



The Tor Project, Inc.

Our mission is to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.

What is Tor?

Online anonymity 1) open source software,
2) network, 3) protocol

Community of researchers, developers,
users, and relay operators

Funding from US DoD, Electronic Frontier
Foundation, Voice of America, Google,
NLnet, Human Rights Watch, NSF, US
State Dept, SIDA, Knight Foundation, ...

The Tor Project, Inc.

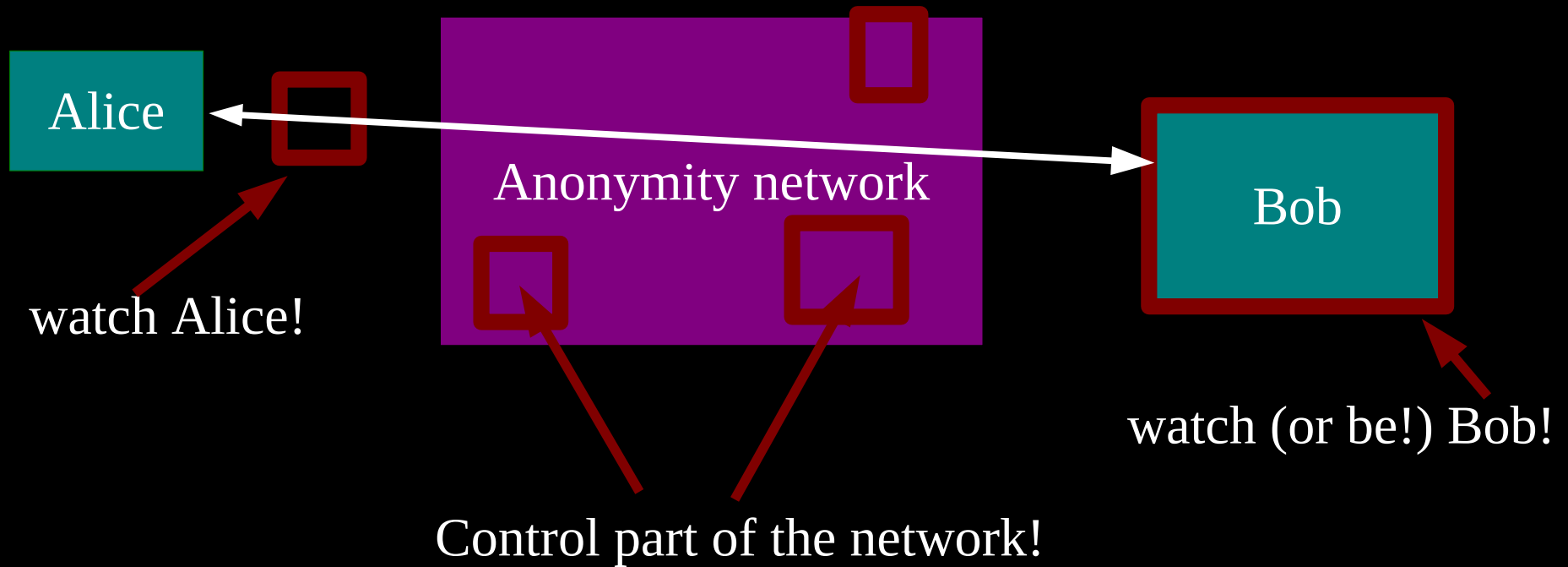


U.S. 501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy

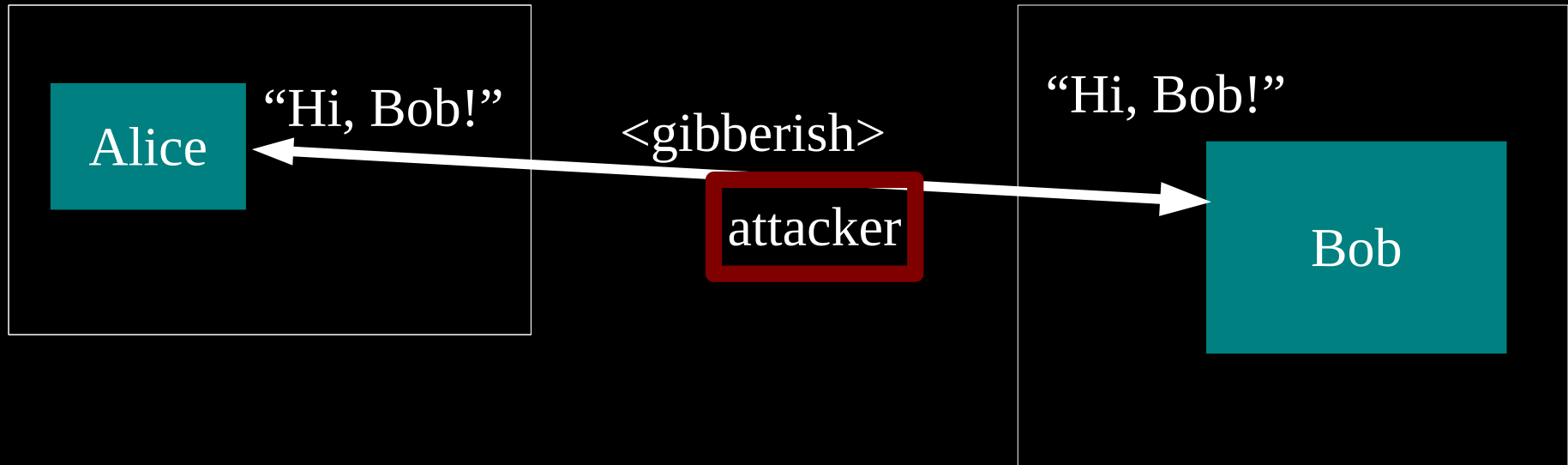


Estimated ~800,000?
daily Tor users

Threat model: what can the attacker do?



Anonymity isn't encryption: Encryption just protects contents.



Anonymity isn't just wishful thinking...

“You can't prove it was me!”

“Promise you won't look!”

“Promise you won't remember!”

“Promise you won't tell!”

“I didn't write my name on it!”

“Isn't the Internet already anonymous?”

Anonymity serves different interests for different user groups.

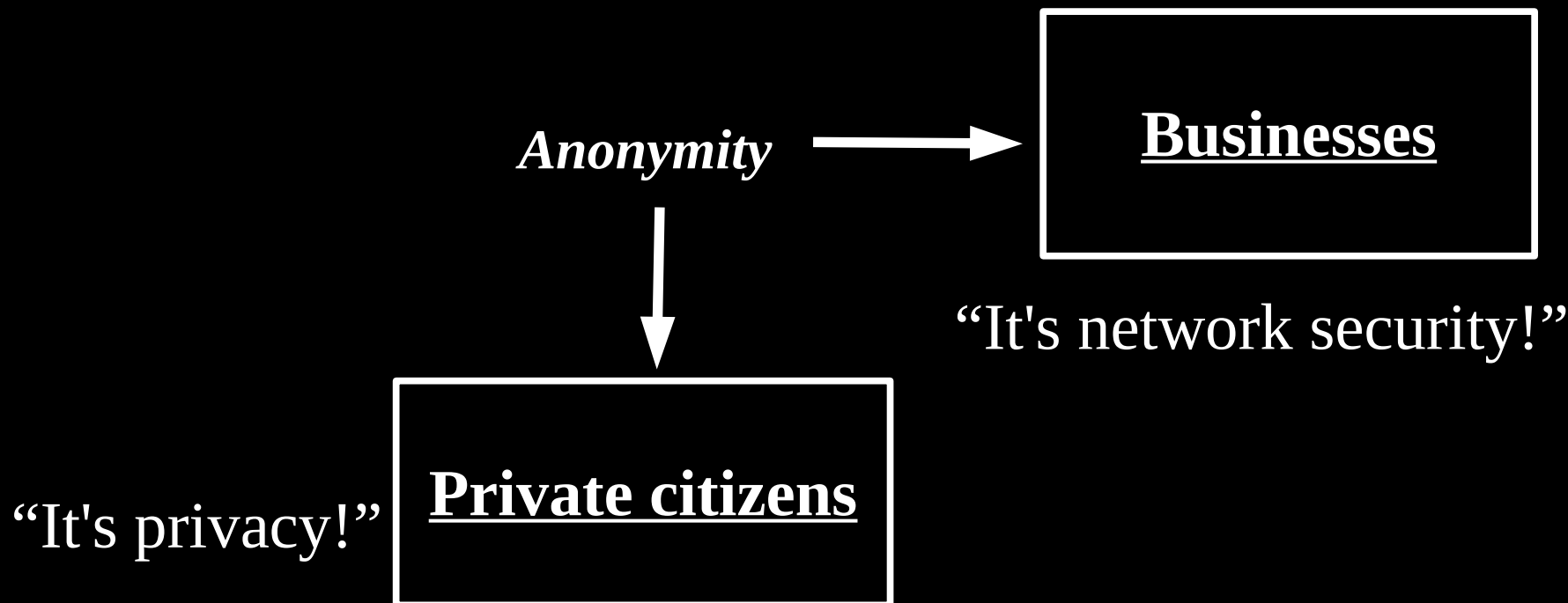
Anonymity



“It's privacy!”

Private citizens

Anonymity serves different interests for different user groups.



Anonymity serves different interests for different user groups.

“It's traffic-analysis resistance!”

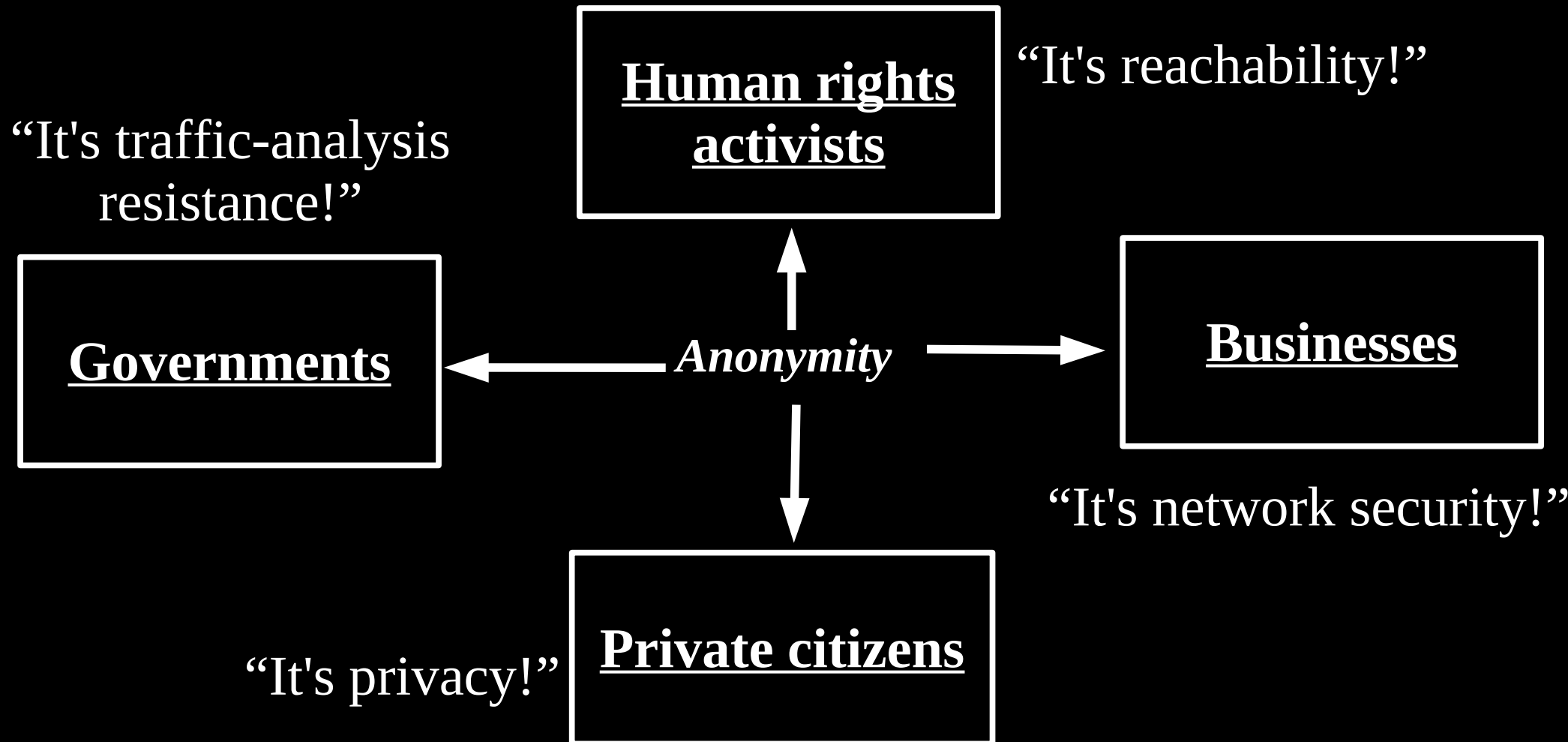


“It's network security!”

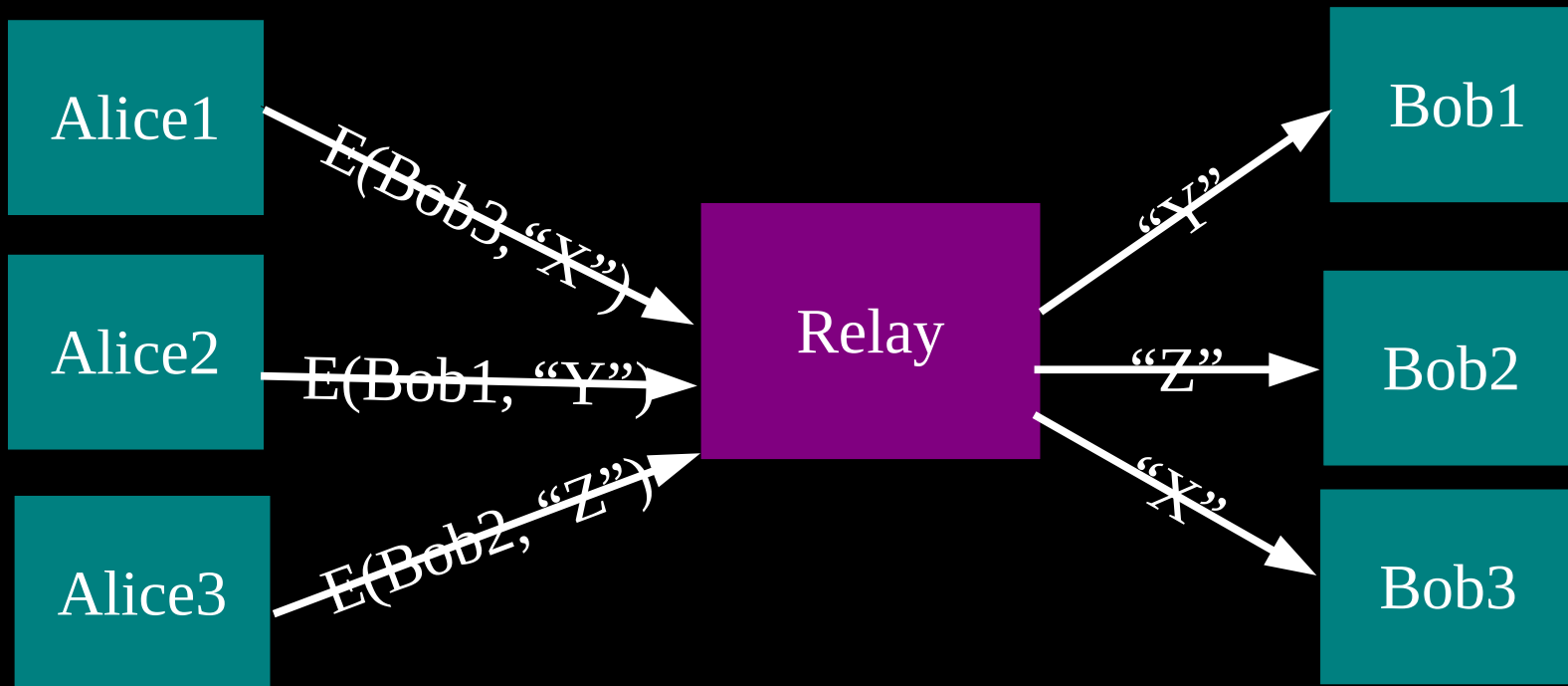
“It's privacy!”



Anonymity serves different interests for different user groups.

