Tor: a quick overview

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

What is Tor?

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

Community of researchers, developers, users, and relay operators

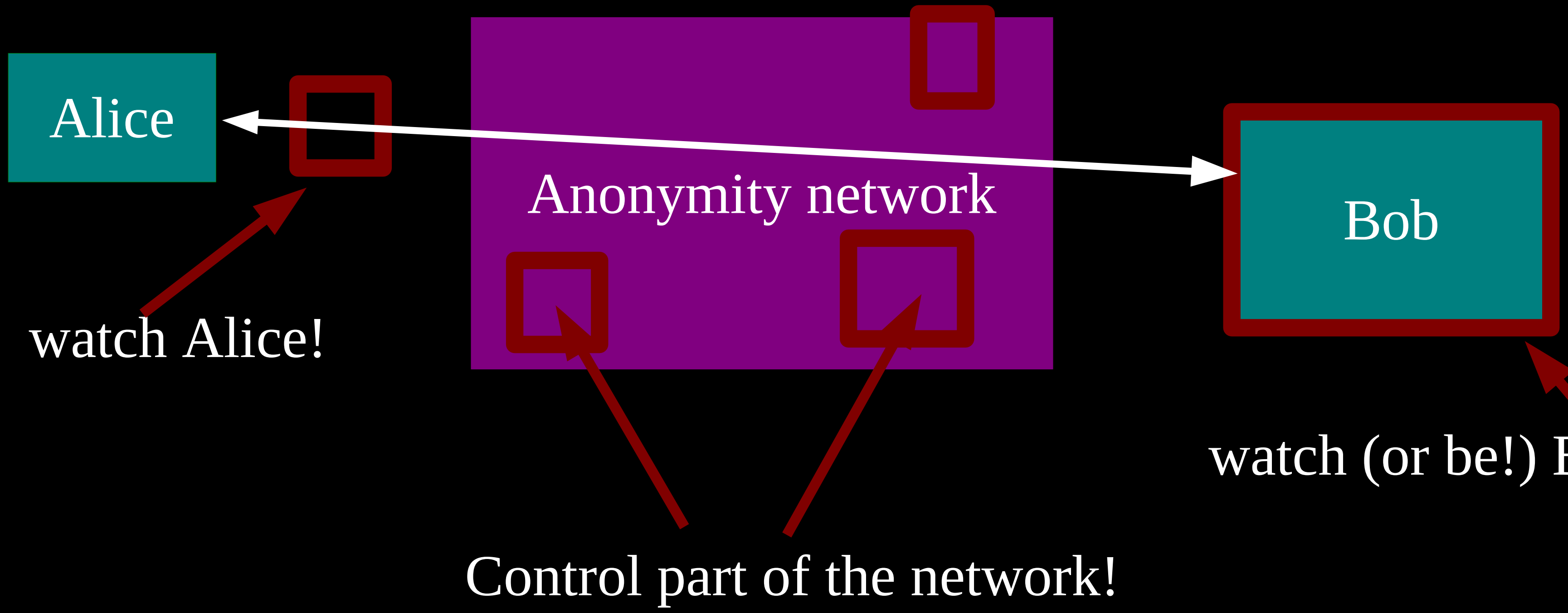
Funding from US DoD, Electronic Frontier Foundation, Voice of America, Google, NLnet, Human Rights Watch, NSF, US State Dept, SIDA, Knight Foundation, ...

The Tor Project, Inc.

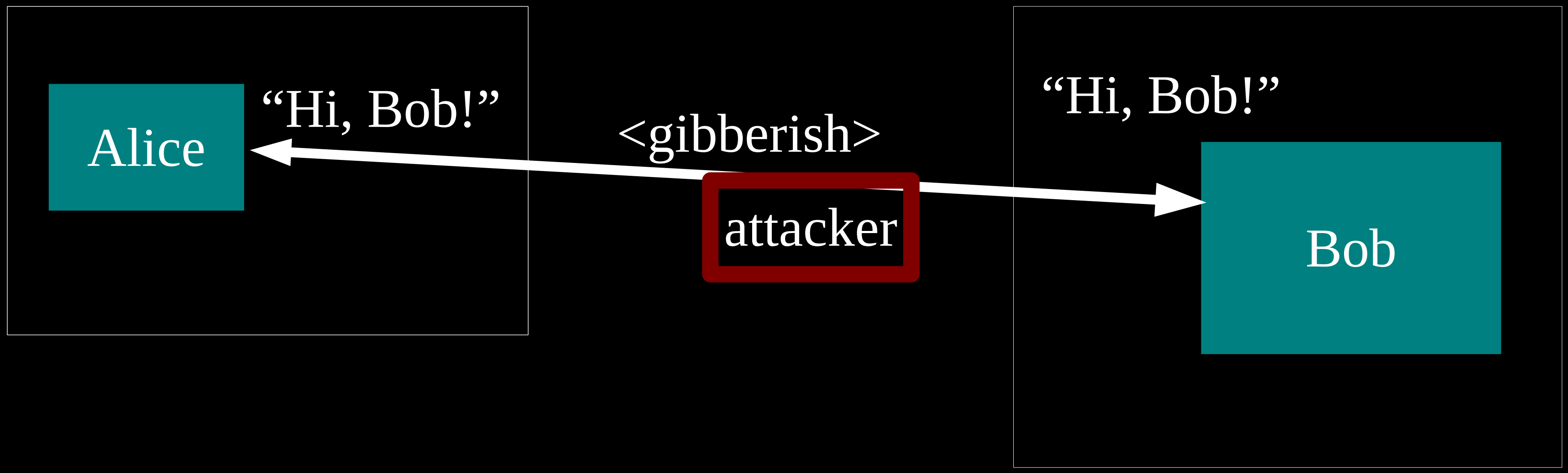
501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy

Estimated 600,000?
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!”

