking
    - Twitter was not entirely blocked but the attempt was good enough (TEData)
- When Egypt unplugged its Internet, no more Tor either.

Directly connecting users from Egypt

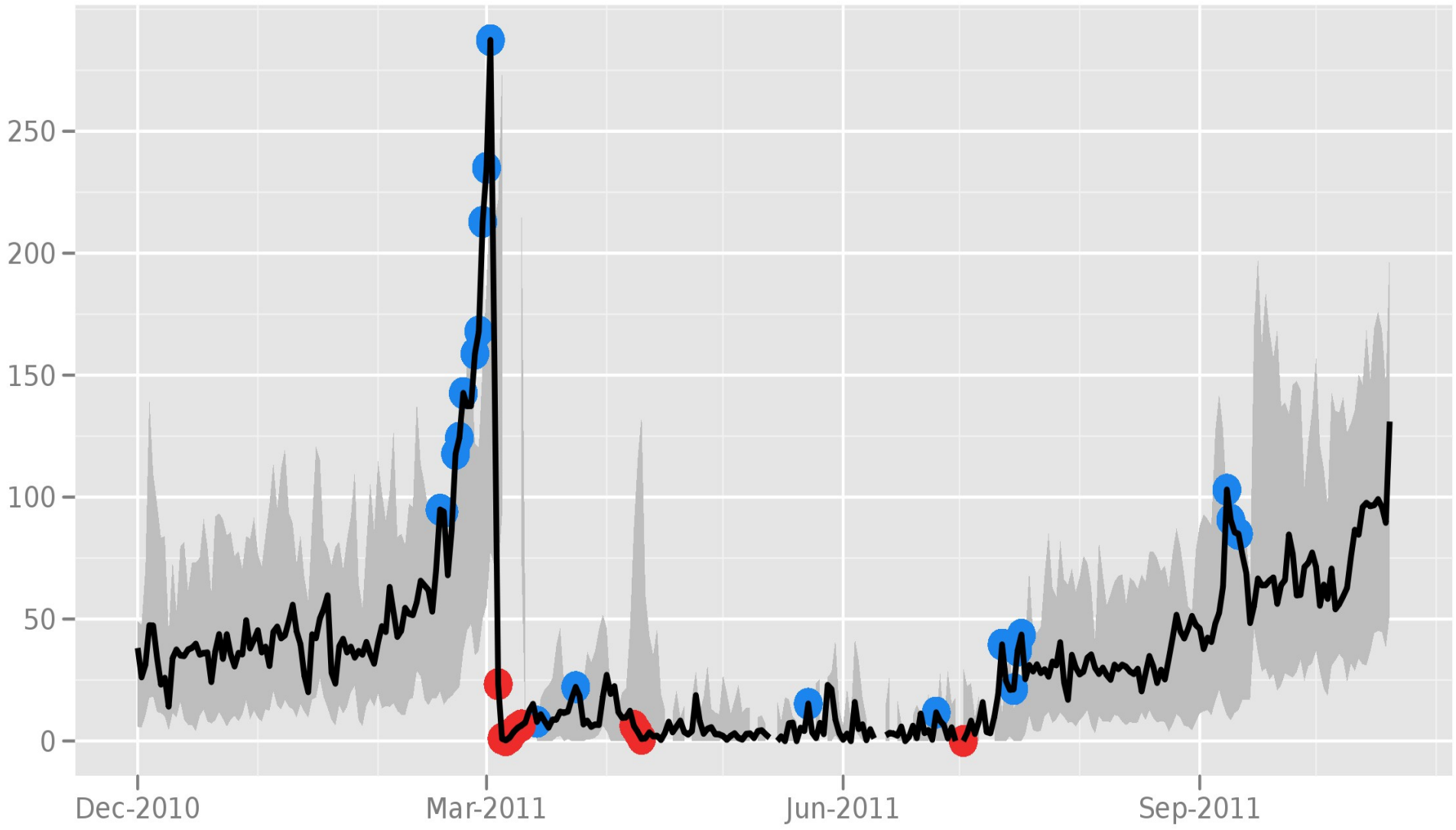


The Tor Project - https://metrics.torproject.org/

Libya (March-July 2011)

- Libya might as well have unplugged its Internet.
- But they did it through throttling, so nobody cared.