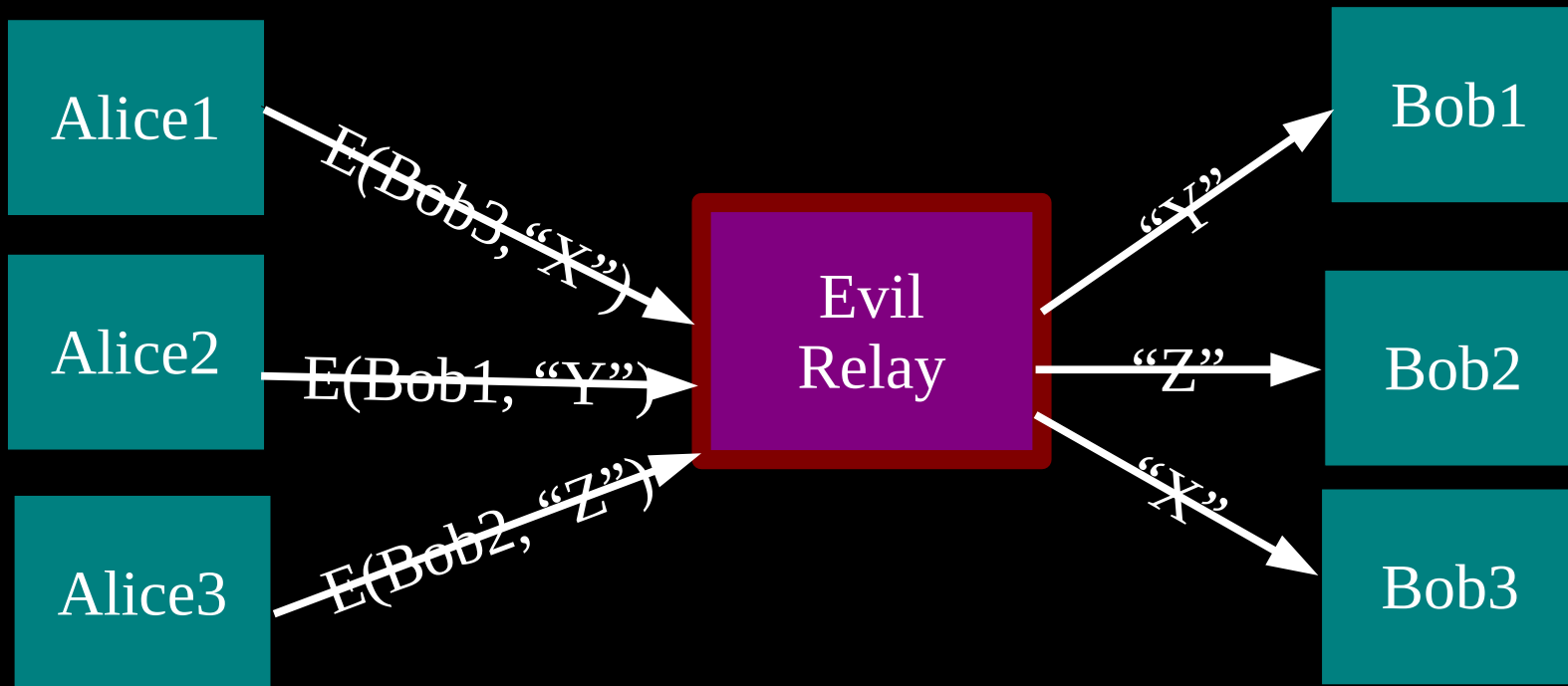


The simplest designs use a single relay to hide connections.

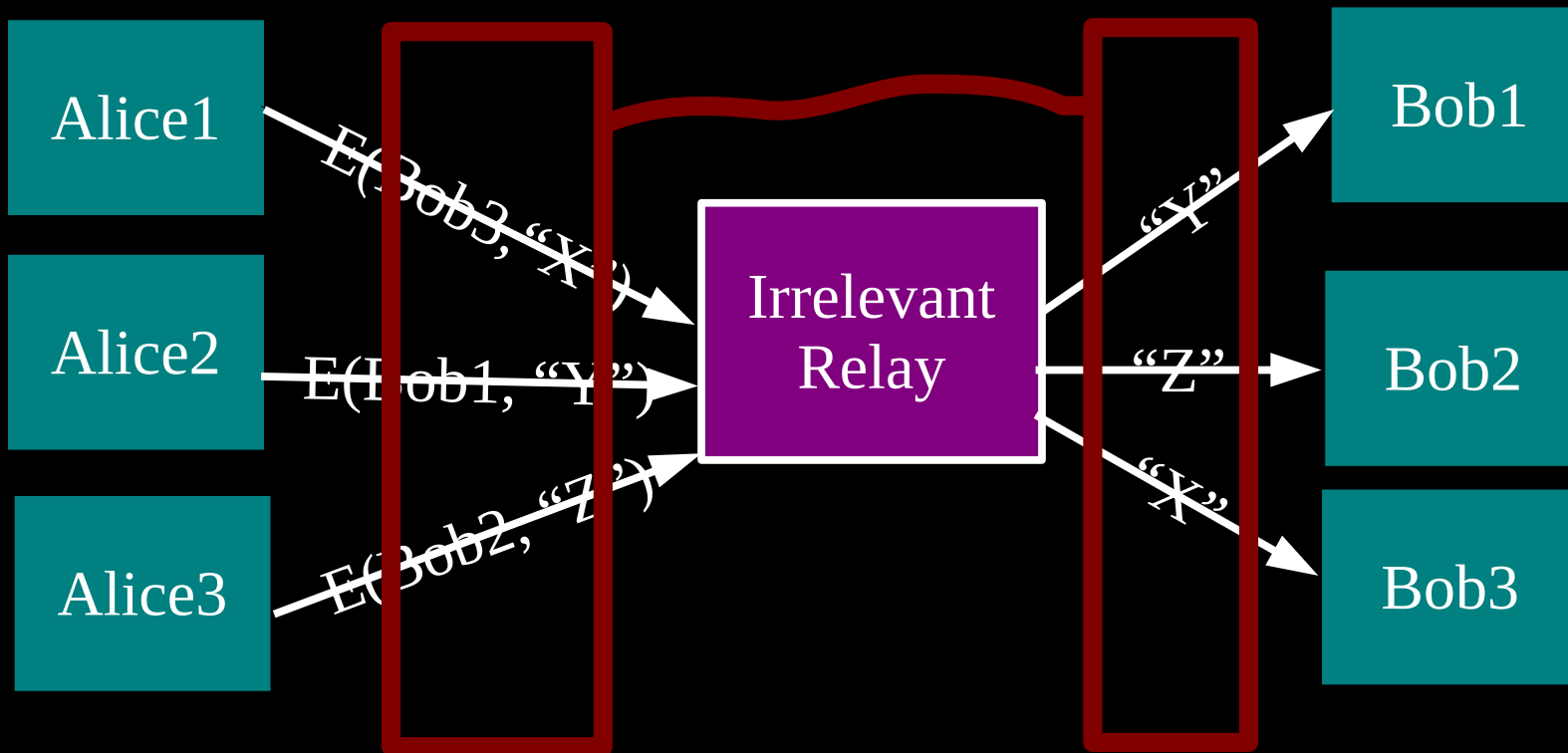


(example: some commercial proxy providers)

**But a single relay (or eavesdropper!)
is a single point of failure.**

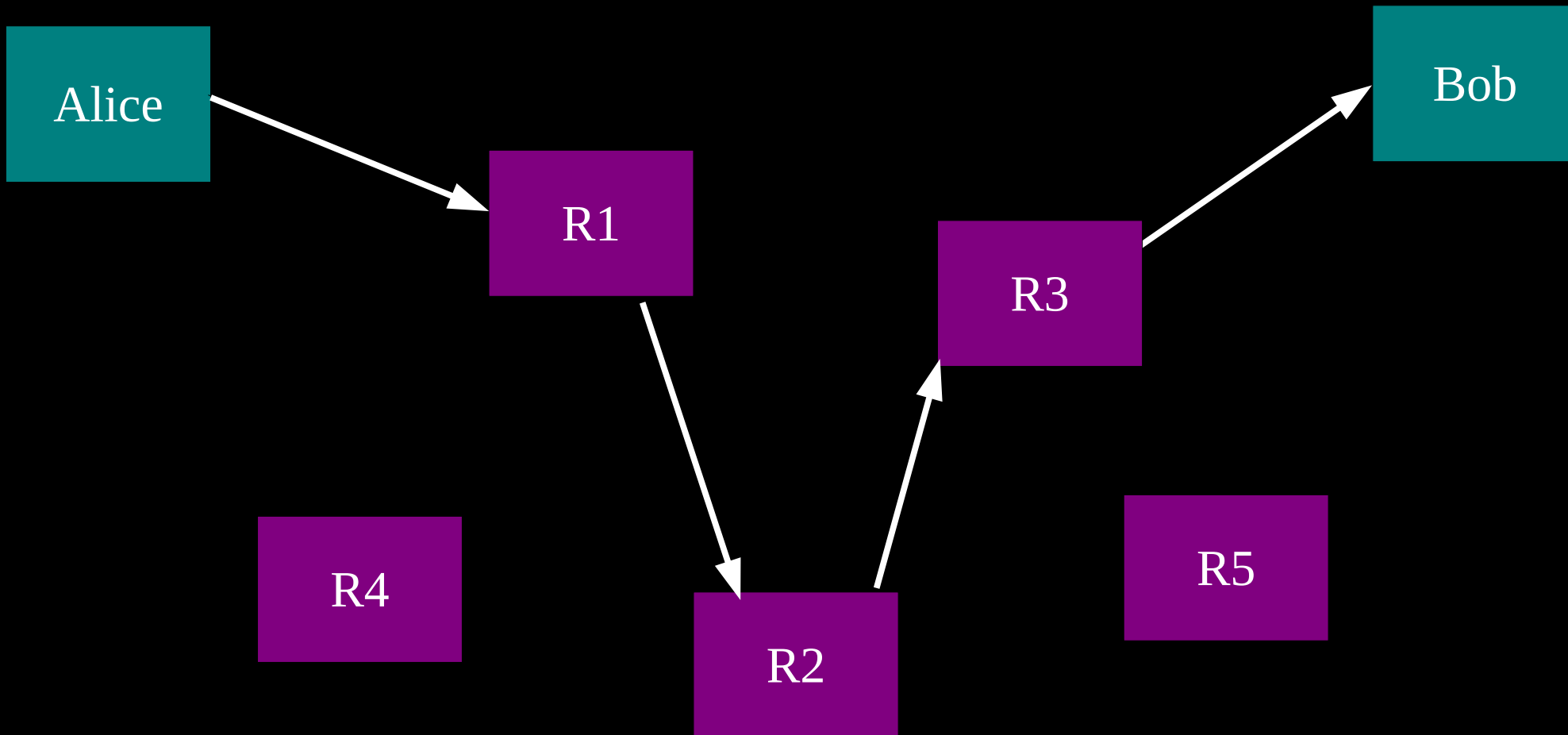


... or a single point of bypass.

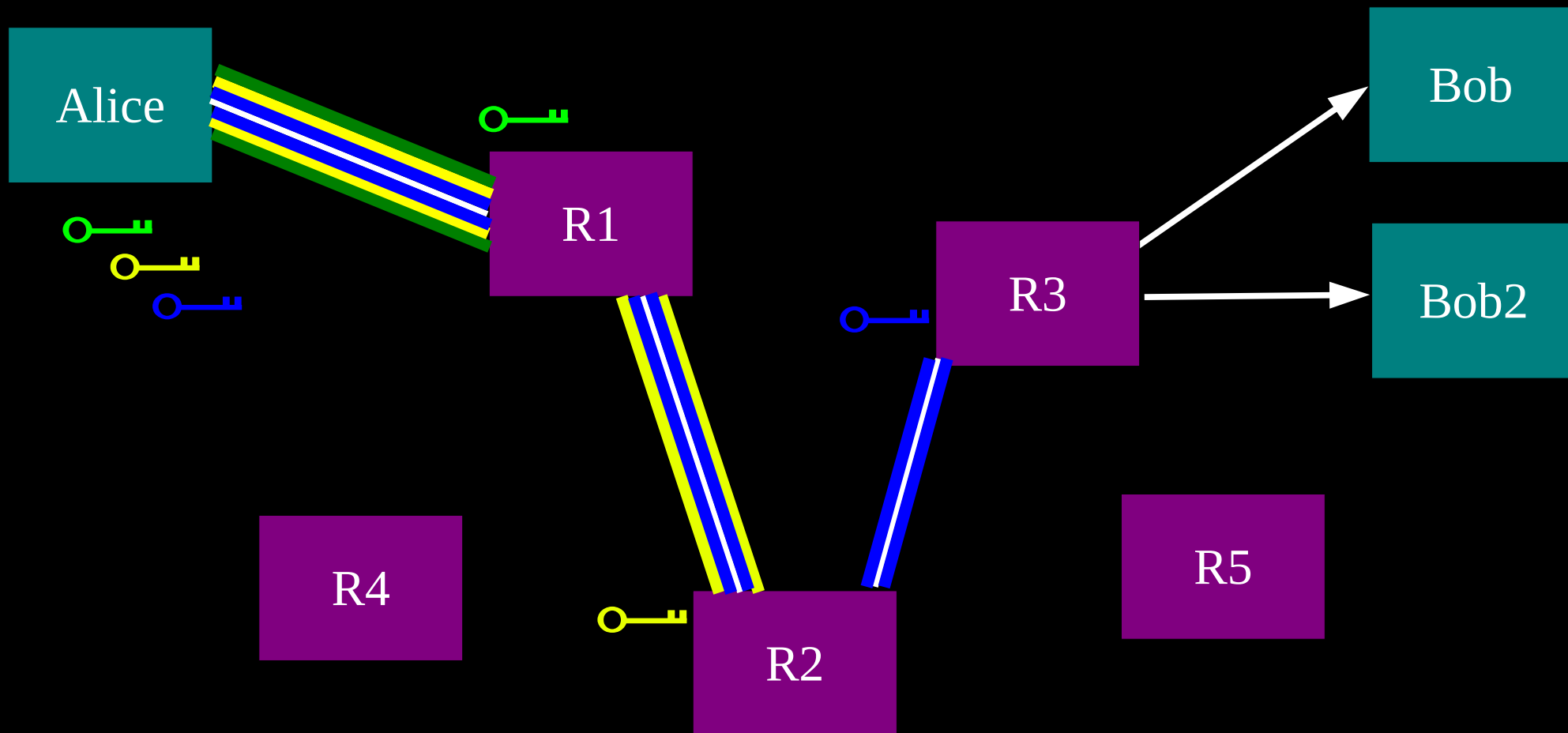


Timing analysis bridges all connections through relay \Rightarrow An attractive fat target

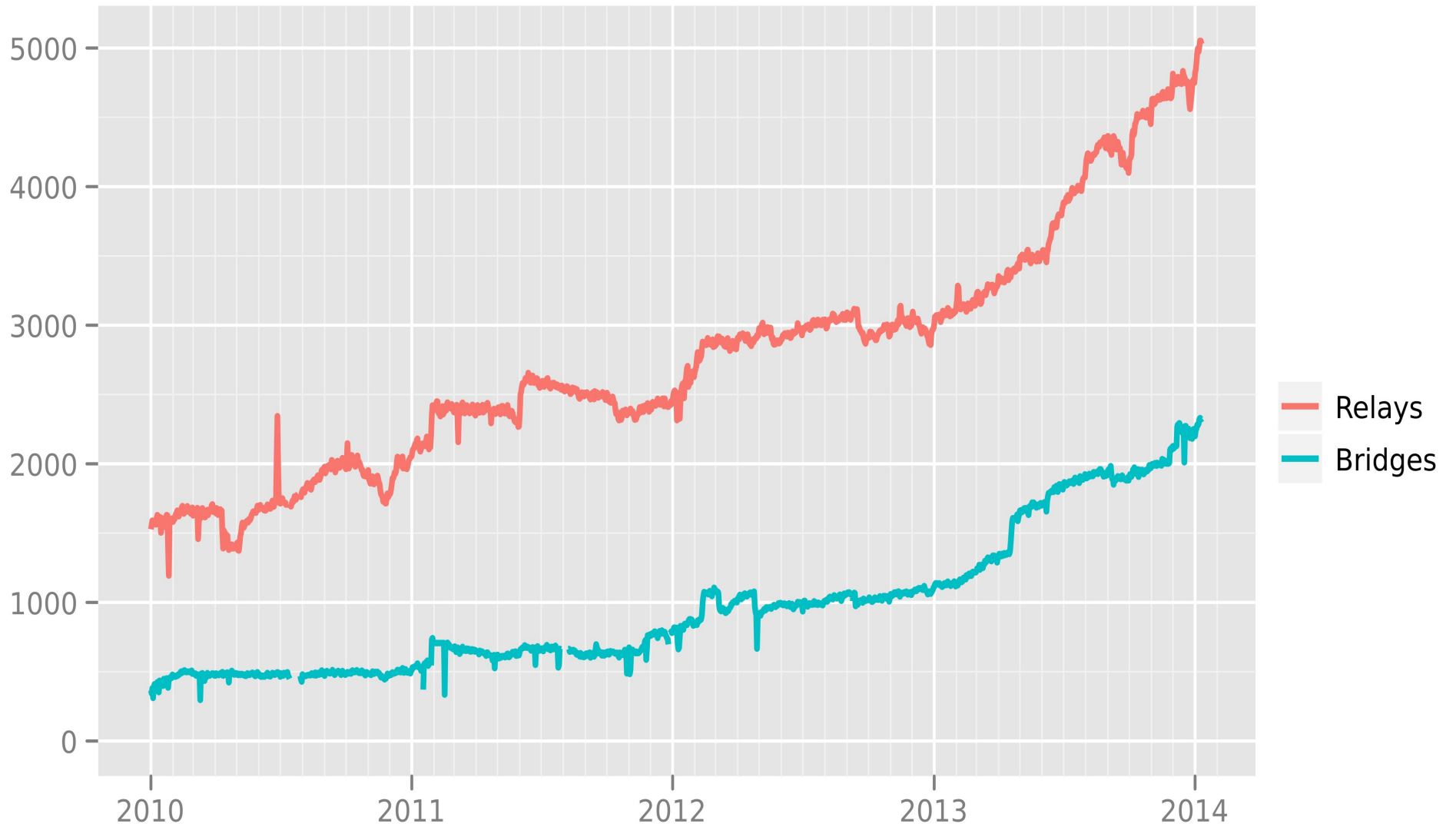
So, add multiple relays so that no single one can betray Alice.