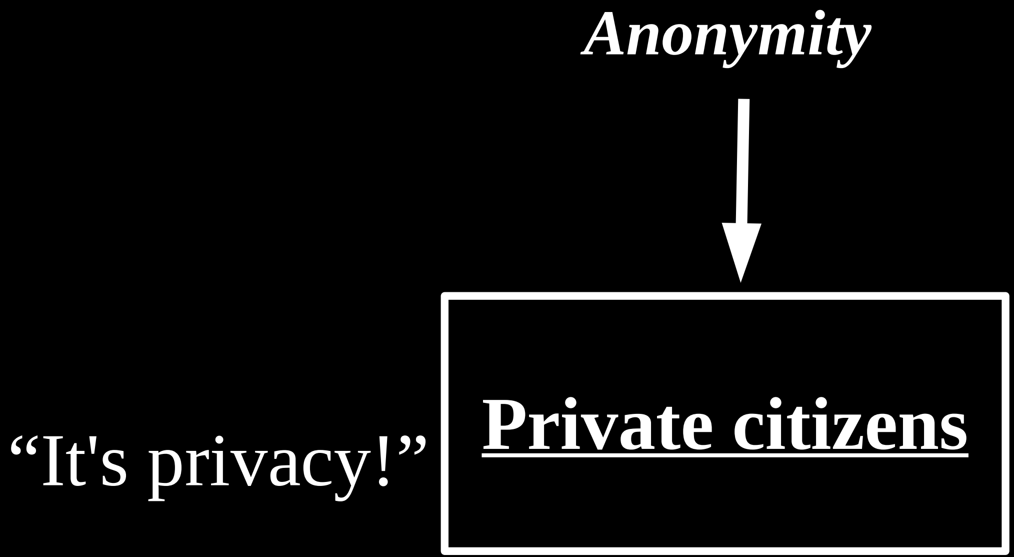
“Promise you won't remember!”

“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.

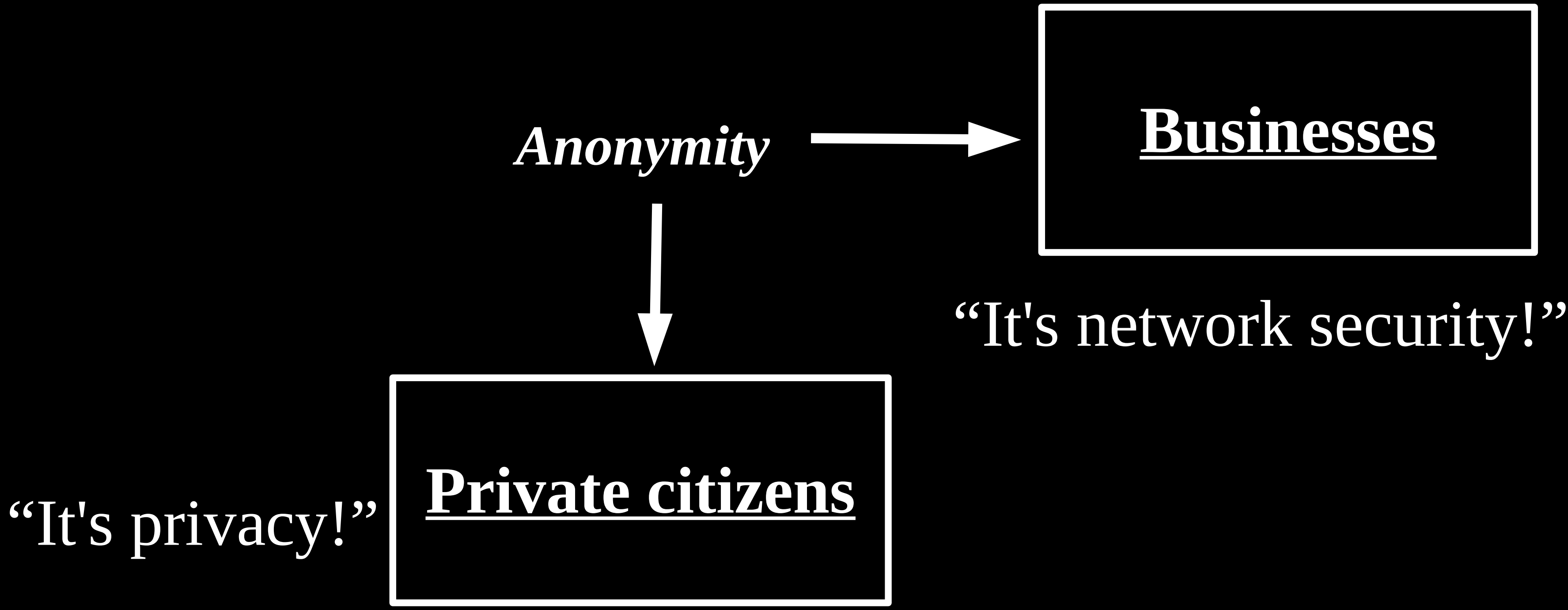


Anonymity

“It's privacy!”

Private citizens

Anonymity serves different interests for different user groups.