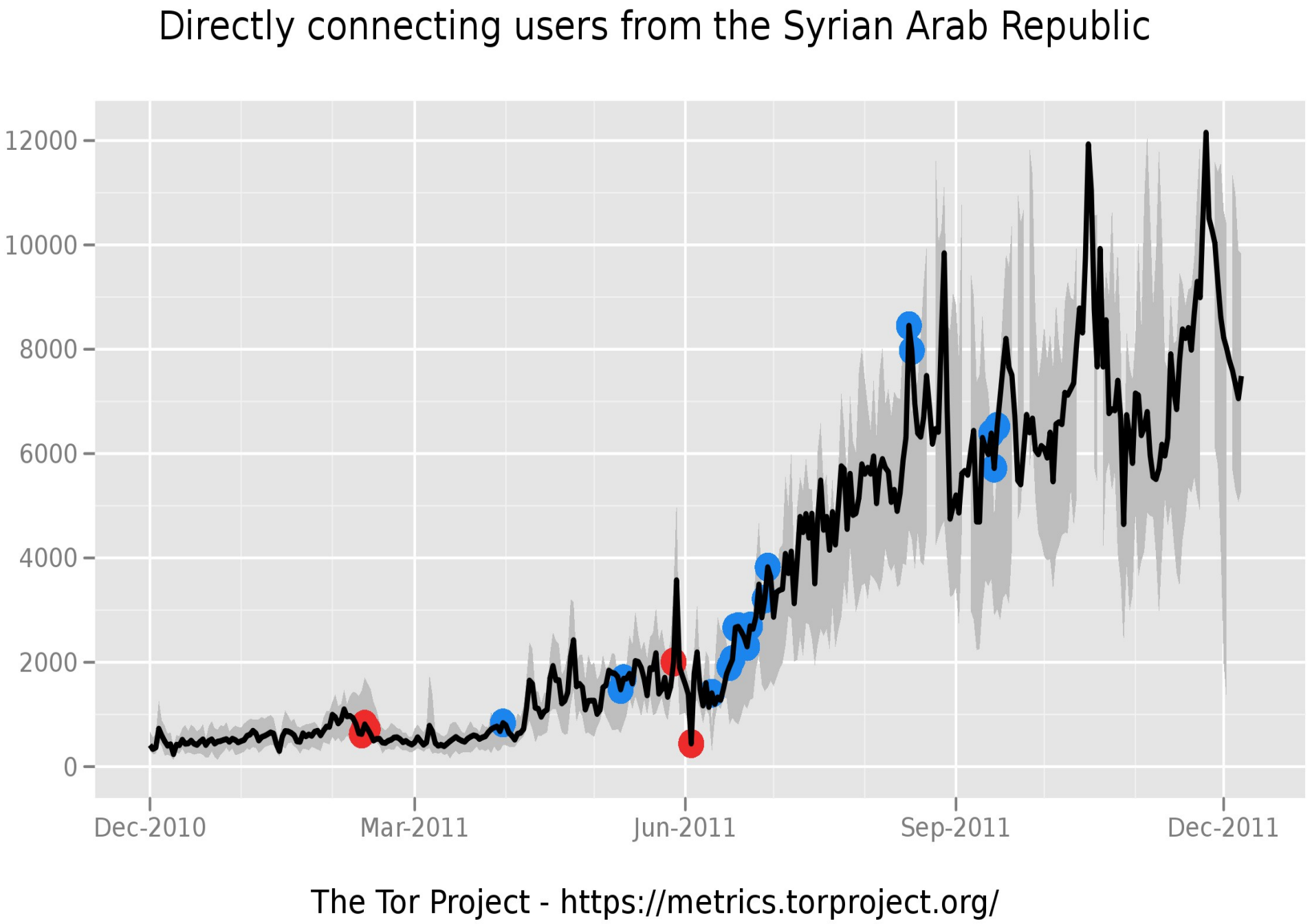
Directly connecting users from Libya



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

Syria (June 2011)

- One ISP briefly DPIed for Tor's TLS renegotiation and killed the connections.
    - Blue Coat, more like *Red Coats!*
- A week later, that ISP went offline. When it came back, no more Tor filters.
- Who was testing what?