**Alice makes a session key with R1
...And then tunnels to R2...and to R3**



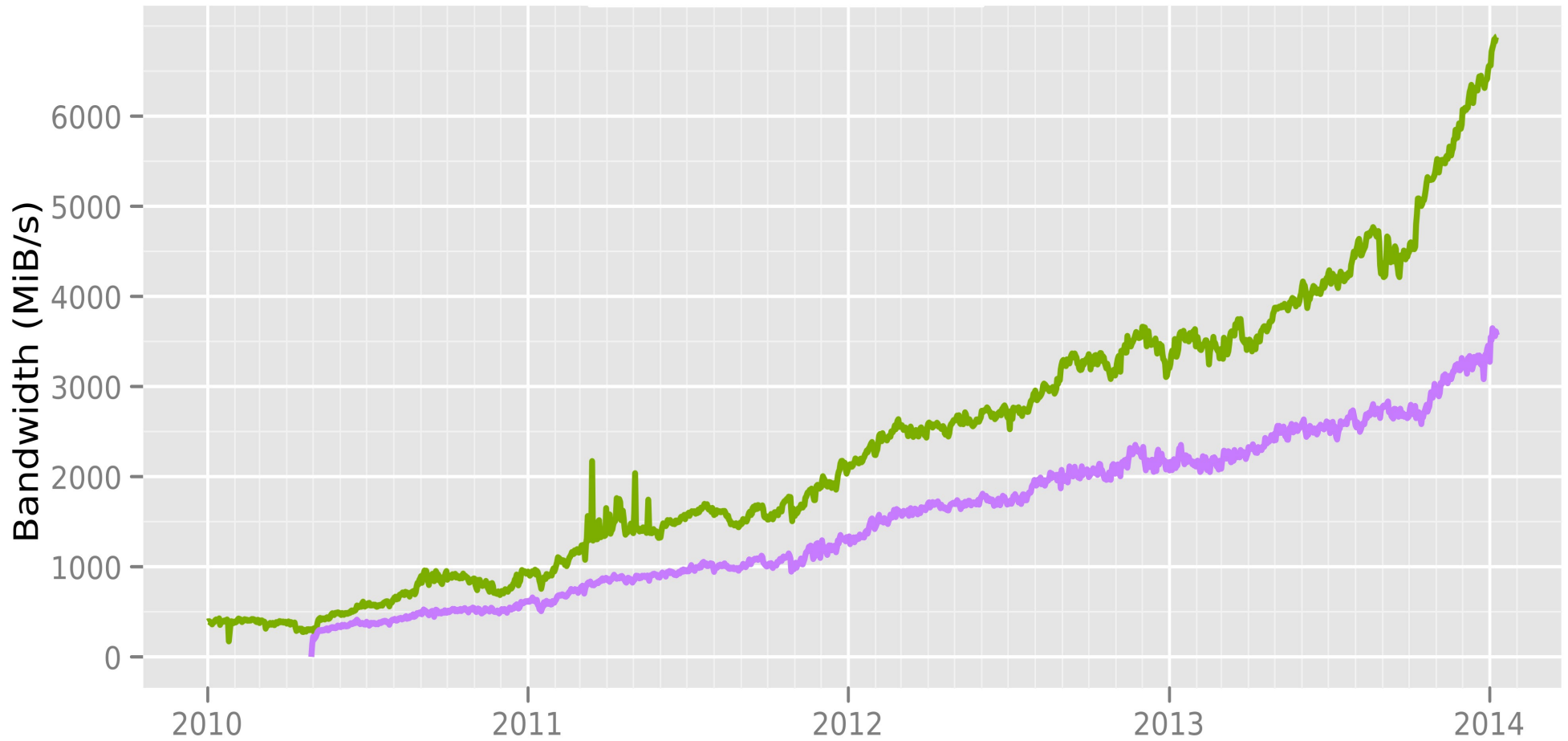
Number of relays



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

Total relay bandwidth

- Advertised bandwidth
- Bandwidth history



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



Tor Research Home

Many people around the world are doing research on how to improve the Tor design, what's going on in the Tor network generally on attacks and defenses for anonymous communication systems. This page summarizes the resources we provide to make your Tor research more effective. The best way to reach us about research is through the [tor-assistants](#) list.

- **Data.** We've been [collecting data to learn more about the Tor network](#): how many relays and clients there are in the network, what capabilities they have, how fast the network is, how many clients are connecting via bridges, what traffic is being carried, etc. We are also developing tools to process these huge data archives and come up with [useful statistics](#). Let us know what other information you'd like to see, and we can work with you to help make sure it gets collected [safely](#) and reliably.
- **Analysis.** If you're investigating Tor, or solving a Tor-related problem, *please* talk to us somewhere along the way, the earlier the better. These days we review too many conference paper submissions that make bad assumptions about solving the wrong problem. Since the Tor protocol and the Tor network are both moving targets, measuring things without understanding what's going on behind the scenes is going to result in bad conclusions. In particular, different groups often unwittingly run a variety of experiments in parallel, and at the same time we're constantly modifying the design and our approaches. If you let us know what you're doing and what you're trying to learn, we can help you understand which variables to expect and how to interpret your results.
- **Measurement and attack tools.** We're building a [repository](#) of tools that can be used to measure, analyze, or attack Tor. Many research groups end up needing to do similar measurements (for example, change the Tor design and then see if latency improves), and we hope to help everybody standardize on a few tools and then make them better. Also, while there are some really neat Tor attacks that people have published about, it's hard to track down a complete list of what they used. Let us know if you have new tools we should list, or improvements to the existing ones. The more the merrier.
- **We need defenses too — not just attacks.** Most researchers find it easy and fun to come up with novel attack ideas for Tor systems. We've seen this result lately in terms of improved congestion attacks, attacks based on remotely measuring throughput, and so on. Knowing how things can go wrong is important, and we recognize that the incentives in the network are aligned with spending energy on designing defenses, but it sure would be great to get more attention to how to defend against attacks. We'd love to help brainstorm about how to make Tor better. As a bonus, your paper might even end up in our "countermeasures" section.
- **In-person help.** If you're doing interesting and important Tor research and need help understanding how the Tor network design works, interpreting your data, crafting your experiments, etc. we can send a Tor researcher to your department.

Tor Controller Interface

- stem
- pytorctl
- jtorctl
- txtorcon

```
meejah@pretend:~/src/txtorcon-github$ make
trial --reporter=text txtorcon.test
.....
.....
.....
-----
Ran 229 tests in 1.140s

PASSED (successes=229)
meejah@pretend:~/src/txtorcon-github$ python examples/launch_tor_endpoint.py
10%: Finishing handshake with directory server
15%: Establishing an encrypted directory connection
20%: Asking for networkstatus consensus
25%: Loading networkstatus consensus
40%: Loading authority key certs
45%: Asking for relay descriptors
80%: Connecting to the Tor network
85%: Finishing handshake with first hop
90%: Establishing a Tor circuit
100%: Done
I have set up a hidden service, advertised at:
http://567zt26xqpvmducs.onion:80
locally listening on IPv4Address(TCP, '0.0.0.0', 31855)
□
```



Tor specs

- The **specifications** aim to give developers enough information to build a compatible version of Tor:
 - Main Tor specification
 - Tor version 3 directory server specification (and older version 2 directory specification)
 - Tor control protocol specification
 - Tor rendezvous specification
 - Tor path selection specification
 - Special hostnames in Tor
 - Tor's SOCKS support and extensions
 - How Tor version numbers work
 - In-progress drafts of new specifications and proposed changes

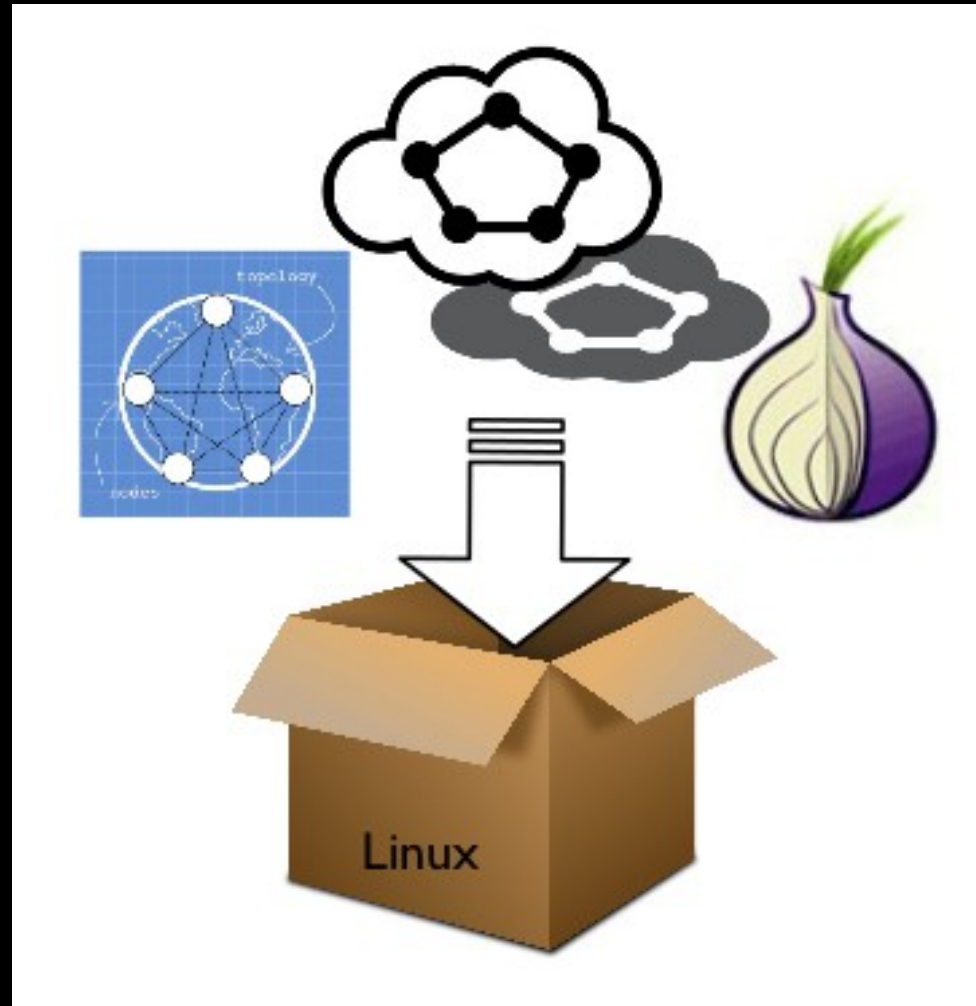
freehaven.net/anonbib/

2012

- ☆ **Congestion-aware Path Selection for Tor** ([PDF](#)) (Cached: [PDF](#))
by Tao Wang, Kevin Bauer, Clara Forero, and [Ian Goldberg](#).
In the Proceedings of Financial Cryptography and Data Security (FC'12), February 2012. ([BibTeX entry](#)) :
- ☆ **BLACR: TTP-Free Blacklistable Anonymous Credentials with Reputation** ([PDF](#)) (Cached: [PDF](#))
by Man Ho Au, Apu Kapadia, and Willy Susilo.
In the Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS), February 2012. ([BibTeX entry](#)) :
- ☆ **Shadow: Running Tor in a Box for Accurate and Efficient Experimentation** ([PDF](#)) (Cached: [PDF](#))
by Rob Jansen and [Nicholas Hopper](#).
In the Proceedings of the Network and Distributed System Security Symposium - NDSS'12, February 2012. ([BibTeX entry](#)) :
- ☆ **Peek-a-Boo, I Still See You: Why Efficient Traffic Analysis Countermeasures Fail** ([PDF](#)) (Cached: [PDF](#))
by Kevin P. Dyer, Scott E. Coull, Thomas Ristenpart, and Thomas Shrimpton.
In the Proceedings of the 2012 IEEE Symposium on Security and Privacy, May 2012. ([BibTeX entry](#)) :
- **LASTor: A Low-Latency AS-Aware Tor Client** ([PDF](#)) (Cached: [PDF](#))
by Masoud Akhondji, Curtis Yu, and Harsha V. Madhyastha.
In the Proceedings of the 2012 IEEE Symposium on Security and Privacy, May 2012. ([BibTeX entry](#)) :
- **LAP: Lightweight Anonymity and Privacy** ([PDF](#)) (Cached: [PDF](#))
by Hsu-Chun Hsiao, Tiffany Hyun-Jin Kim, Adrian Perrig, Akira Yamada, Sam Nelson, Marco Gruteser, and Wei Ming.
In the Proceedings of the 2012 IEEE Symposium on Security and Privacy, May 2012. ([BibTeX entry](#)) :
- **How (not) to build a transport layer for anonymity overlays** ([PDF](#)) (Cached: [PDF](#))

Tor network simulators

- **Shadow**
- **ExperimenTor**
- **Chutney**
- **Puppetor**

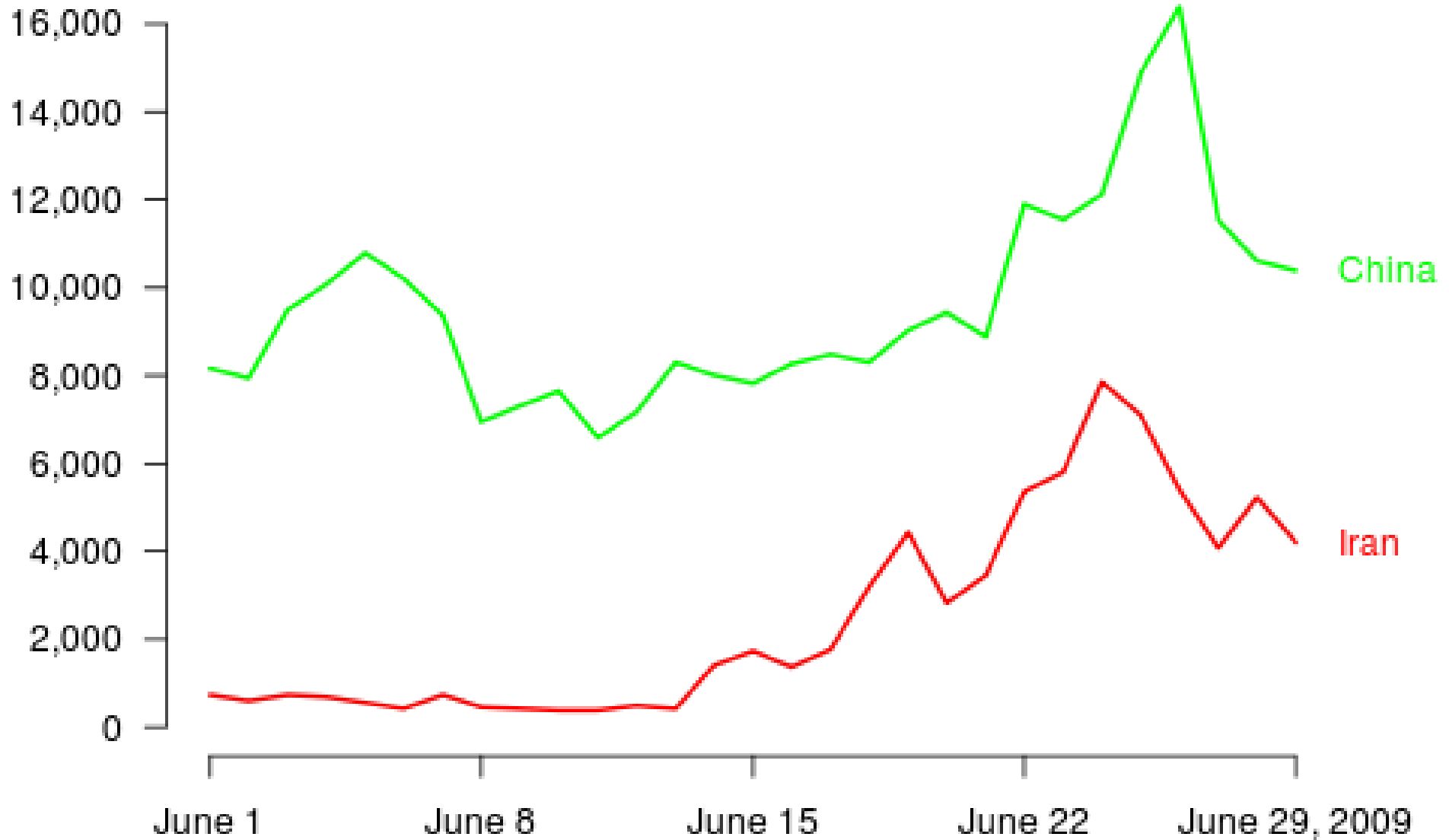


Relay descriptor archives

The relay descriptor archives contain all documents that the directory authorities make available about the network of relays. They include network statuses, server (relay) descriptors, and extra-info descriptors. The data formats are described [here](#).