Anonymity

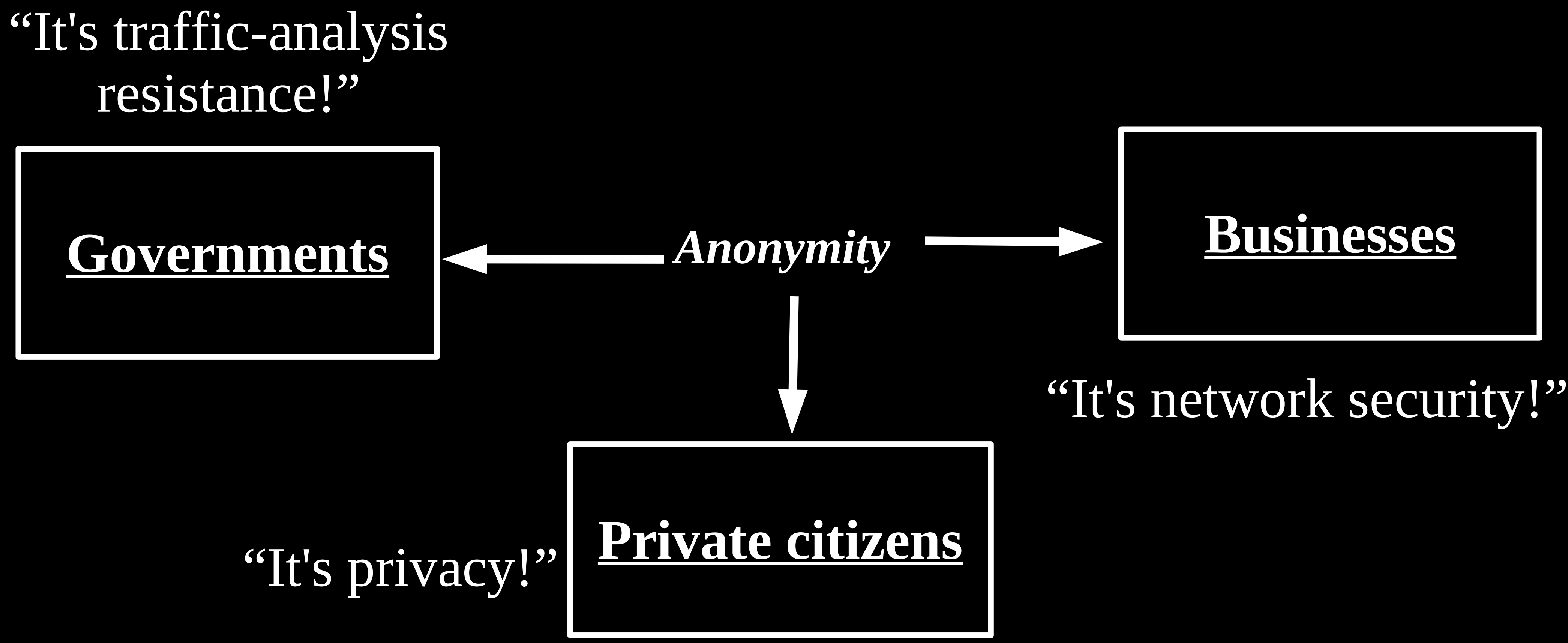
Businesses

“It's network security!”

Private citizens

“It's privacy!”

Anonymity serves different interests for different user groups.



Anonymity

Governments

“It's traffic-analysis resistance!”

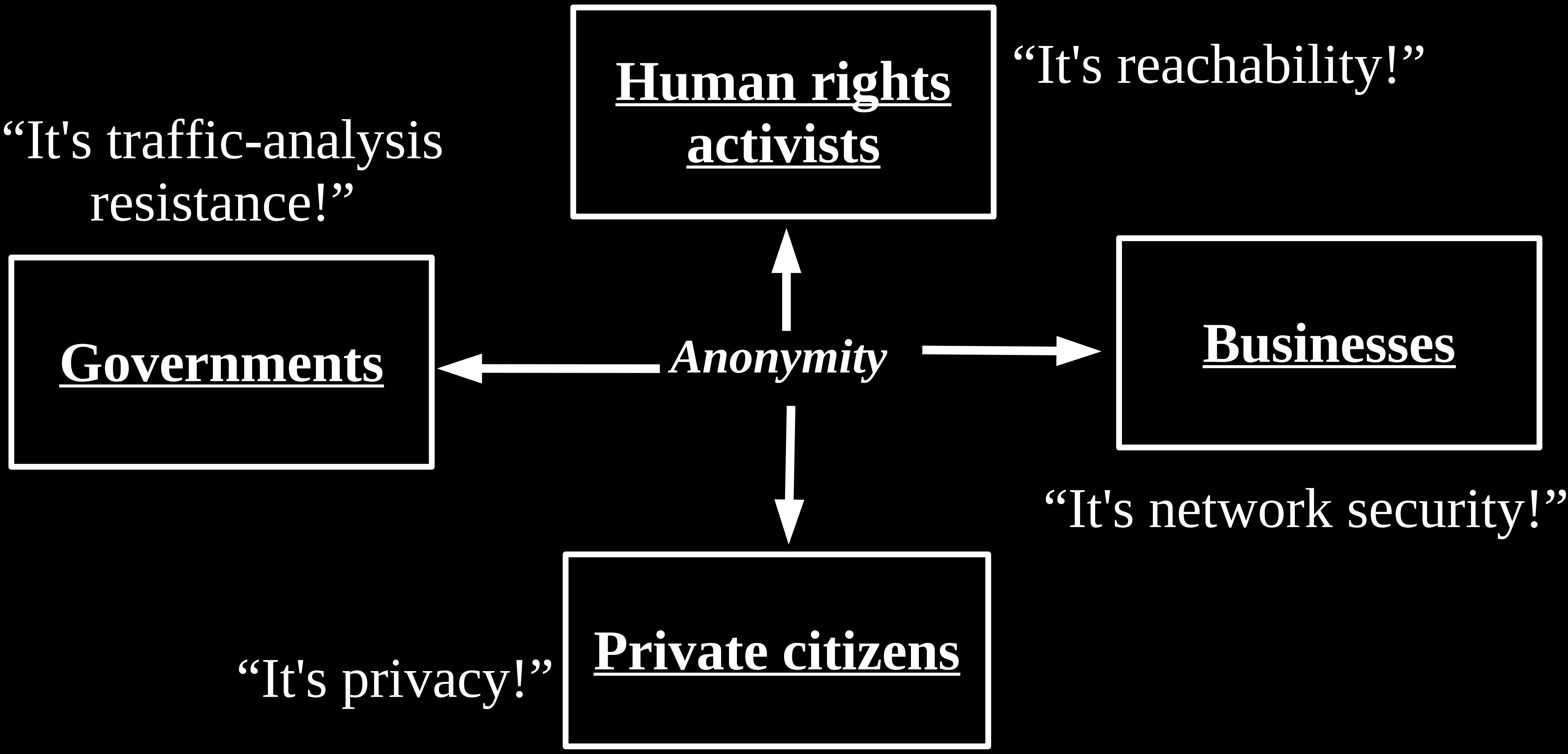
Businesses

“It's network security!”

Private citizens

“It's privacy!”

Anonymity serves different interests for different user groups.



Human rights activists

“It's reachability!”

“It's traffic-analysis resistance!”