Directly connecting users from the Syrian Arab Republic
12000
10000
8000
6000
4000
2000
0
Dec-2010
Mar-2011
Jun-2011
Sep-2011
Dec-2011
The Tor Project - https://metrics.torproject.org/

A tale of two circumvention systems

- Ultrasurf
  - Distinguishable behavior
  - Lots of unnecessary data in logs
  - Evidence of unproxied traffic
- Tor
  - Looks like SSL
  - No extra details in logs

Bluecoat logs from Syria (worse)

- 2011-08-05 23:45:19 539 31.9.244.83 - - - OBSERVED "unavailable" - 200 TCP_NC_MISS GET text/html; %20charset=UTF-8 http 74.125.39.106 80 **/gwt/n?u=http://114.42.119.186/MzYwOWEwMjZn/k6IPd6kevXg2/1KQEH7fij/XAojkR9c/14g2SRugC7Hx/vba1vA -** "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)" 82.137.200.44 2409 230 -

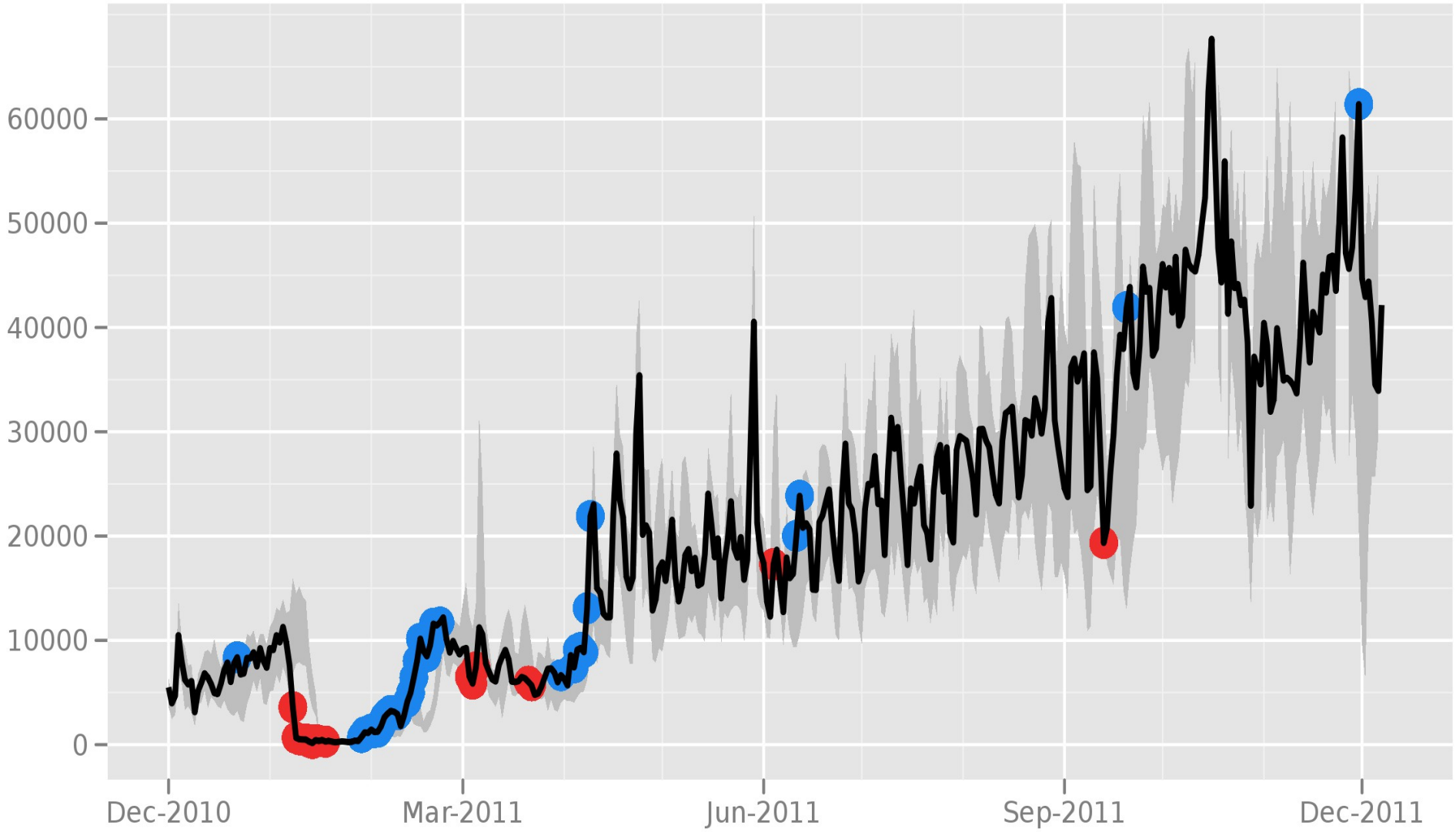
Bluecoat logs from Syria (better)