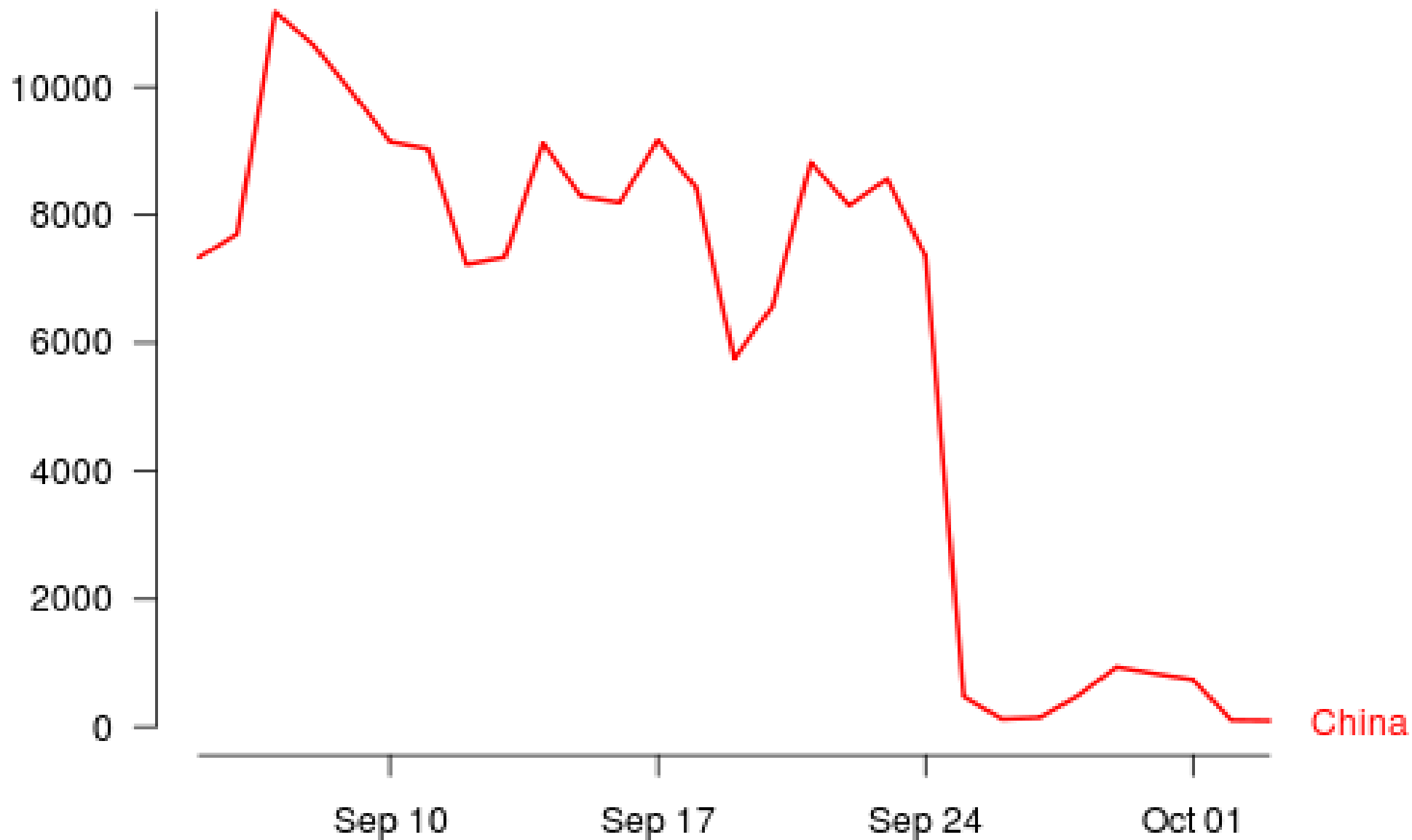
May 2013		server descriptors	extra-infos	v3 votes	v3 statuses
April 2013		server descriptors	extra-infos	v3 votes	v3 statuses
March 2013		server descriptors	extra-infos	v3 votes	v3 statuses
February 2013		server descriptors	extra-infos	v3 votes	v3 statuses
January 2013		server descriptors	extra-infos	v3 votes	v3 statuses
December 2012		server descriptors	extra-infos	v3 votes	v3 statuses
November 2012		server descriptors	extra-infos	v3 votes	v3 statuses
October 2012		server descriptors	extra-infos	v3 votes	v3 statuses
September 2012		server descriptors	extra-infos	v3 votes	v3 statuses
August 2012		server descriptors	extra-infos	v3 votes	v3 statuses
July 2012		server descriptors	extra-infos	v3 votes	v3 statuses
June 2012		server descriptors	extra-infos	v3 votes	v3 statuses
May 2012		server descriptors	extra-infos	v3 votes	v3 statuses
April 2012		server descriptors	extra-infos	v3 votes	v3 statuses
March 2012	v2 statuses	server descriptors	extra-infos	v3 votes	v3 statuses
February 2012	v2 statuses	server descriptors	extra-infos	v3 votes	v3 statuses
January 2012	v2 statuses	server descriptors	extra-infos	v3 votes	v3 statuses
December 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v3 statuses
November 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v3 statuses
October 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v3 statuses
September 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v3 statuses
August 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v3 statuses

New or returning Tor clients per day



<https://torproject.org>

Number of directory requests to directory mirror trusted



<https://torproject.org>

Attackers can block users from connecting to the Tor network

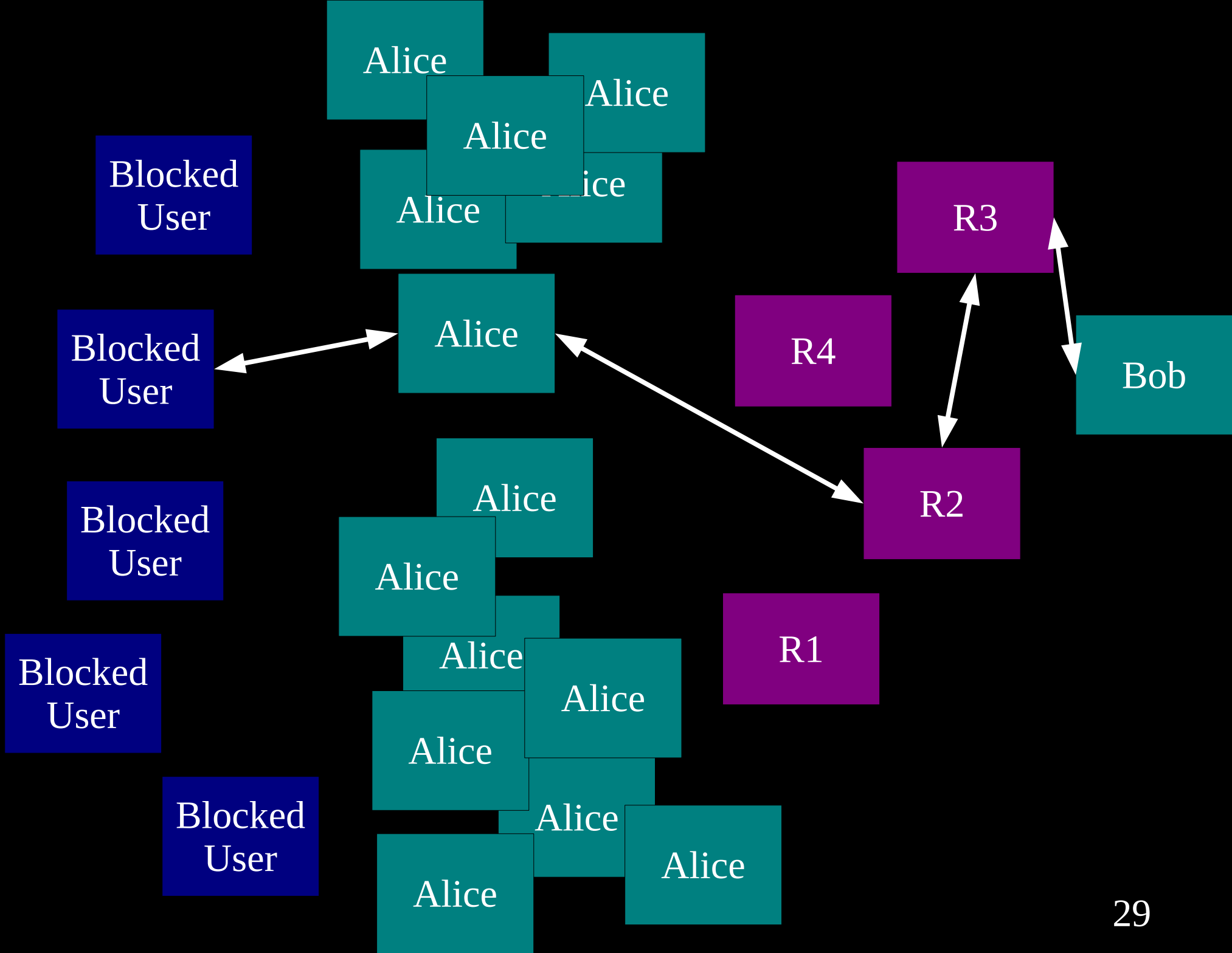
- 1) By blocking the directory authorities
- 2) By blocking all the relay IP addresses in the directory, or the addresses of other Tor services
- 3) By filtering based on Tor's network fingerprint
- 4) By preventing users from finding the Tor software (usually by blocking website)

Relay versus Discovery

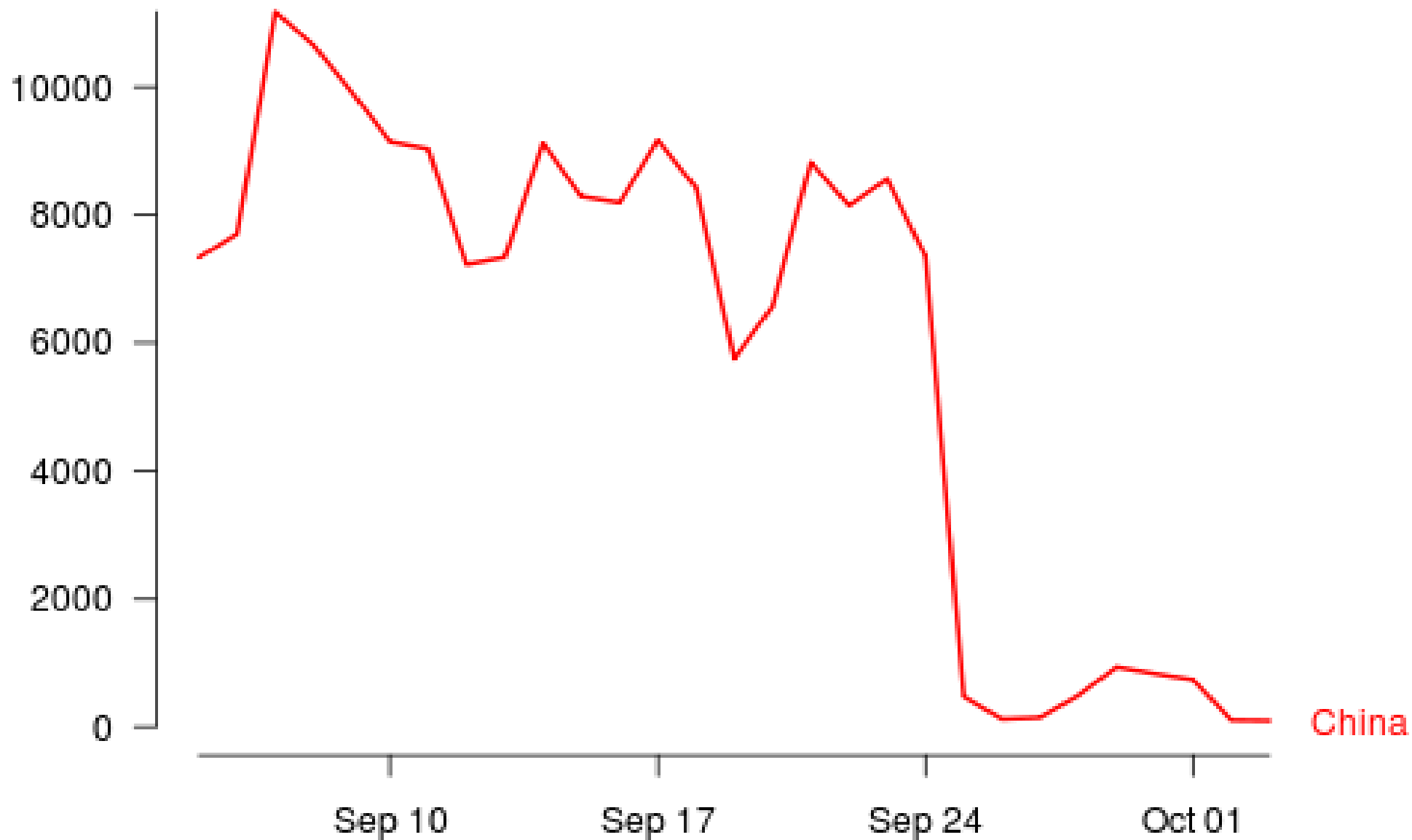
There are two pieces to all these “proxying” schemes:

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

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

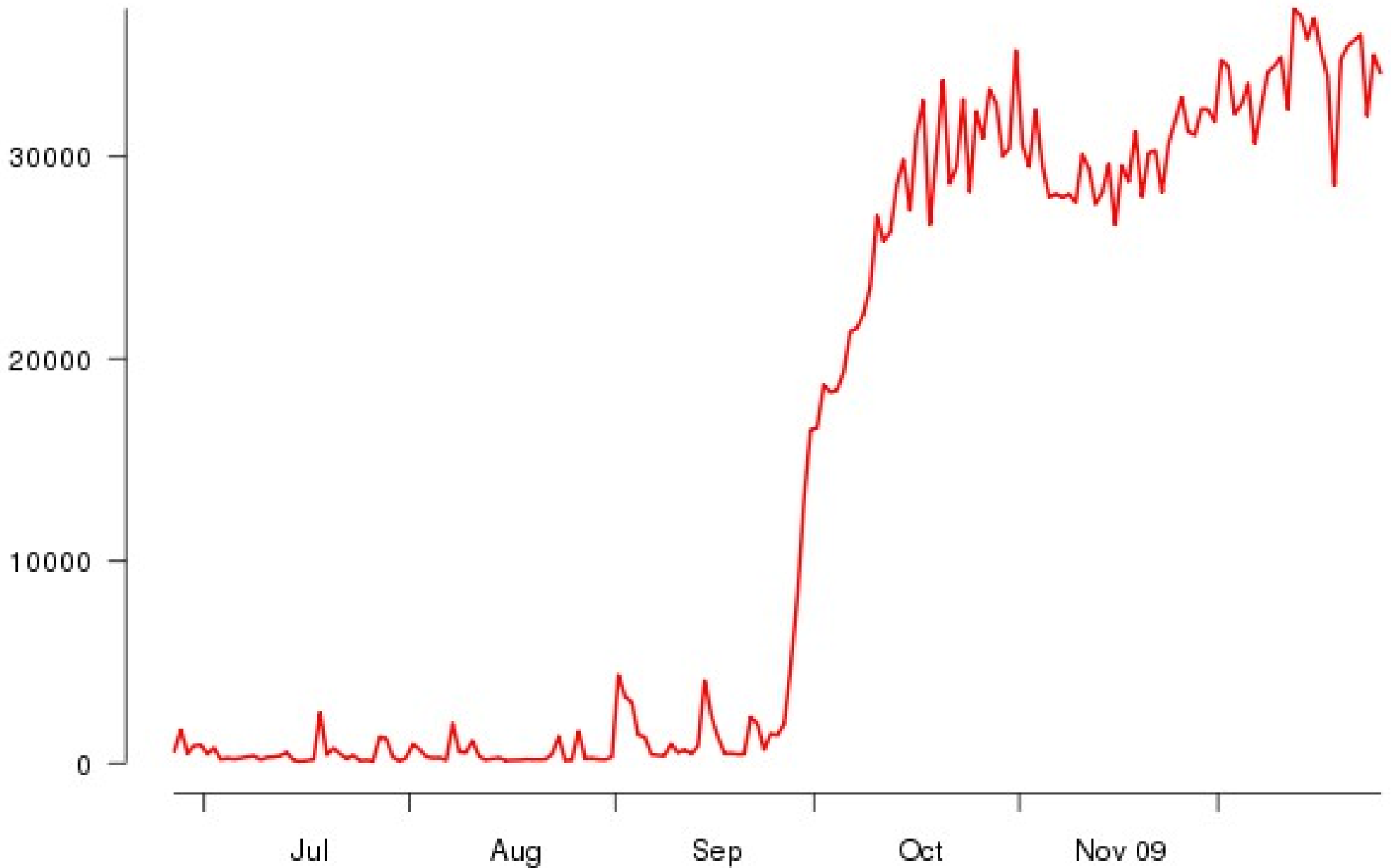


Number of directory requests to directory mirror trusted

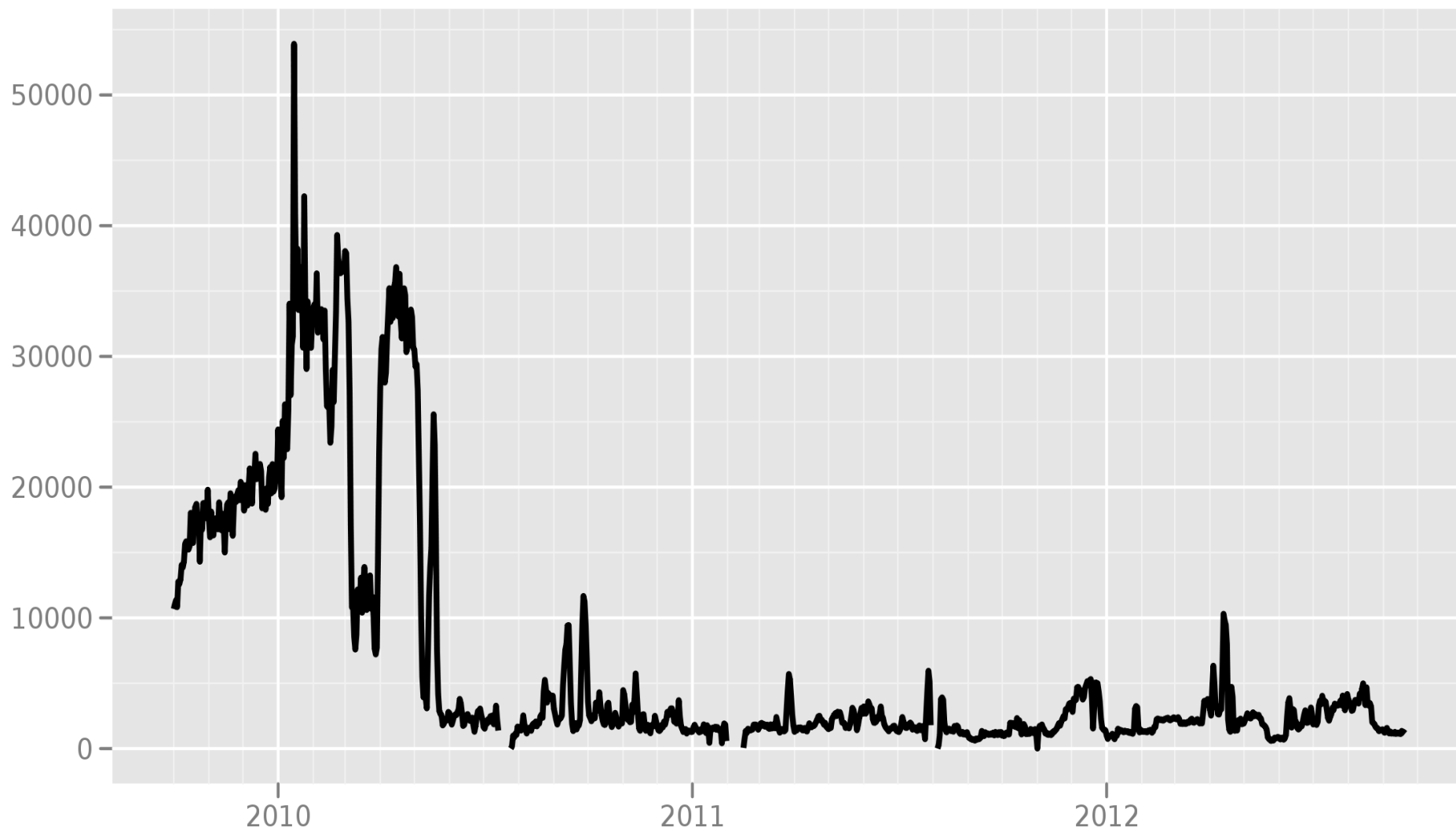


<https://torproject.org>

Chinese Tor users via bridges



Bridge users from China



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

خطراً!