Governments

Anonymity

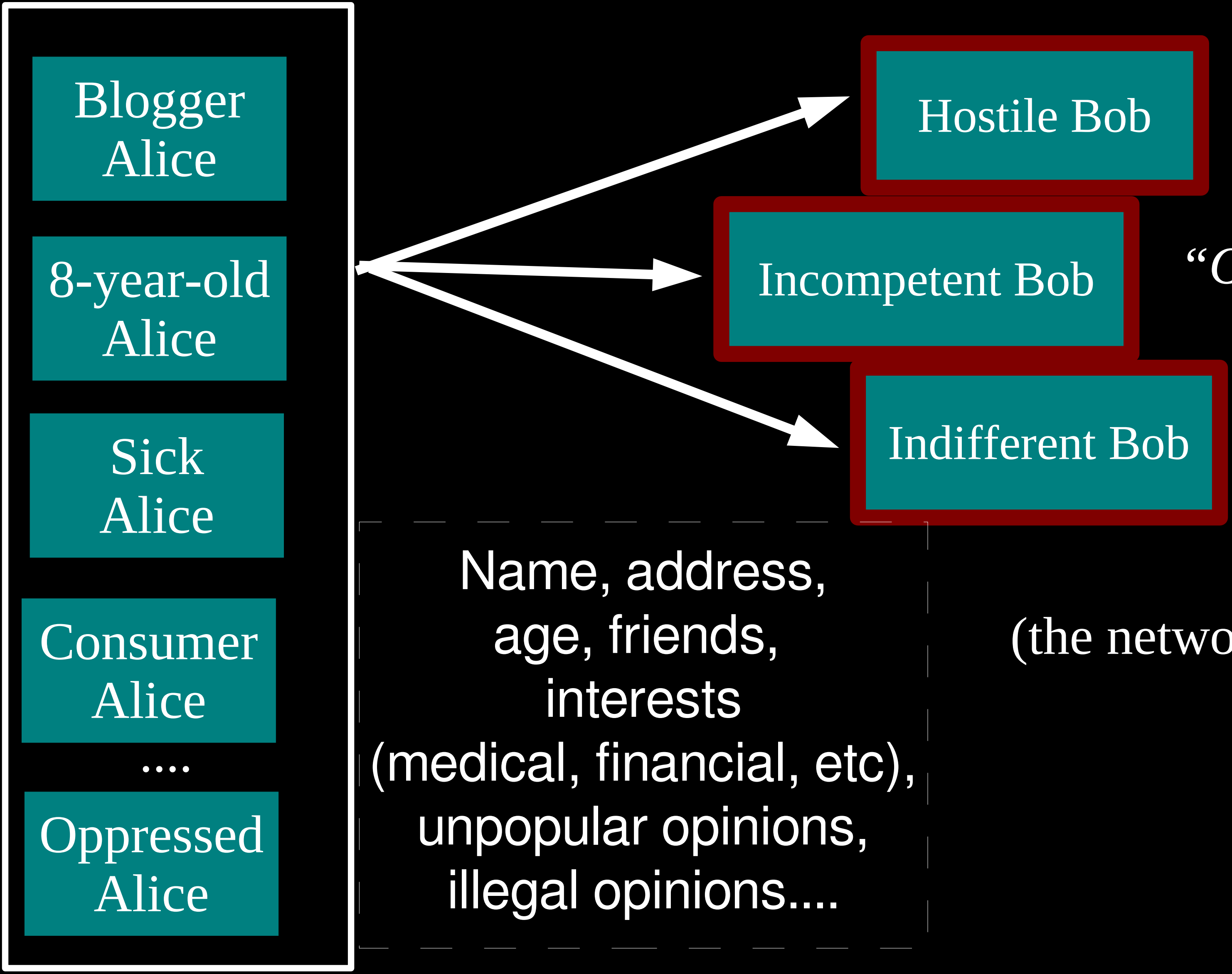
Businesses

“It's network security!”

“It's privacy!”

Private citizens

Regular citizens don't want to be watched and tracked.



Blogger Alice

8-year-old Alice

Sick Alice

Consumer Alice

....

Oppressed Alice

Hostile Bob

“I sell the logs.”

Incompetent Bob

“Oops, I lost the logs.”
The AOL fiasco

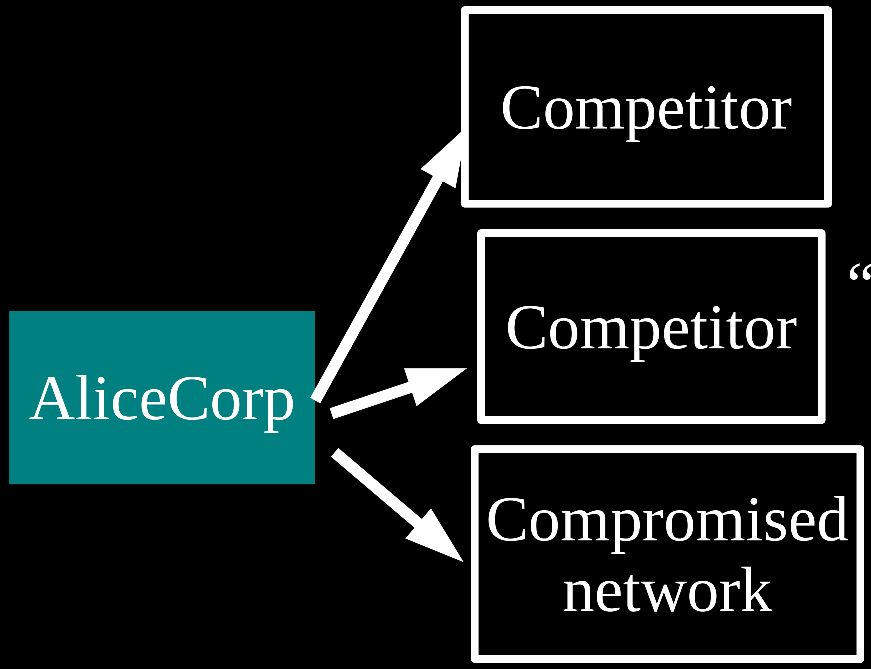
Indifferent Bob

“Hey, they aren't ***my*** *secrets.”*

Name, address, age, friends, interests (medical, financial, etc), unpopular opinions, illegal opinions....

(the network can track too)

Businesses need to keep trade secrets.