- 2011-08-05 23:52:31 166849 82.137.249.41 - - - OBSERVED "unavailable" - 200 TCP_TUNNELED CONNECT - tcp 208.83.223.34 80 / - - - 82.137.200.44 4086 2657 -

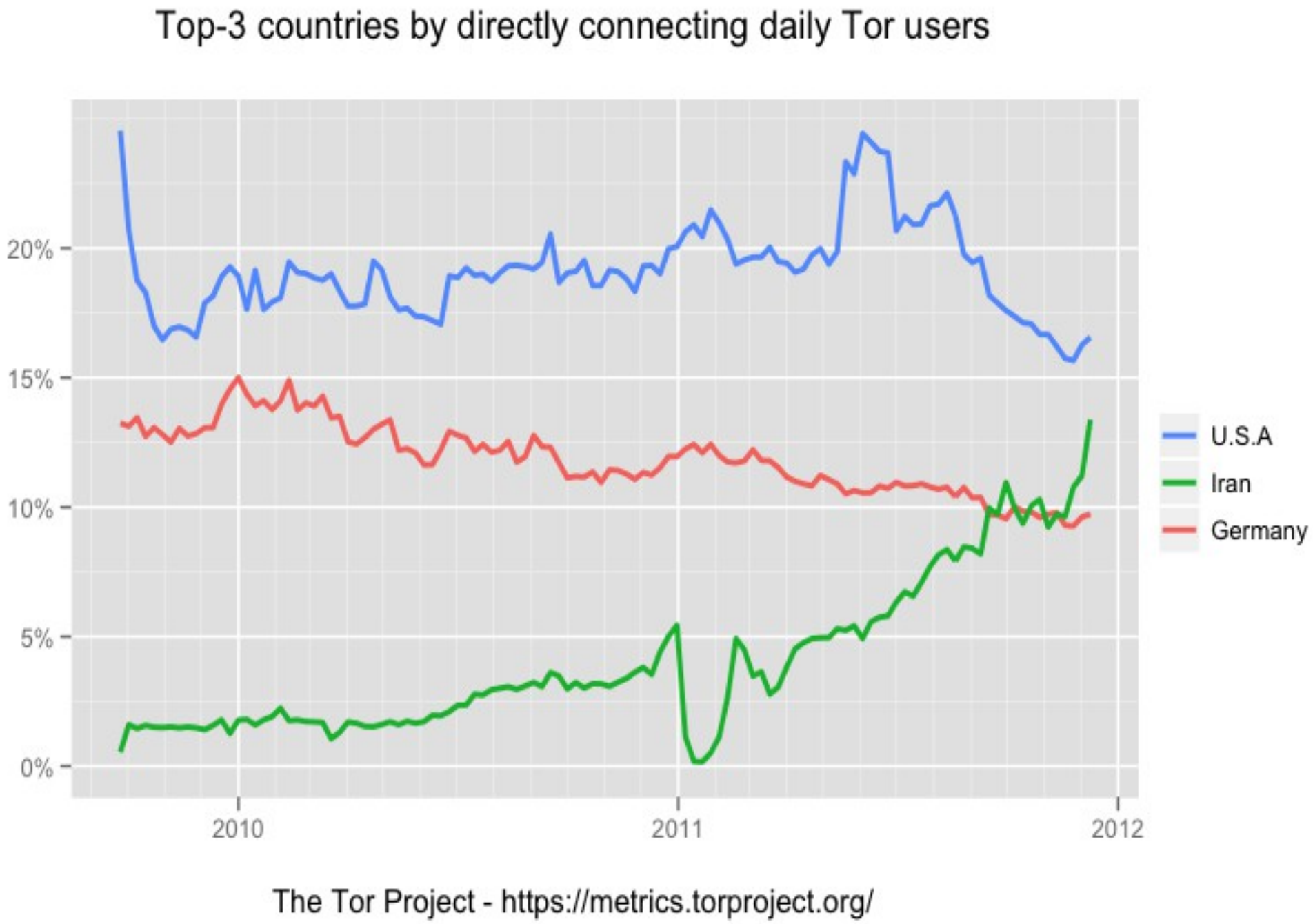
Iran (September 2011)