تصفح بأمان!

عذراً، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.
تشكل شبكة الإنترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتماله محتوى مدرج تحت "فئات المحتويات المخظورة" حسب تصنيف "السياسة التنظيمية لإدارة النفاذ للإنترنت" لهيئة تنظيم الاتصالات بدولة الإمارات العربية المتحدة.

إذا كانت لديك وجهة نظر مختلفة، الرجاء انقر [هنا](#).

Surf Safely!

This website is not accessible in the UAE.

The Internet is a powerful medium for communication, sharing and serving our daily learning needs. However, the site you are trying to access contains content that is prohibited under the "Internet Access Management Regulatory Policy" of the Telecommunications Regulatory Authority of the United Arab Emirates.

If you believe the website you are trying to access does not contain any such content, please [click here](#).

© 2009 Launching IT LLC

يالله بالستر...!



ببيرة المتحدة.

وخدمة متطلبات بدخوله لاشتماله "ة" حسب تصنيف تنظيم الاتصالات

Surf Safe

This website is

The Internet is a p serving our daily le access contains con

Your request was denied because of its conte

9:28 AM
3G
Site Blocke... x
+

ء على اللوائح والقوانين مع [unblock.kw@kw.zain](#)

<http://torproject.org/>

<http://torproject.org/>

Site Blocked

eb site has been blocked for violating tions and laws of Kingdom of Bahrain.

نوابين في مملكته

elieve the requested page should be blocked please [click here](#).

تجب تفعل بالضغط

Notice...

تم حظر هذا الموقع بسبب اجتهاده على محتويات تعارض مع قوانين السلطنة. عليه يرجى تعبئة الاستمارة أدناه اذا كنت تعتقد بان الموقع لا يتضمن أي من هذه المحتويات.

This site has been blocked due to content that is contrary to the laws of the Sultanate. if you believe that the website you are trying to access does not contain any such content, please fill in and submit the form below:

WebSite*

Email Address*

Comments*

غير متاح.

ي أن لا تُحجب

المملكة العربية
www.internet.go

10:00 AM

Blocked URL

Sorry, the requested page is unavailable.

قاع المطلوب غير متاح.

If you believe the requested page should not be blocked please [click here](#).

هذه الصفحة ينبغي ان لا تُحجب فضل بالضغط هنا.

For more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa

للمزيد من المعلومات عن خدمة الإنترنت في المملكة العربية السعودية، انقر هنا: www.internet.gov.sa

KT WATA... 9:21 ص 87%

Tweet Blocked by Mada Com...

هذا الموقع محظور

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.

مضى للإصالات
mada Mada Communications

ان الموقع الذي حاول زيارته محجوب

Access to this website is prohibited

ان الموقع الذي حاول زيارته محجوب وذلك طبقاً للقوانين واللوائح المتبعة بهذا الشأن. اذا كنت تعتقد ان هذا الموقع قد تم حجبه عن طريق الخطأ يرجى تعبئة الاستمارة التالية وارسلها للقيام بمعالجة الموقع. شكراً جزيلاً

This site is blocked according to the government 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 * الاسم

Email * العنوان الإلكتروني

Blocked URL * www. .com اسم النطاق

Comments استفسارك

Submit

oops رُفَا

لقد تم منع الدخول إلى هذا الموقع

This site has been blocked

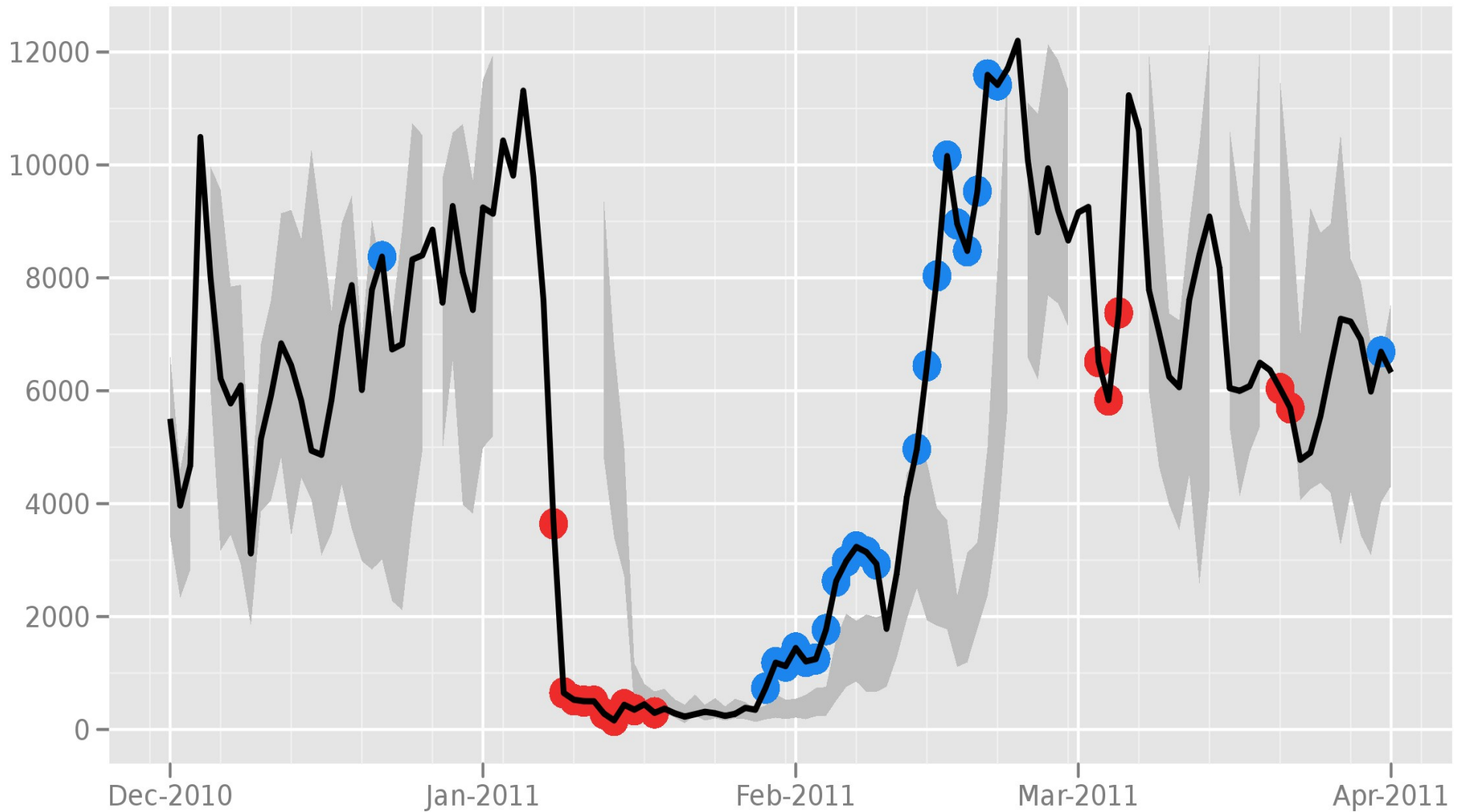
تم إيقاف عملية الدخول إلى الموقع الذي تحاول زيارته نظراً لاحتوائه على محتويات محظورة

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 help@isp.qa

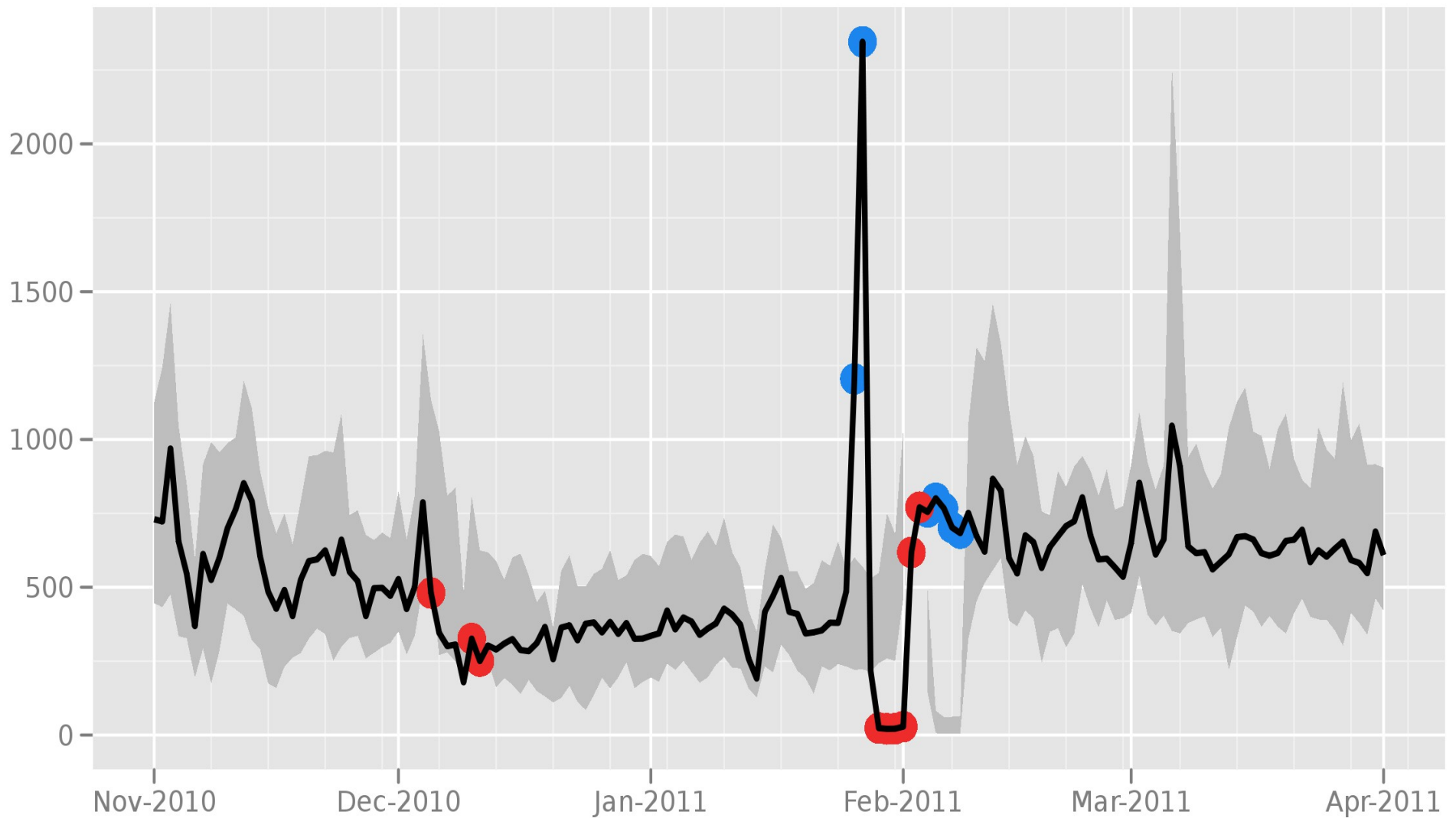
If you feel this is an error then please send

Directly connecting users from the Islamic Republic of Iran



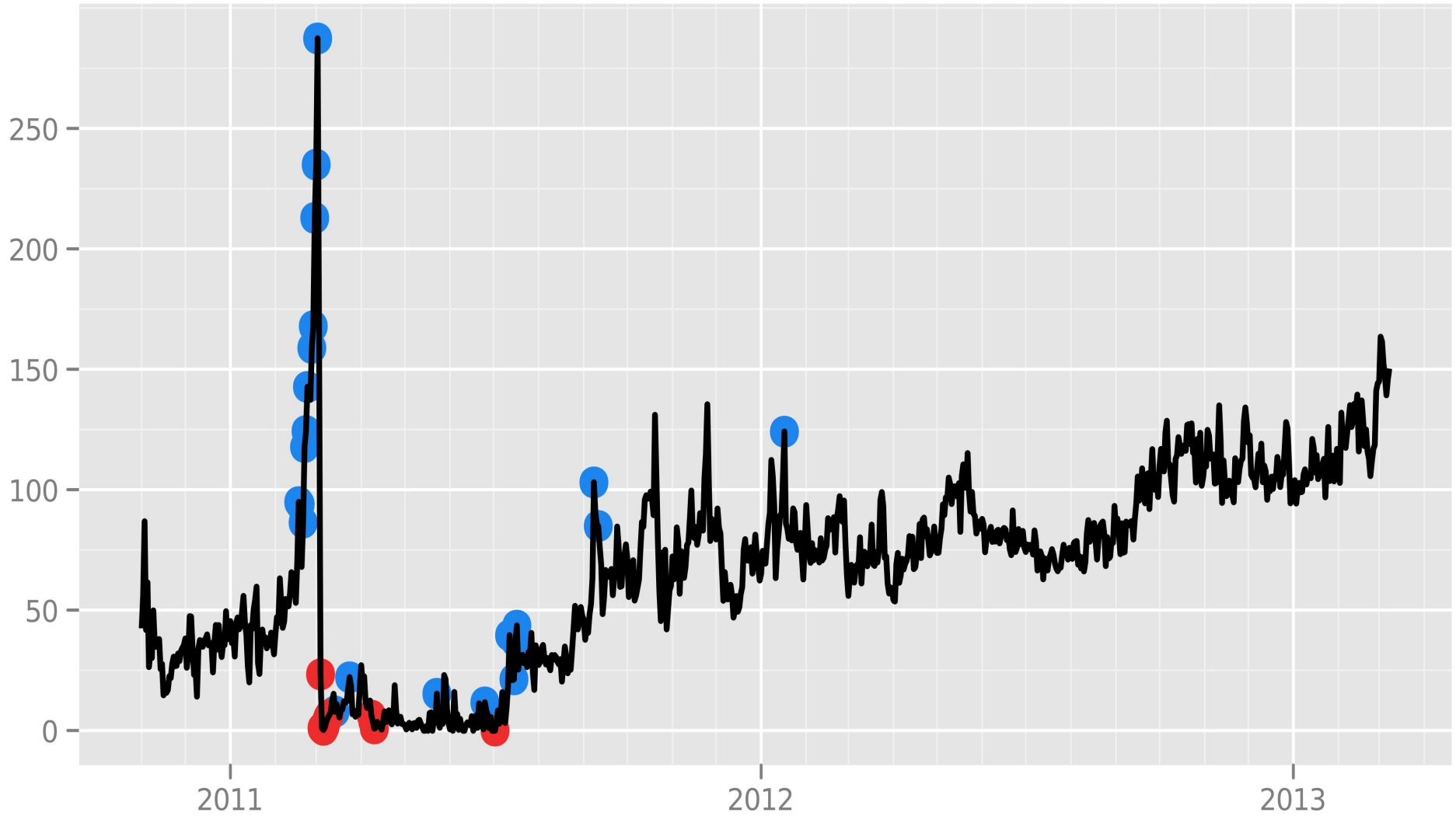
The Tor Project - <https://metrics.torproject.org/>

Directly connecting users from Egypt



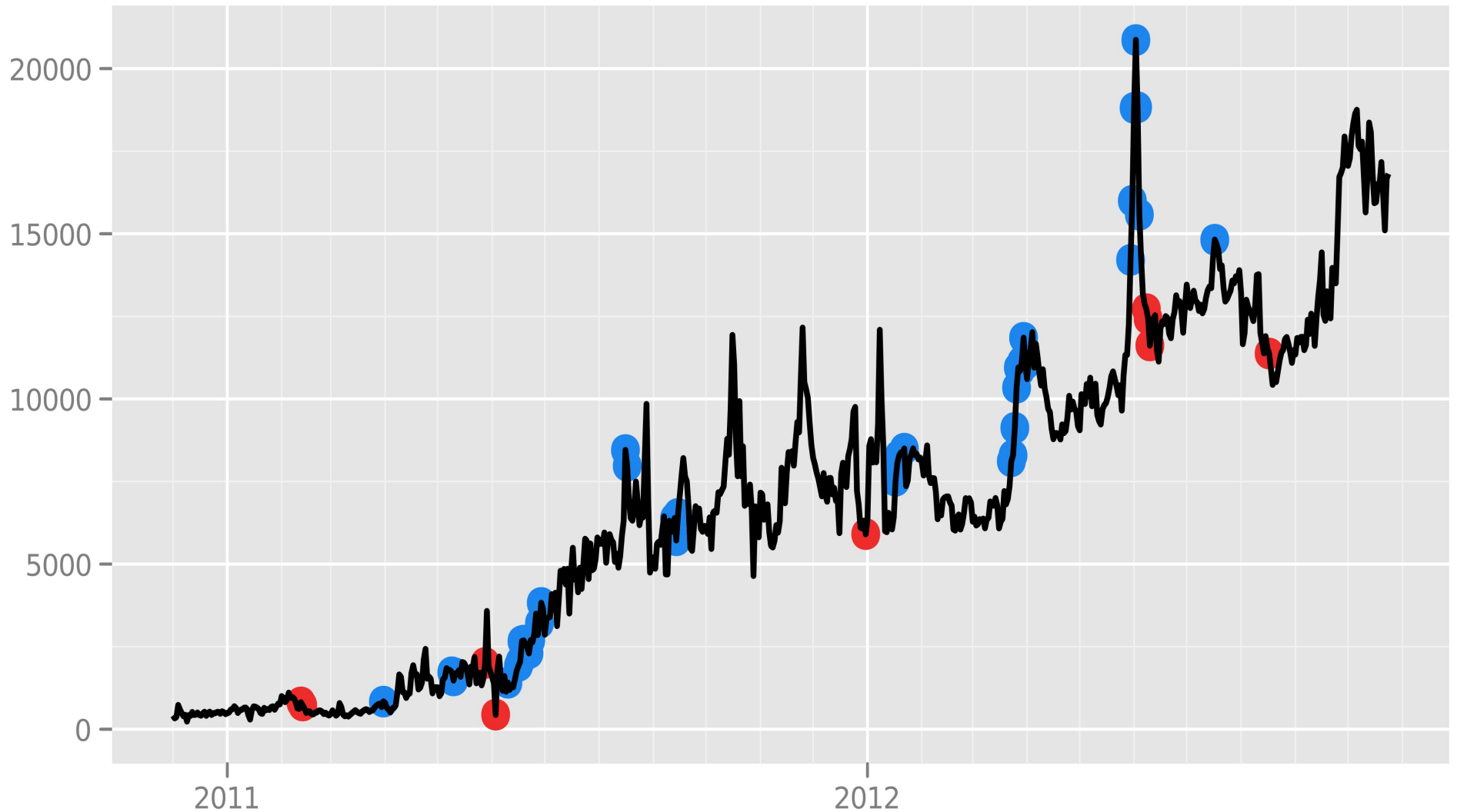
The Tor Project - <https://metrics.torproject.org/>