AliceCorp

Competitor

Competitor

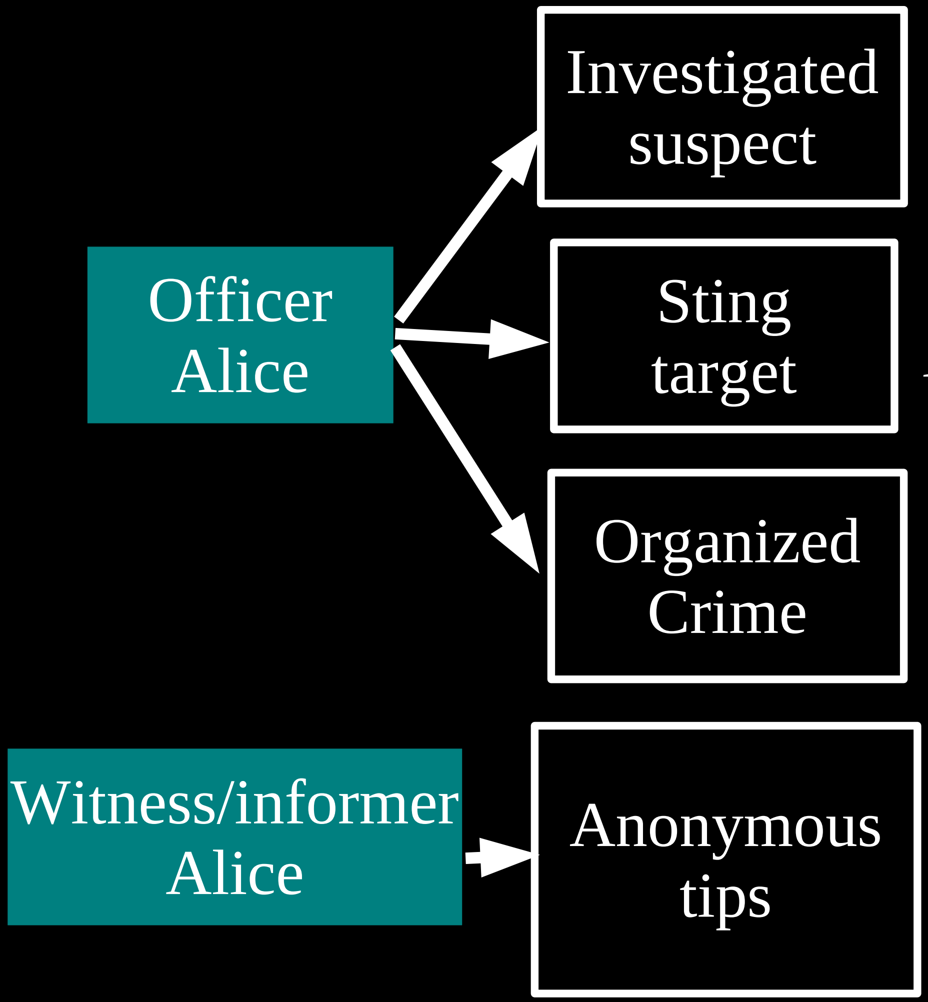
Compromised network

“Oh, your employees are reading our patents/jobs page/product sheets?”

“Hey, it's Alice! Give her the 'Alice' version!”

“Wanna buy a list of Alice's suppliers? What about her customers? What about her engineering department's favorite search terms?”

Law enforcement needs anonymity to get the job done.



Officer Alice

Investigated suspect

"Why is alice.localpolice.gov reading my website?"

Sting target

"Why no, alice.localpolice.gov!
I would never sell counterfeits on ebay!"

Organized Crime

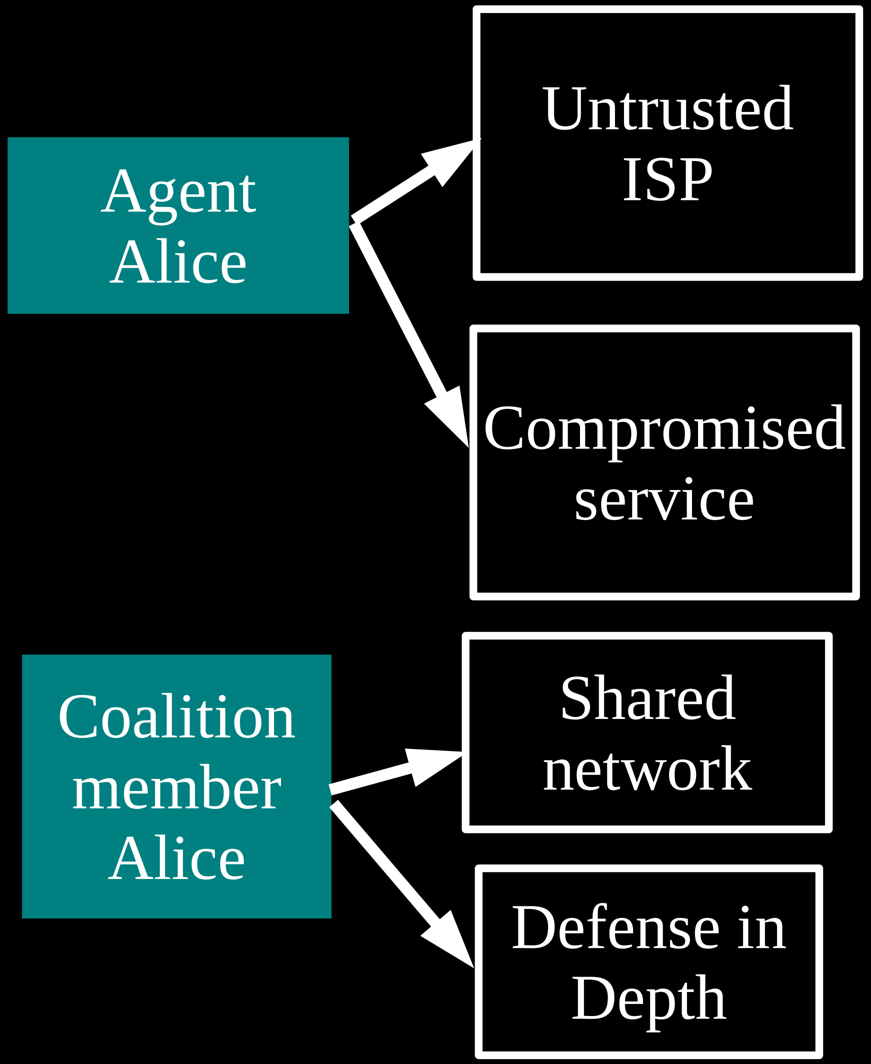
"Is my family safe if I go after these guys?"

Witness/informer Alice

Anonymous tips

"Are they really going to ensure my anonymity?"

Governments need anonymity for their security



“What will you bid for a list of Baghdad IP addresses that get email from .gov?”