- This time, DPI for SSL and look at our TLS certificate lifetime.
- (Tor rotated its TLS certificates every 2 hours, because key rotation is good, right?)
- Now our certificates last for a year
- These are all low-hanging fruit. How do we want the arms race to go?

Directly connecting users from the Islamic Republic of Iran



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


Top-3 countries by directly connecting daily Tor users
20%
15%
10%
5%
0%
2010
2011
2012
U.S.A
Iran
Germany
The Tor Project - https://metrics.torproject.org/

October 2011 advances?

- Iran DPIs for SSL, recognizes Tor, and throttles rather than blocks?
- China DPIs for SSL, does active follow-up probing to see what sort of SSL it is?
- https://trac.torproject.org/projects/tor/ticket/4185

December 2011

Reports of redirection of traffic in Iran to peyvandha.ir

What we're up against

Govt firewalls used to be stateless. Now they're buying fancier hardware.

Burma vs Iran vs China

New filtering techniques spread by commercial (American) companies :(

How to separate “oppressing employees” vs “oppressing citizens” arms race?

- What's the difference anyway?

What we're up against

Blue Coat

SmartFilter

Websense

Nokia

Cisco

And many many more (See Jacob's RECon2011 talk for more details)

Tor's safety comes from diversity

- #1: Diversity of relays. The more relays we have and the more diverse they, the fewer attackers are in a position to do traffic confirmation. (Research problem: measuring diversity over time)
- #2: Diversity of users and reasons to use it. 40000 users in Iran means almost all of them are normal citizens.

BridgeDB needs a feedback cycle

- Measure how much use each bridge sees
- Measure bridge blocking
- Then adapt bridge distribution to favor efficient distribution channels
- (Need to invent new distribution channels)

Measuring bridge reachability

- Passive: bridges track incoming connections by country; clients self-report blockage (via some other bridge)
- Active: scan bridges from within the country; measure remotely via FTP reflectors
- Bridges test for duplex blocking

Other components

- Traffic camouflaging
  - Super-encrypt so no recognizable bytes? Shape like HTTP?
  - We're working on a modular transport API
  - Need “obfuscation” metrics?

We must reject so-called “lawful interception” and data retention

To understand the scope of the market and the reach of the market - we encourage you to look at the BuggedPlanet Wiki and to read about the WikiLeaks release of the Spyfiles:

http://spyfiles.org/

http://buggedplanet.info/


I CAN HAZ
FREEDOM?
TorProject.org