Directly connecting users from Libya



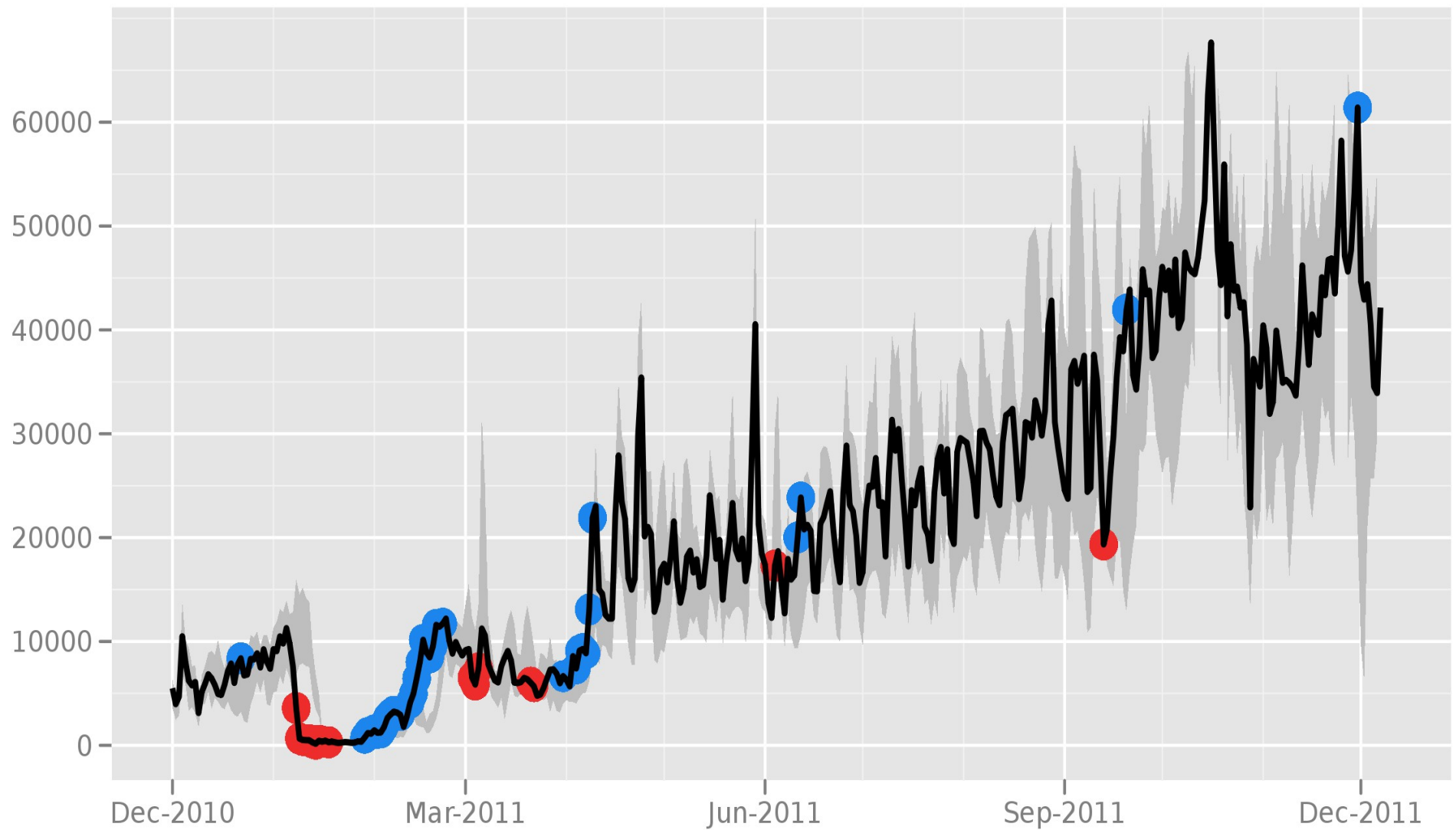
The Tor Project - <https://metrics.torproject.org/>

Directly connecting users from the Syrian Arab Republic



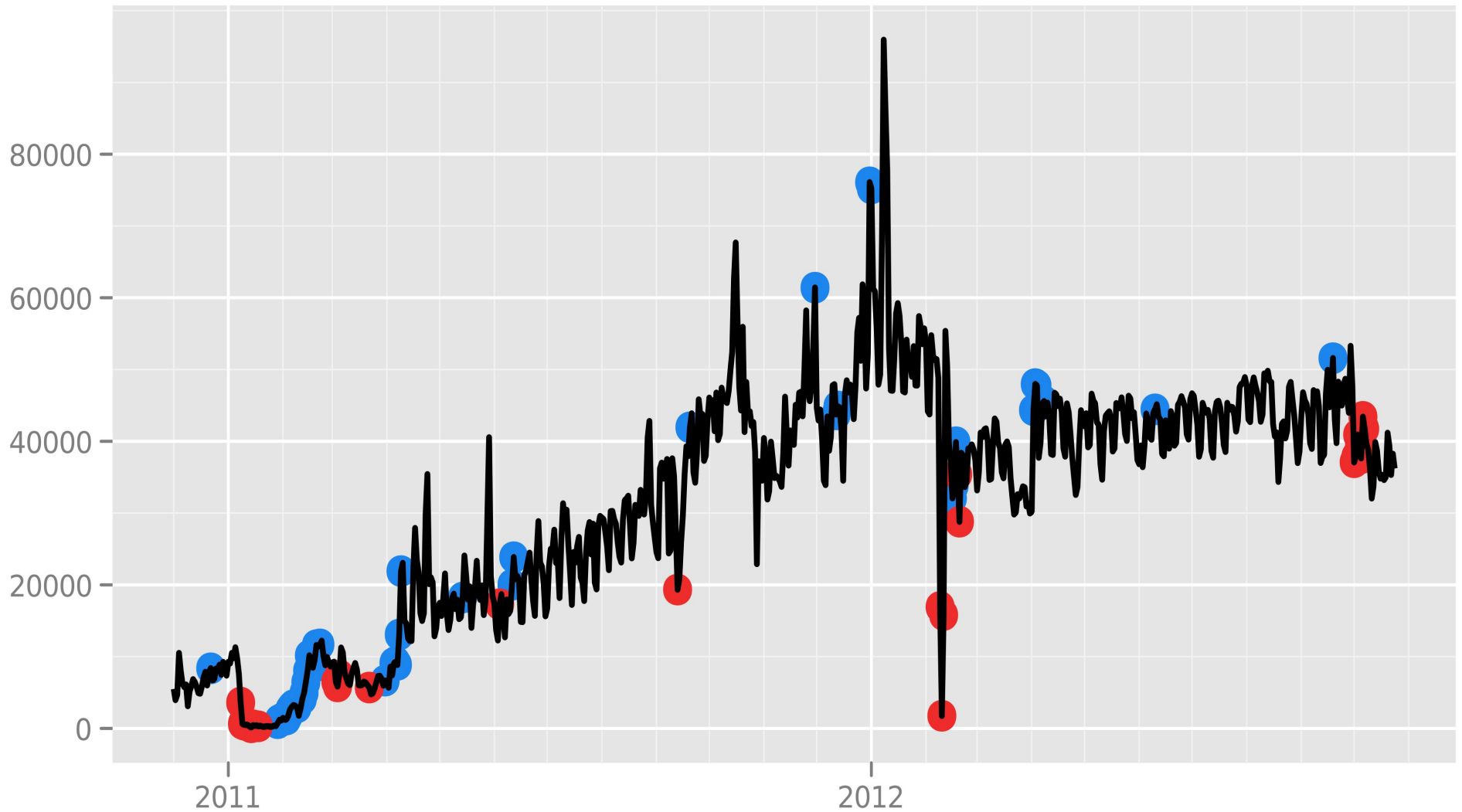
The Tor Project - <https://metrics.torproject.org/>

Directly connecting users from the Islamic Republic of Iran



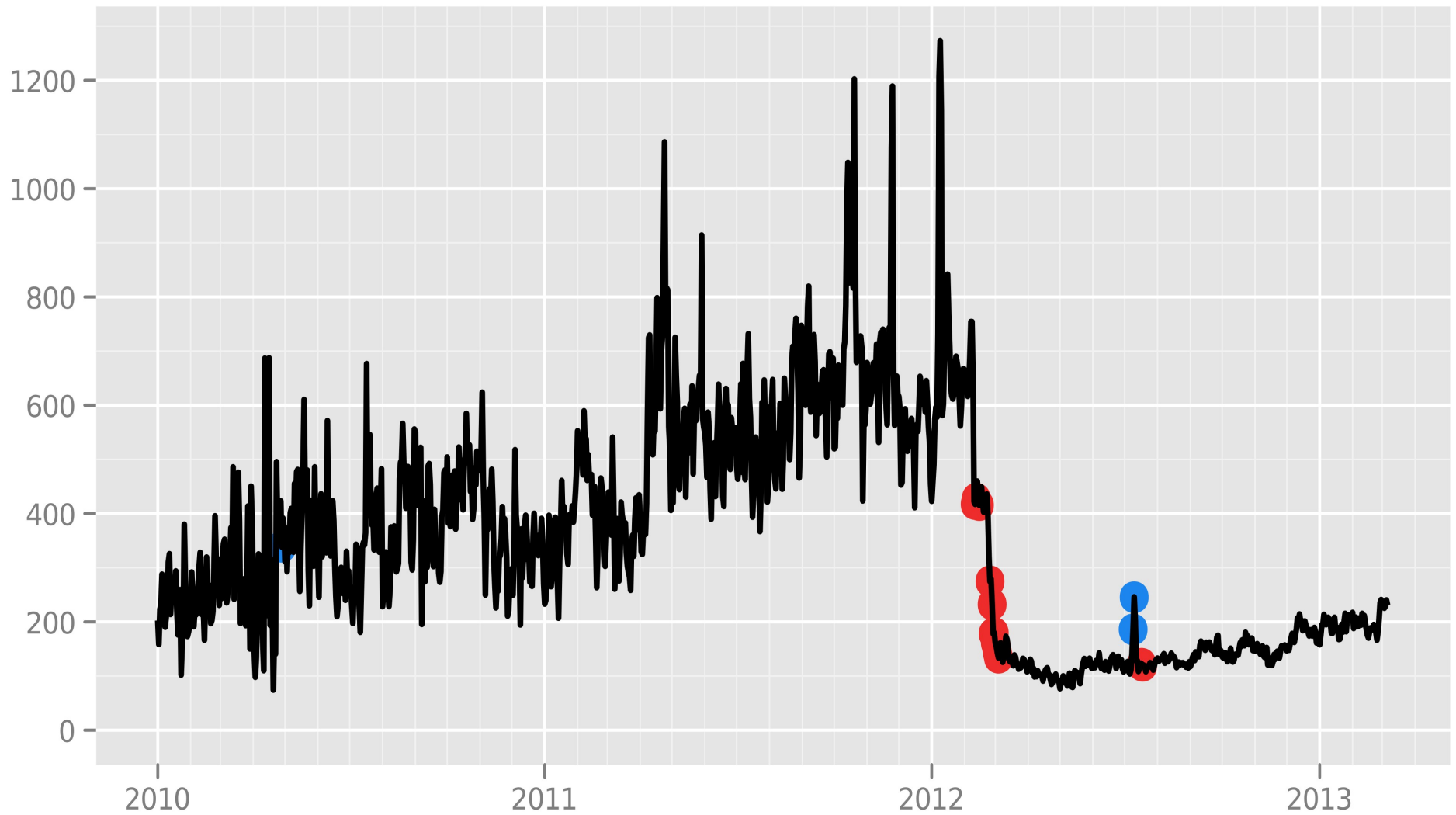
The Tor Project - <https://metrics.torproject.org/>

Directly connecting users from Iran



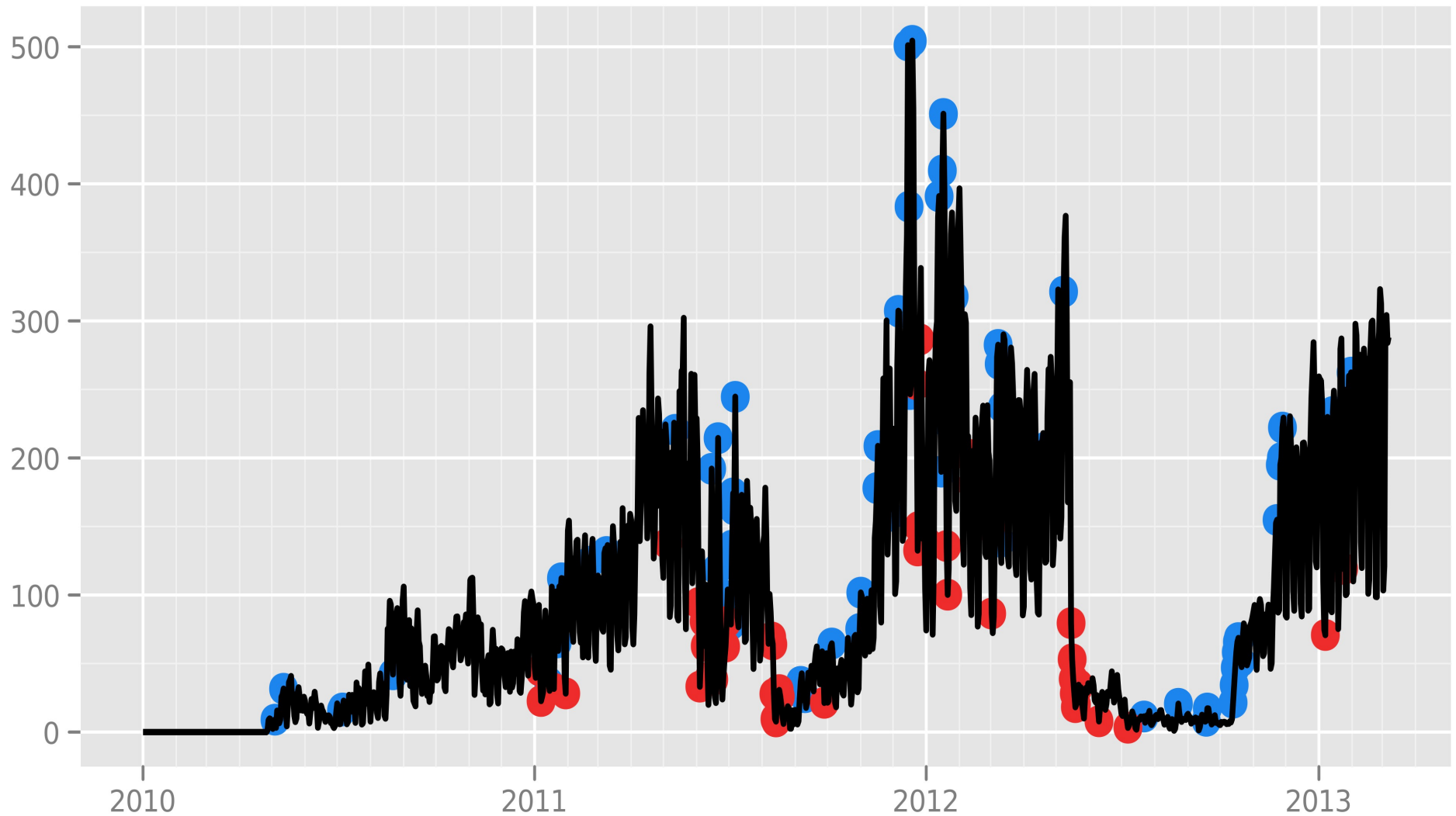
The Tor Project - <https://metrics.torproject.org/>