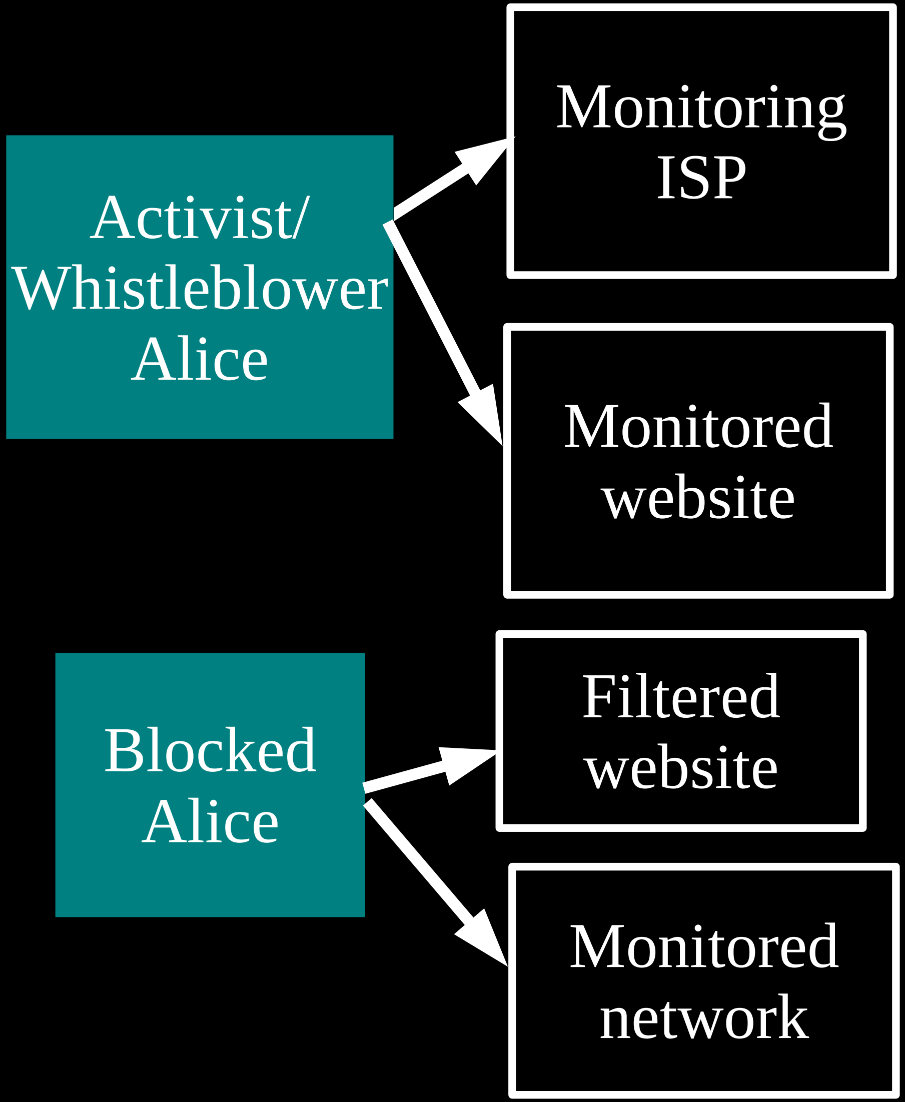
“Somebody in that hotel room just checked his Navy.mil mail!”

“What **does** *FBI Google for?”*

“Do I really want to reveal my internal network topology?”

“What about insiders?”

Journalists and activists need Tor for their personal safety



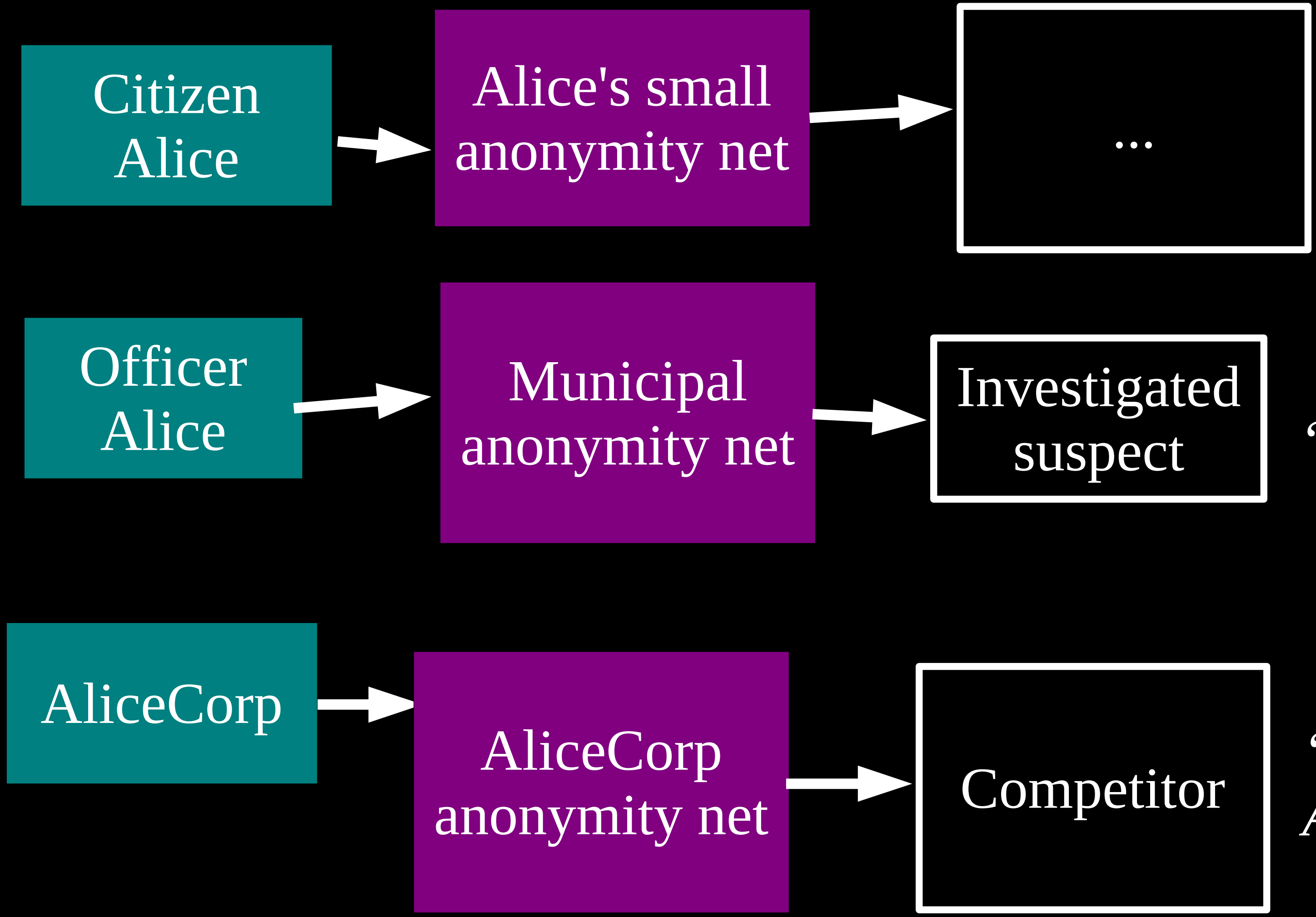
"Did you just post to that website?"

"Where are the bloggers connecting from?"
"I run livejournal and track my users"
"Of course I tell China about my users"

"What does the Global Voices website say today?"
"I want to tell people what's going on in my country"

"I think they're watching. I'm not even going to try."

You can't get anonymity on your own: private solutions are ineffective...

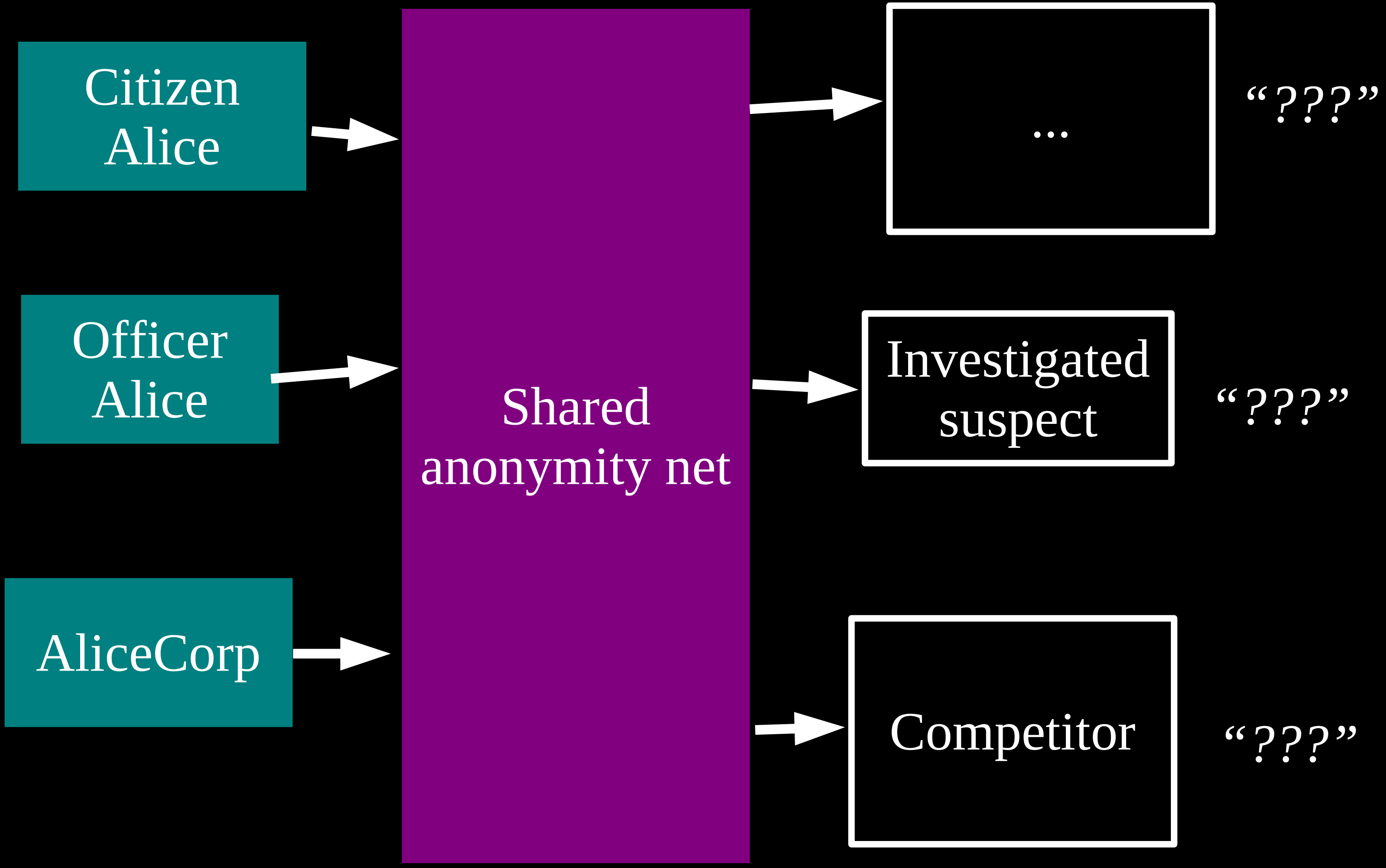


“One of the 25 users on AliceNet.”