Directly connecting users from Kazakhstan



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

Directly connecting users from Ethiopia



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

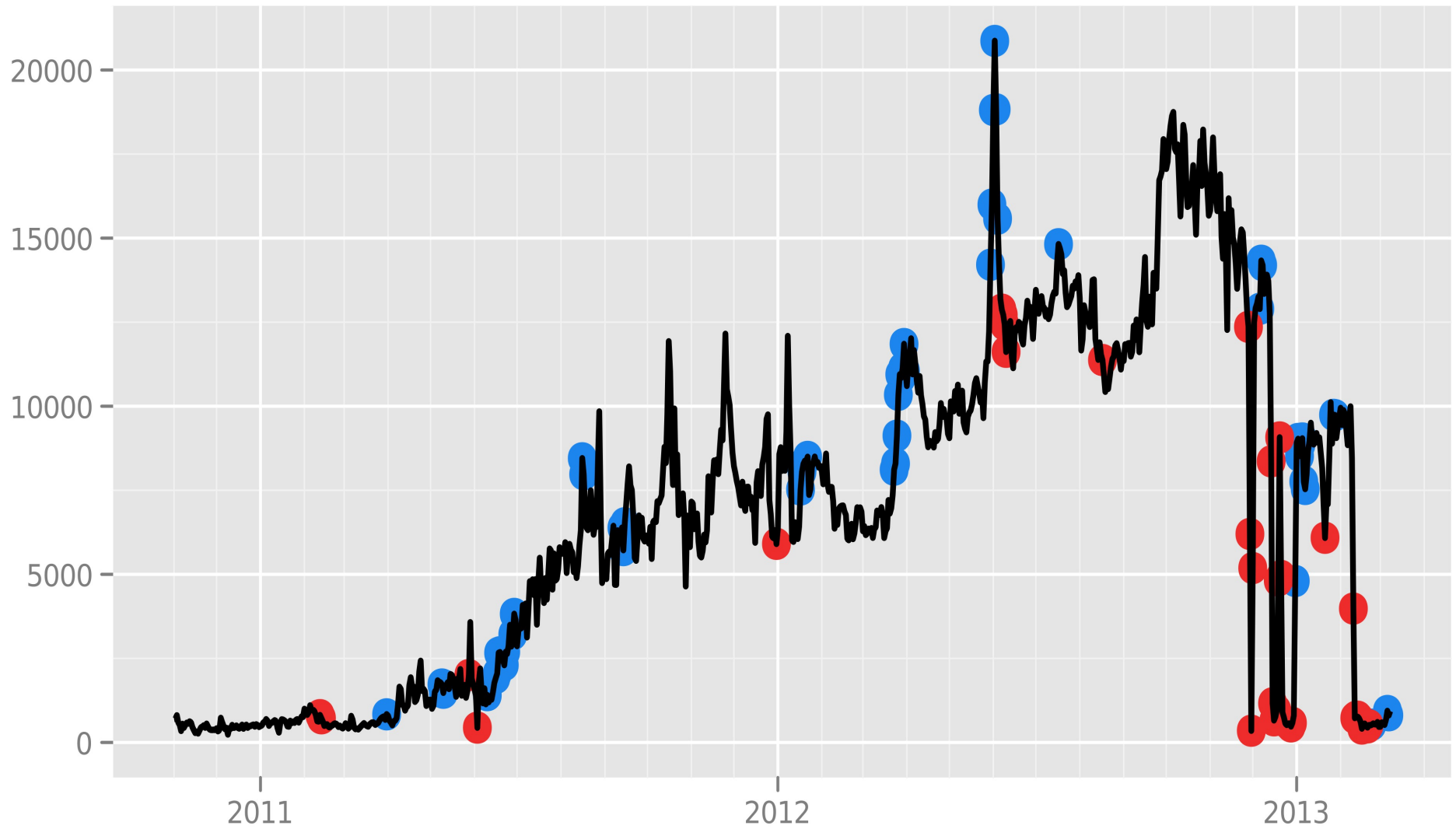
What we're up against

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

Burma vs Iran vs China

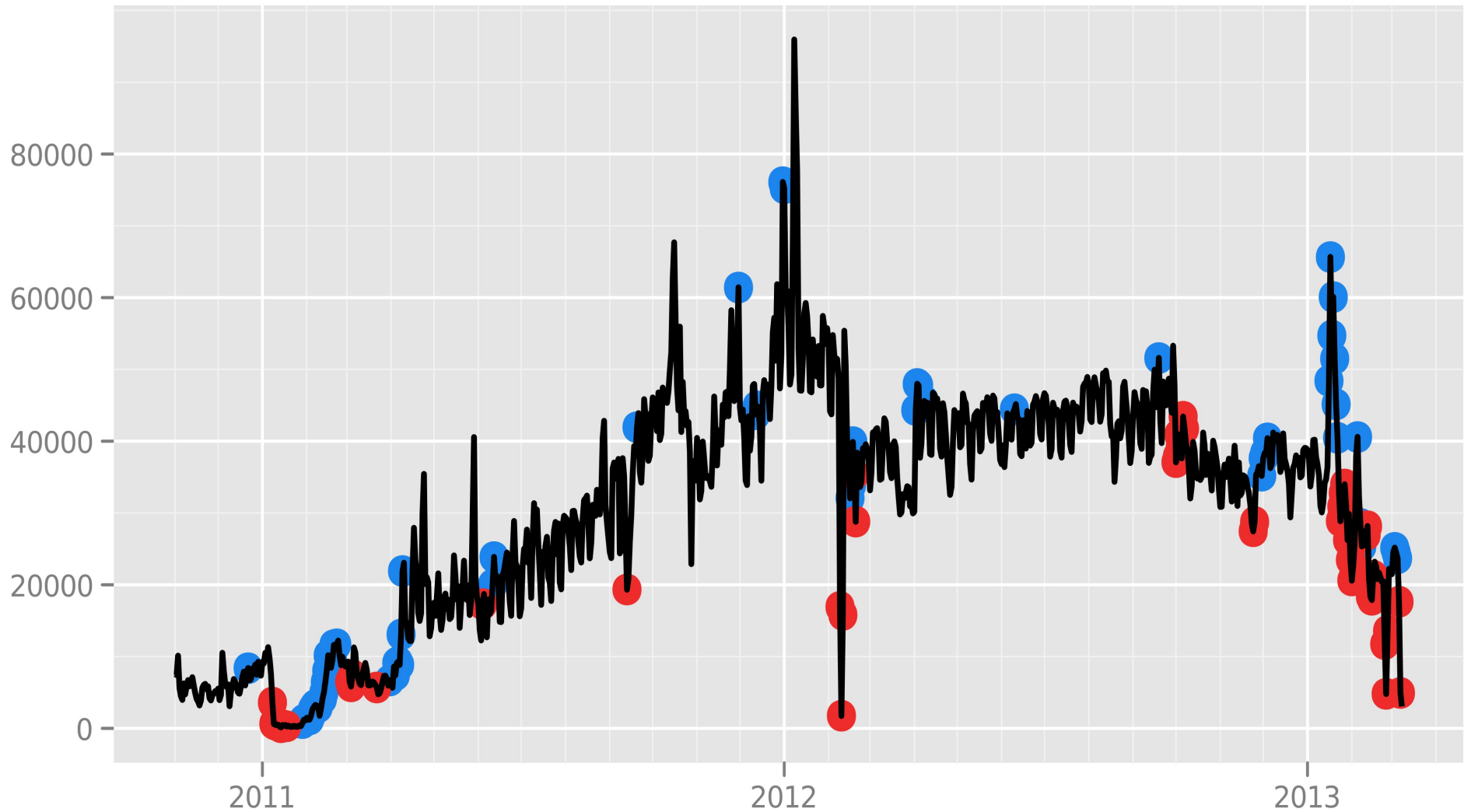
New filtering techniques spread by commercial (American) companies :(

Directly connecting users from the Syrian Arab Republic



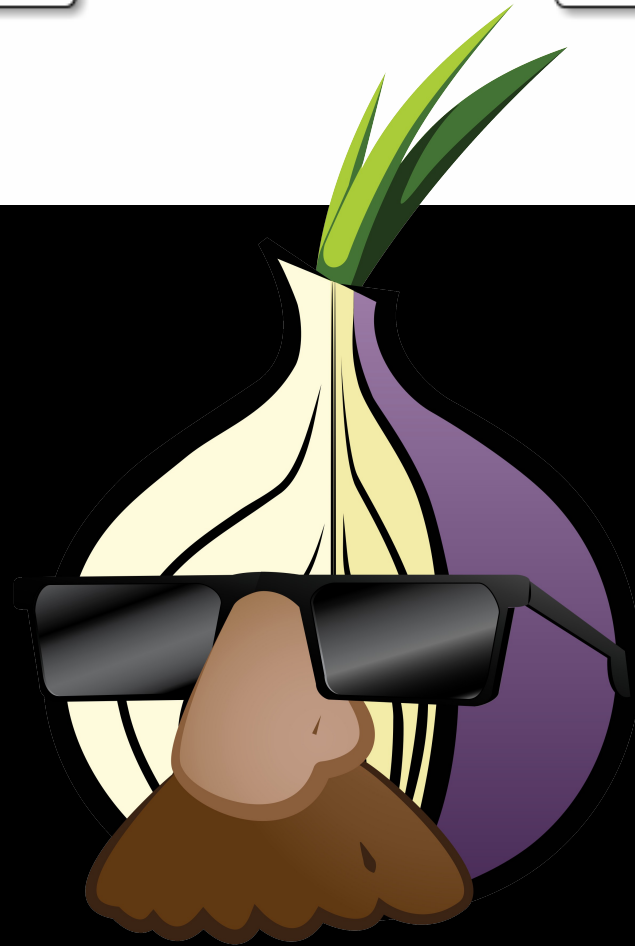
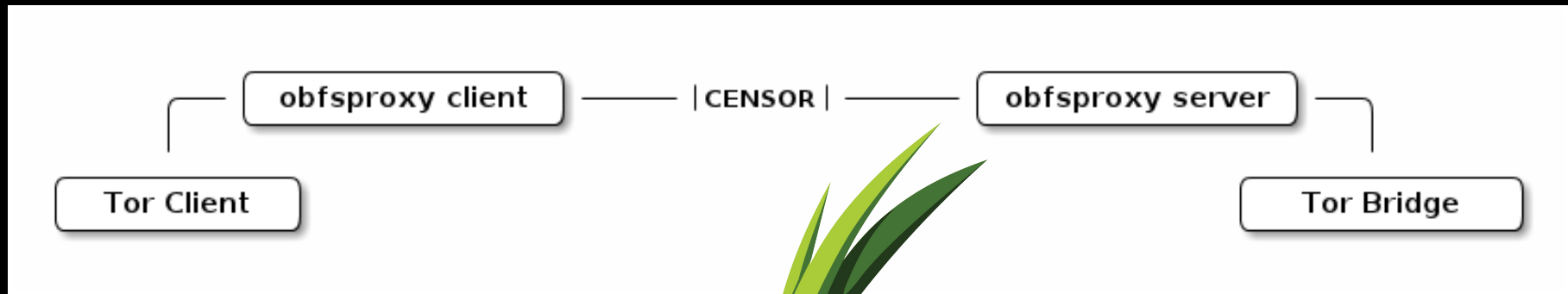
The Tor Project - <https://metrics.torproject.org/>

Directly connecting users from Iran



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

Modularity



Pluggable transports

- Flashproxy (Stanford), websocket
- FTEProxy (Portland St), http via regex
- Stegotorus (SRI/CMU), http
- Skypemorph (Waterloo), Skype video
- uProxy (Google), webrtc
- Lantern (BNS), social network based
- ScrambleSuit (Karlstad), obfs-based
- Telex (Michigan/Waterloo), traffic divert

Tor's safety comes from diversity

- #1: Diversity of relays. The more relays we have and the more diverse they are, 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. 50000 users in Iran means almost all of them are normal citizens.

Tor's anonymity comes from...

- The first 100,000 users (user diversity)
- The last 1,000,000 users (end-to-end correlation resistance)
- The first 1,000 relays (location diversity)

Only a piece of the puzzle

Assume the users aren't attacked by their hardware and software

No spyware installed, no cameras watching their screens, etc

Users can fetch a genuine copy of Tor?

I CAN HAZ
FREEDOM?





Stinks (U)



CT SIGDEV



JUN 2012

Derived From: _____
Dated: _____
On: _____



“Still the King of high secure,
low latency Internet Anonymity”

Contenders for the throne:

- None

NSA/GCHQ programs that affect Tor

- Quick Ant (QFD), Quantum Insert, Foxacid
- Quantum for cookie tests (good thing we moved away from Torbutton's “toggle”)
- Remember, they can do these things even more easily to non-Tor users
- At least they can't target specific Tor users (until they identify themselves)
- “Don't worry, we never attack Americans” (!)

Perception

- DoJ's aborted study finding 3% bad content on the Tor network
- How do you compare one Snowden leak to ten true reviews on Yelp?
- BBC's Silk Road articles telling people how to buy drugs safely

Trip report: Tor trainings for the Dutch and Belgian police

[View](#)[Edit](#)

Posted February 5th, 2013 by [arma](#) in [internet censorship](#), [law enforcement](#), [trip report](#)

In January I did Tor talks for the Dutch regional police, the Dutch national police, and the Belgian national police. Jake and I also did a brief inspirational talk at [Bits of Freedom](#), as well as the closing keynote for the Dutch [National Cyber Security Centre's](#) yearly [conference](#).

You may recall that one of my side hobbies lately has been teaching law enforcement about Tor — see my previous entries about [teaching the FBI about Tor](#) in 2012 and visiting the [Stuttgart](#) detectives in 2008 back when we were discussing data retention in Germany. Before this blog started I also did several Tor talks for the US DoJ, and even one for the Norwegian [Kripos](#).

Now is a good time to talk to the Dutch police, first because they're still smarting from the [DigiNotar disaster](#) in 2011, but second because of their 2012 ambitions to [legalize](#) breaking into foreign computers when they aren't sure what country they're in. (I say legalize because [they already did it!](#))

Below are some discussion points that made an impression on me.

- I started the trip with a [talk](#) to about 80 people from the Dutch regional police. Apparently each regional police group has basically one cybercrime person, and pretty much all of them came to learn about Tor. These are the people who advise their police groups about how to handle Tor cases, so they're exactly the ones who need to know about services like [ExoneraTor](#). (Afterwards, one of the national police thanked me heartily for teaching the regional police about Tor, since it makes *his* job easier.)
- One issue that came up repeatedly during the talks: what if a bad guy runs a Tor exit relay to provide plausible deniability when somebody shows up as his door? My first thought is that anybody who runs a Tor exit relay in order to attract *less* attention from

- [Add a New](#)
- [Manage E](#)
- [Admin Co](#)
- [Manage U](#)
- [Add an E](#)
- [Manage E](#)
- [Manage F](#)

Search

Upcoming

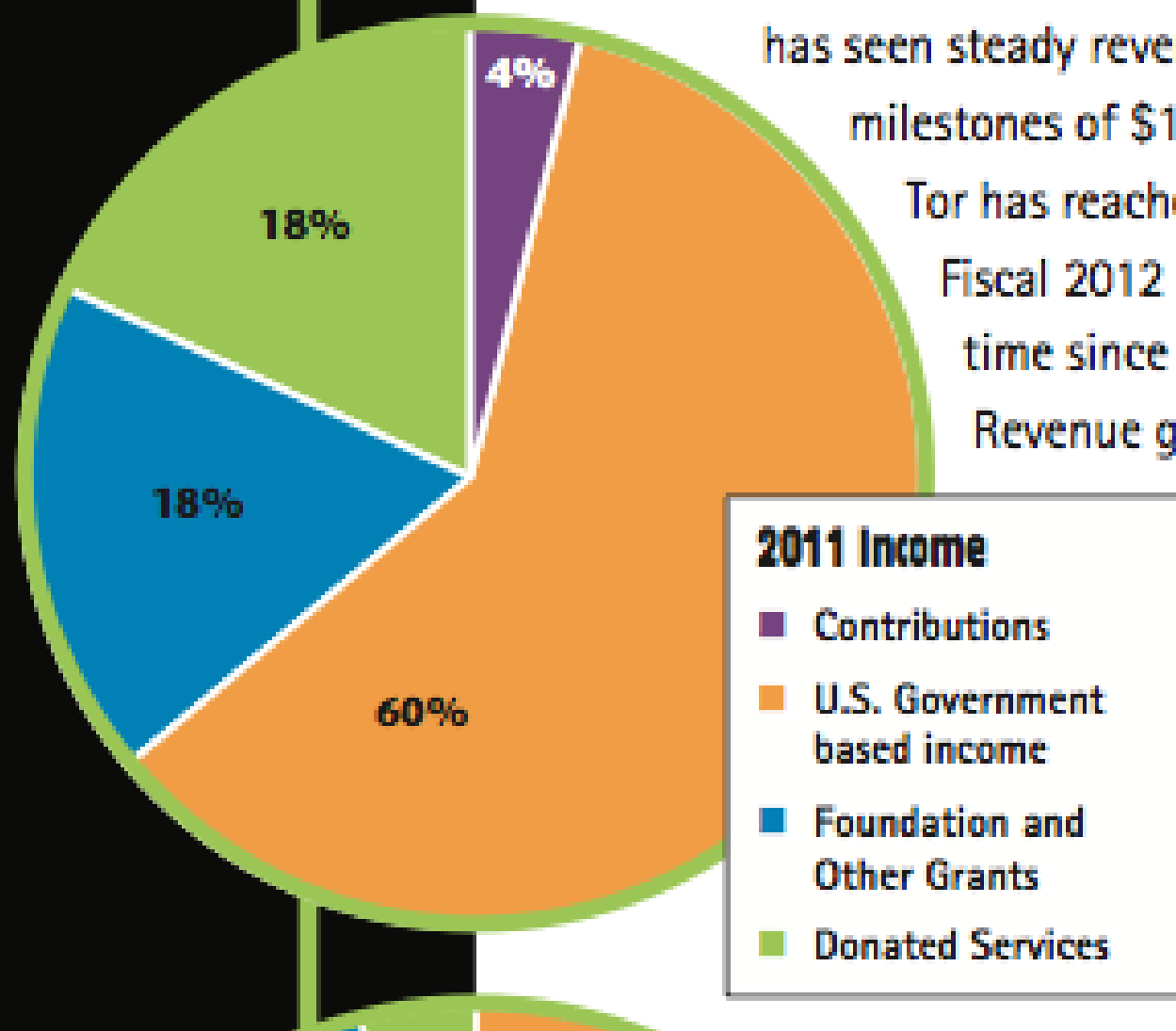
- [Lunar @ Conferen](#)
- [Roger @ Worksho Enhanci Blooming](#)
- [Tor at Pr Technolo](#)
- [Roger @](#)

Financial Review

Tor's fiscal 2012 marked another year of financial improvement. The organization has seen steady revenue growth since its inception. Significant milestones of \$1,253,241 in 2009, \$1,574,119 in 2010, and \$1,875,000 in 2011. Tor has reached new heights in 2012 with over \$2,000,000 in revenue. Fiscal 2012 results also provided a new financial record: The Tor Project Inc. has reached a new high in revenue. Revenue growth was driven by diversity in

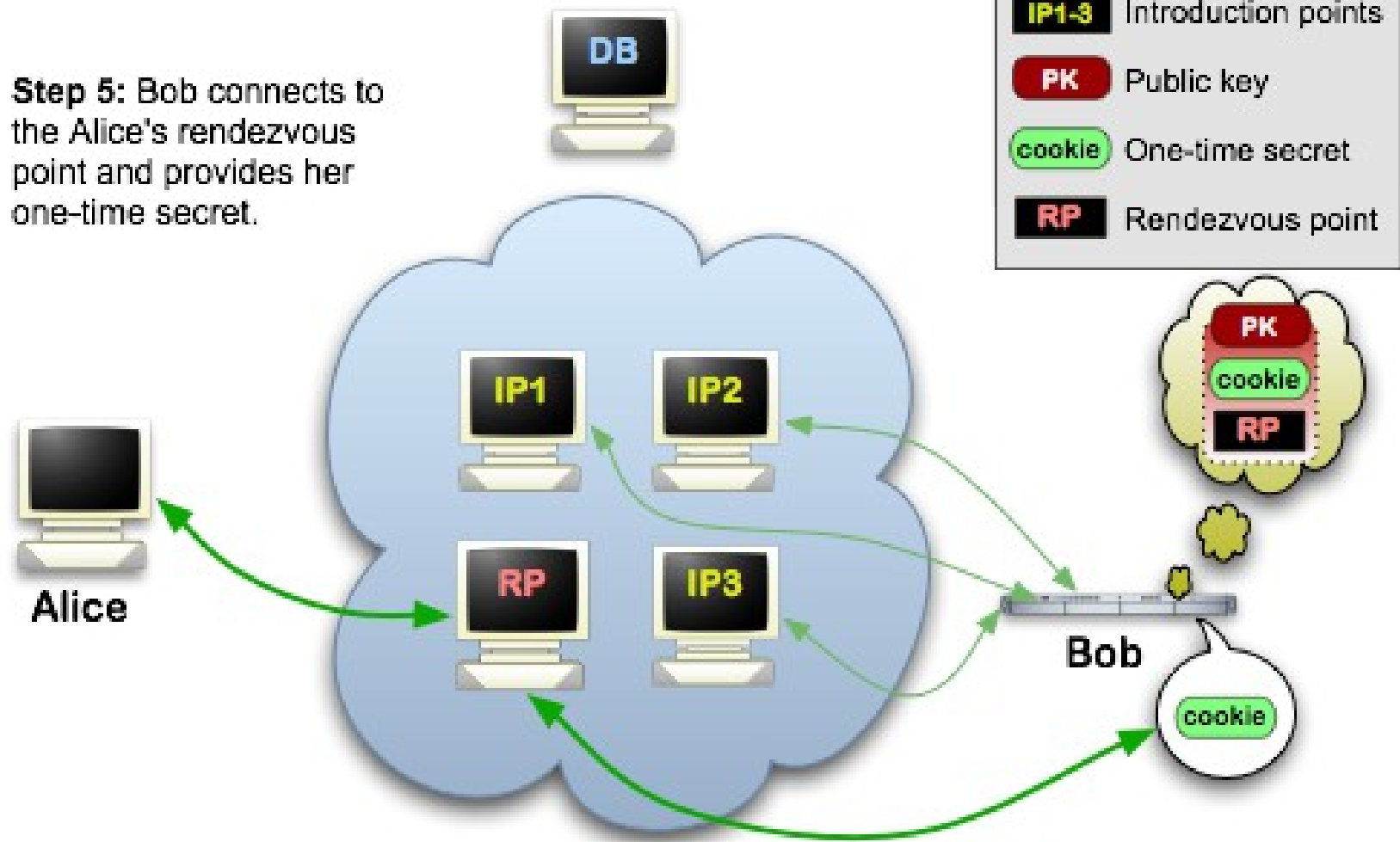
U.S. government federal funding from the State Department, the National Endowment for Democracy, the U.S. Agency for International Development, Google, the Swedish International Development Cooperative Agency, and private

Fiscal responsibility is important to maintain financial stability, and Tor is committed to being sufficient to maintain operations. Tor is proud to report that, since



Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



High-profile hidden services

The media has promoted a few hot topics:

- WikiLeaks (~2010)
- Farmer's market (pre-2013)
- Freedom Hosting (2013)
- Silk Road (2013)

There are many more (eg: many GlobaLeaks deployments, etc) which aren't well known by the media (yet).

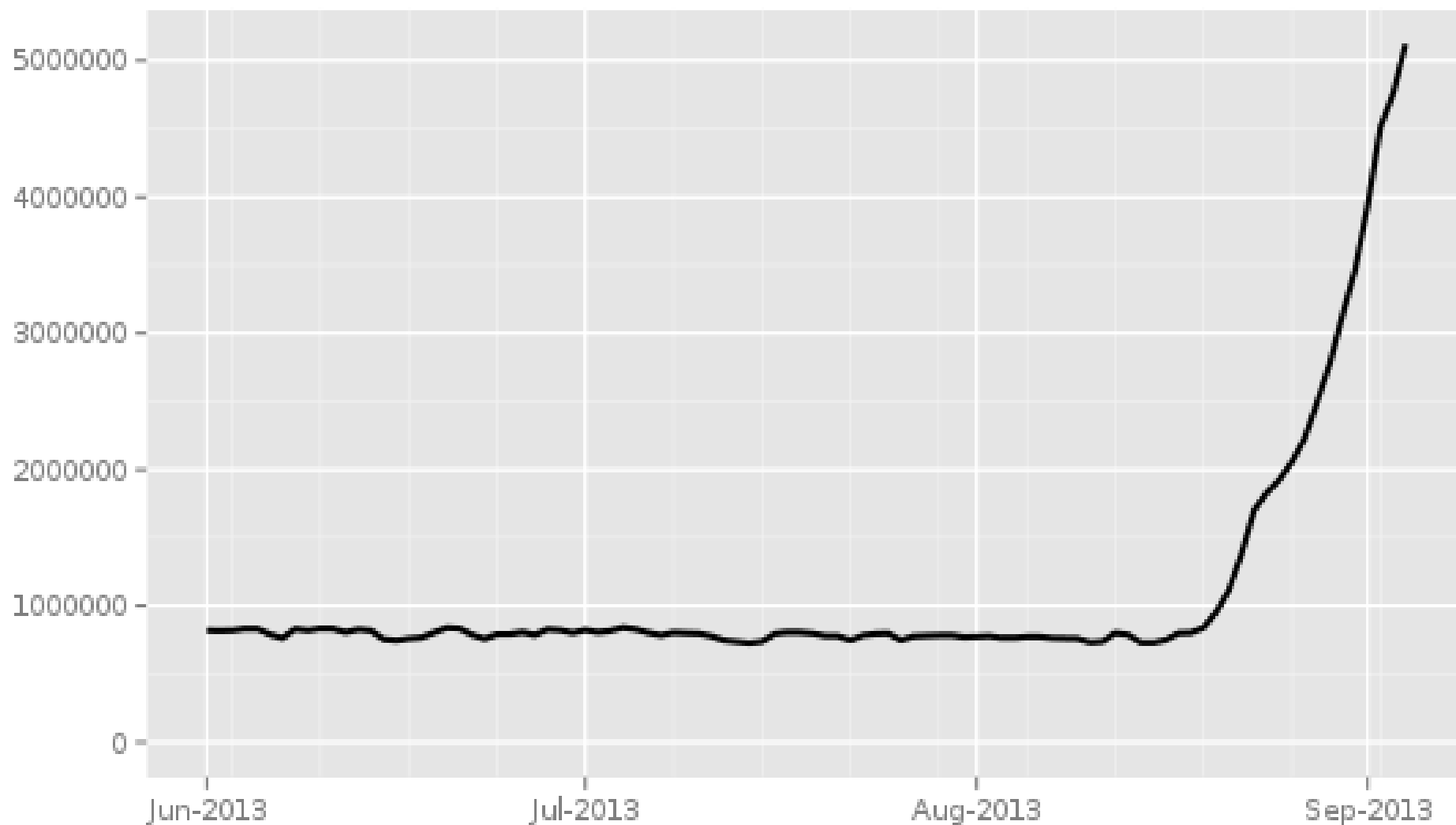
So what should Tor's role in the world be?

- Can't be solely technical (anymore, if it ever could have been)
- But technical is what we're best at (at least, historically)
- Remember how important diversity of users is

Three ways to destroy Tor

- 1) Legal / policy attacks
- 2) Make ISPs hate hosting exit relays
- 3) Make services hate Tor connections
 - Yelp, Wikipedia, Google, Skype, ...

Directly connecting users



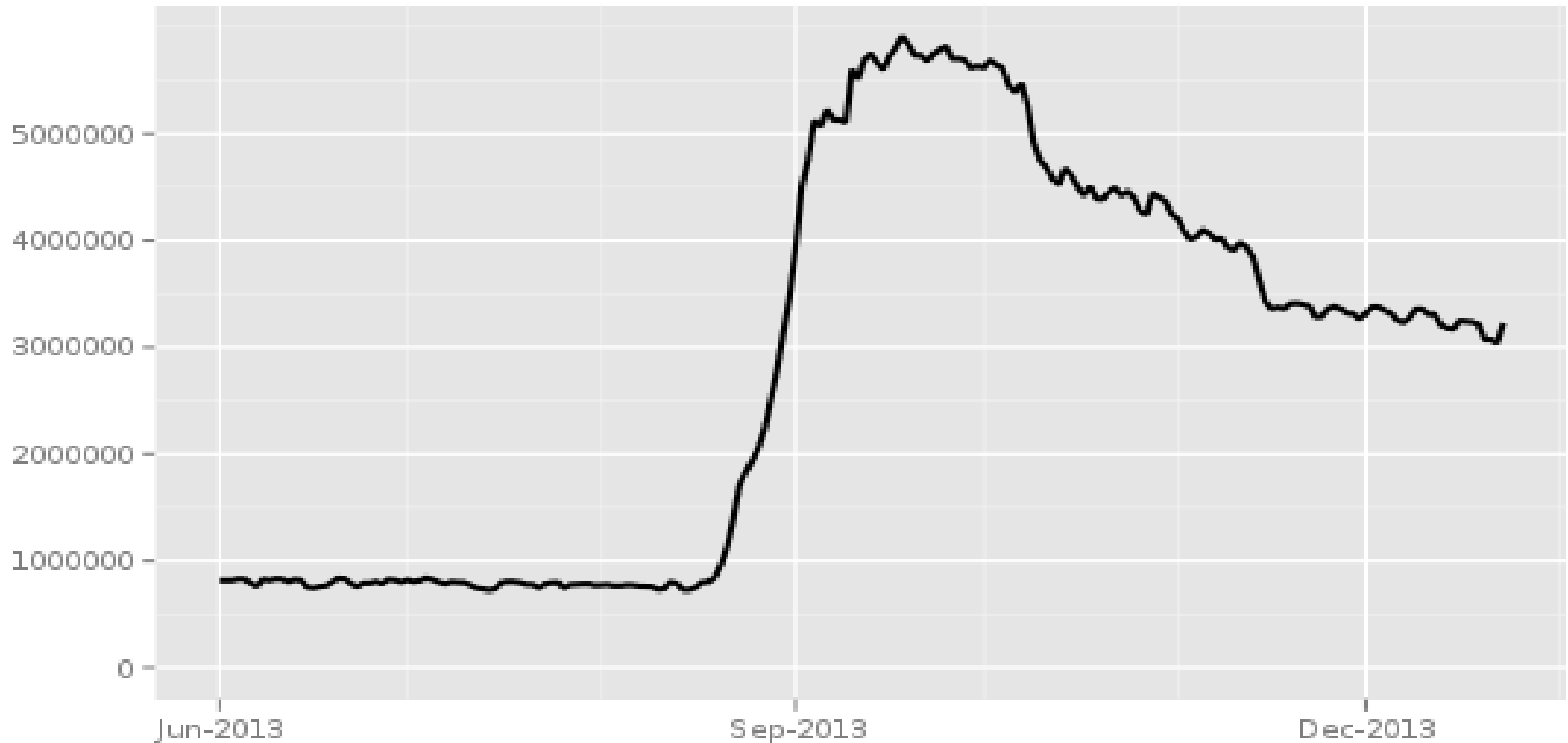
The Tor Project - <https://metrics.torproject.org/>

Botnet

- Some jerk in the Ukraine signed up 5 million bots as Tor clients (not relays)
- Our scalability work paid off!
- Good thing it wasn't malicious.
- Ultimately it didn't work: everybody noticed, and Microsoft has been cleaning up the bots

Number of daily Tor users

Directly connecting users



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

So what's next?

- “Tor: endorsed by Egyptian activists, Wikileaks, NSA, GCHQ, Chelsea Manning, Snowden, ...”
- Different communities like Tor for different reasons.

Tor Browser Bundle 3.x

- Deterministic Builds
- “Tor launcher” extension, no Vidalia
- Asks if you want bridges first
- Local homepage, so much faster startup
- Security slider (for e.g. JavaScript)
- Privacy fixes, e.g. font enumeration

- New Identity
- Cookie Protections
- Preferences...
- About Torbutton...
- Open Network Settings...

Congratulations!

This browser is configured to use Tor.

You are now free to browse the Internet anonymously.

[Test Tor Network Settings](#)

Search securely with Startpage.

What Next?

Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.

[Tips On Staying Anonymous »](#)

You Can Help!




There are many ways you can help make the Tor Network faster and stronger:


- [Run a Tor Relay Node »](#)
- [Volunteer Your Services »](#)
- [Make a Donation »](#)



The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. [Learn more about The Tor Project »](#)

Orbot

🔥 Connected to the Tor network

 Orbot   

powered by The Tor Project 

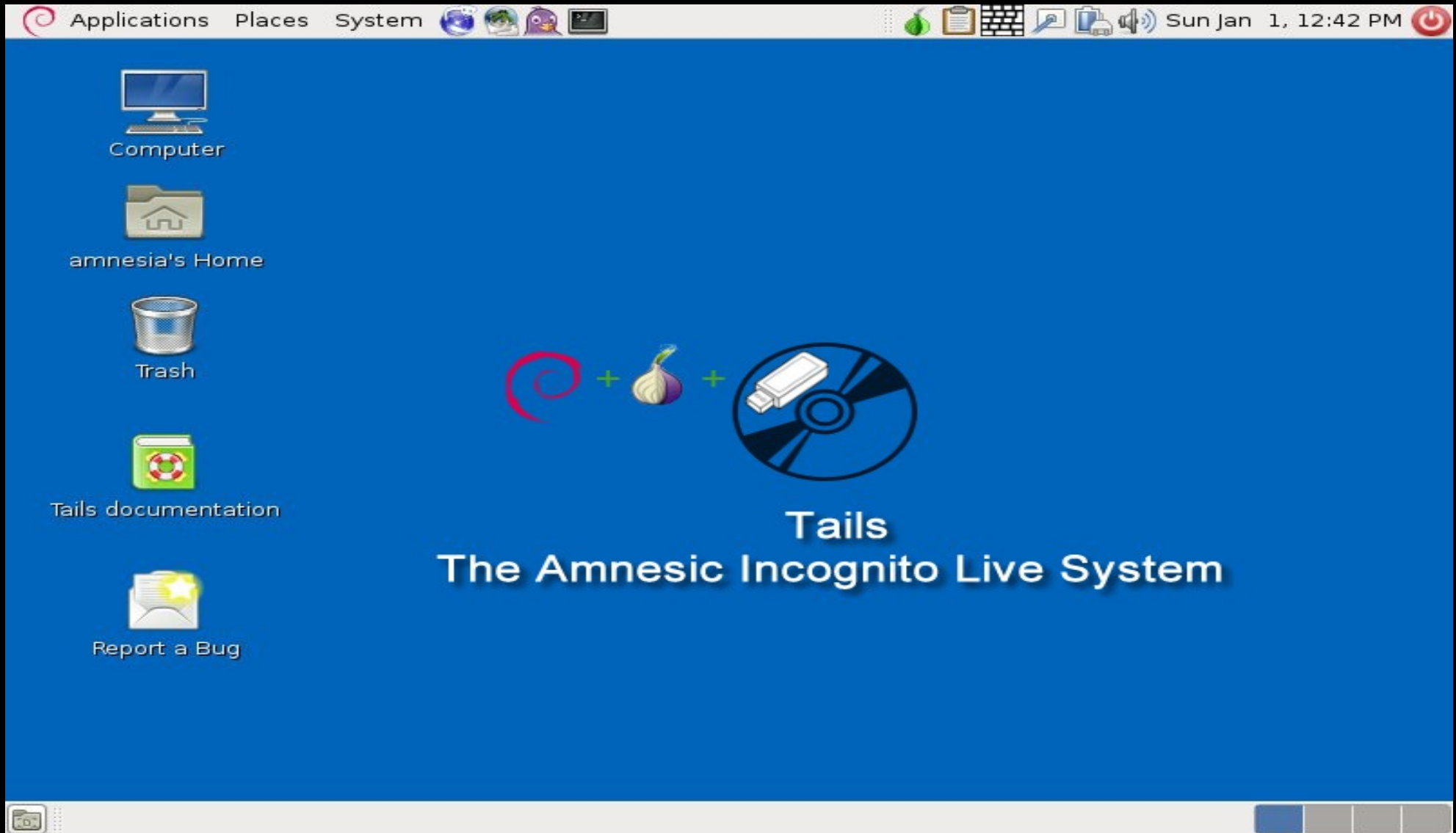



Connected to the Tor network

Download 98.2kbps / 94.1KB	<input type="button" value="Log"/>	Upload 4.5kbps / 18.4KB
--------------------------------------	------------------------------------	-----------------------------------

← 🏠 ☰

Tails LiveCD



“Core” Tor tasks

- Core Tor (specs, design, hidden services)
- Tor Browser Bundle, deterministic builds
- Metrics and measurements
- Bridges and pluggable transports
- Helping the research community
- Outreach and education