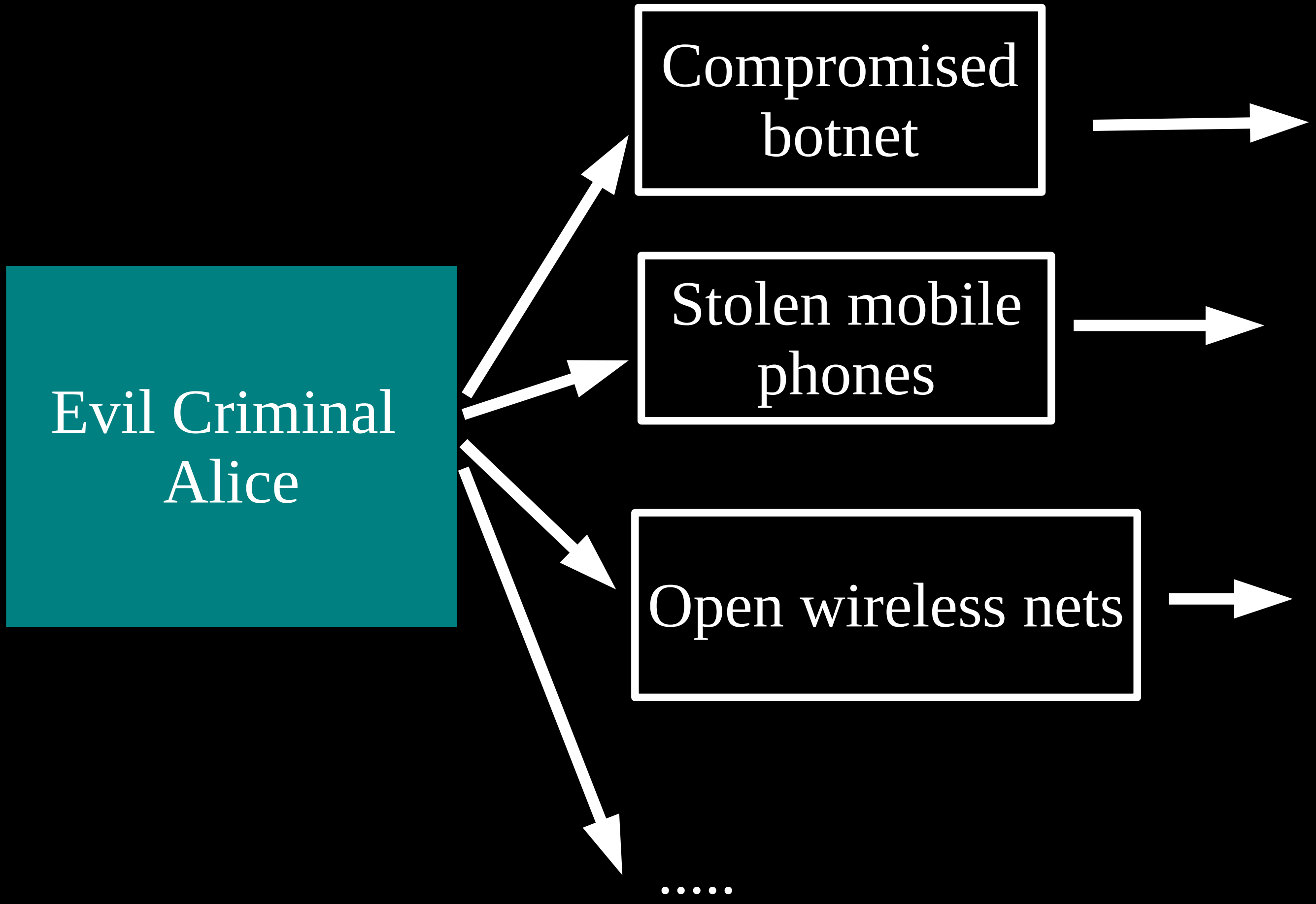
“Looks like a cop.”

“It's ***somebody*** *at AliceCorp!”*

… so, anonymity loves company!



Yes, bad people need anonymity too. But they are *already* doing well.



Evil Criminal Alice

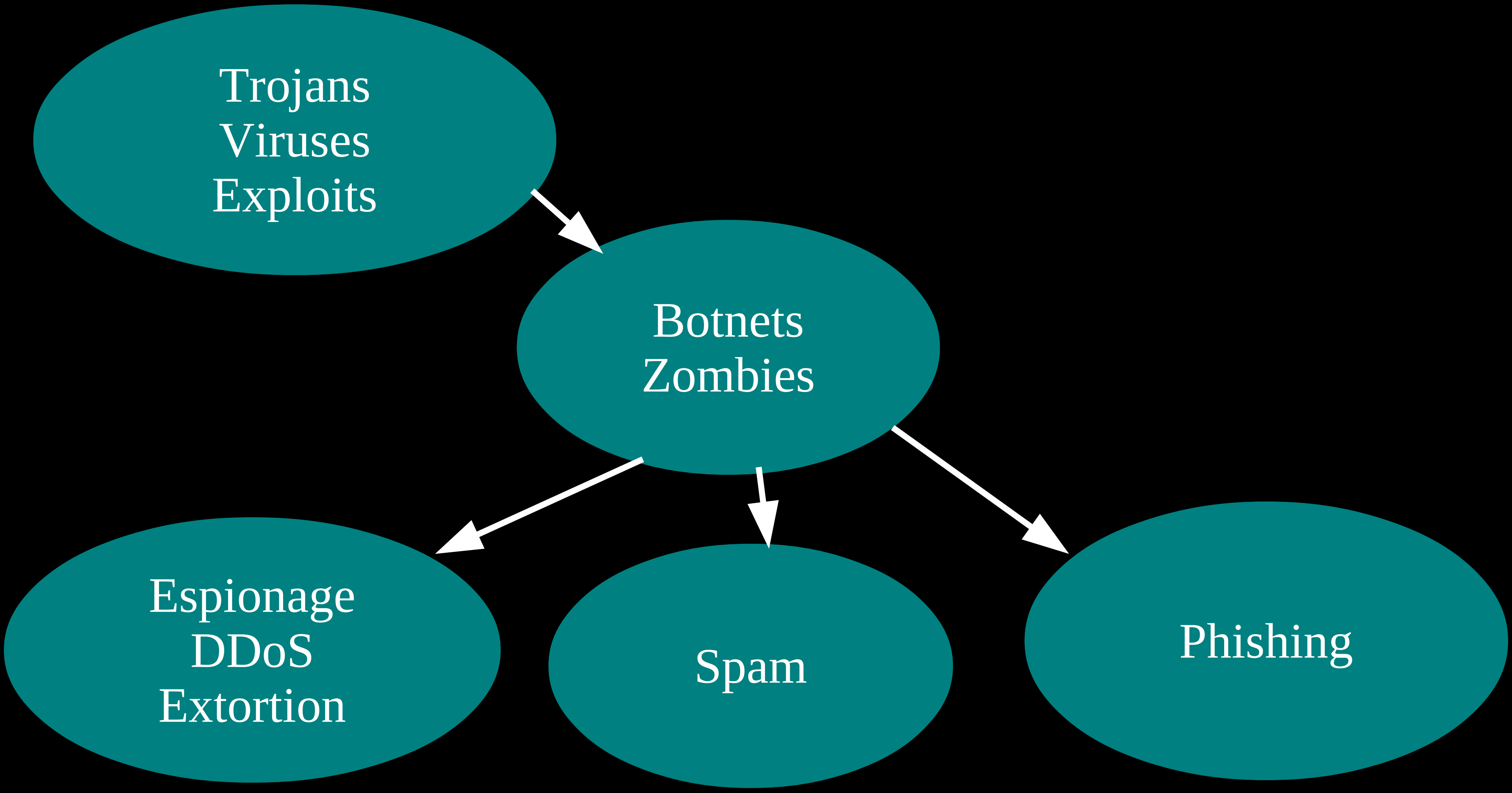
Compromised botnet

Stolen mobile phones

Open wireless nets

.....

Current situation: Bad people on the Internet are doing fine



Trojans
Viruses
Exploits

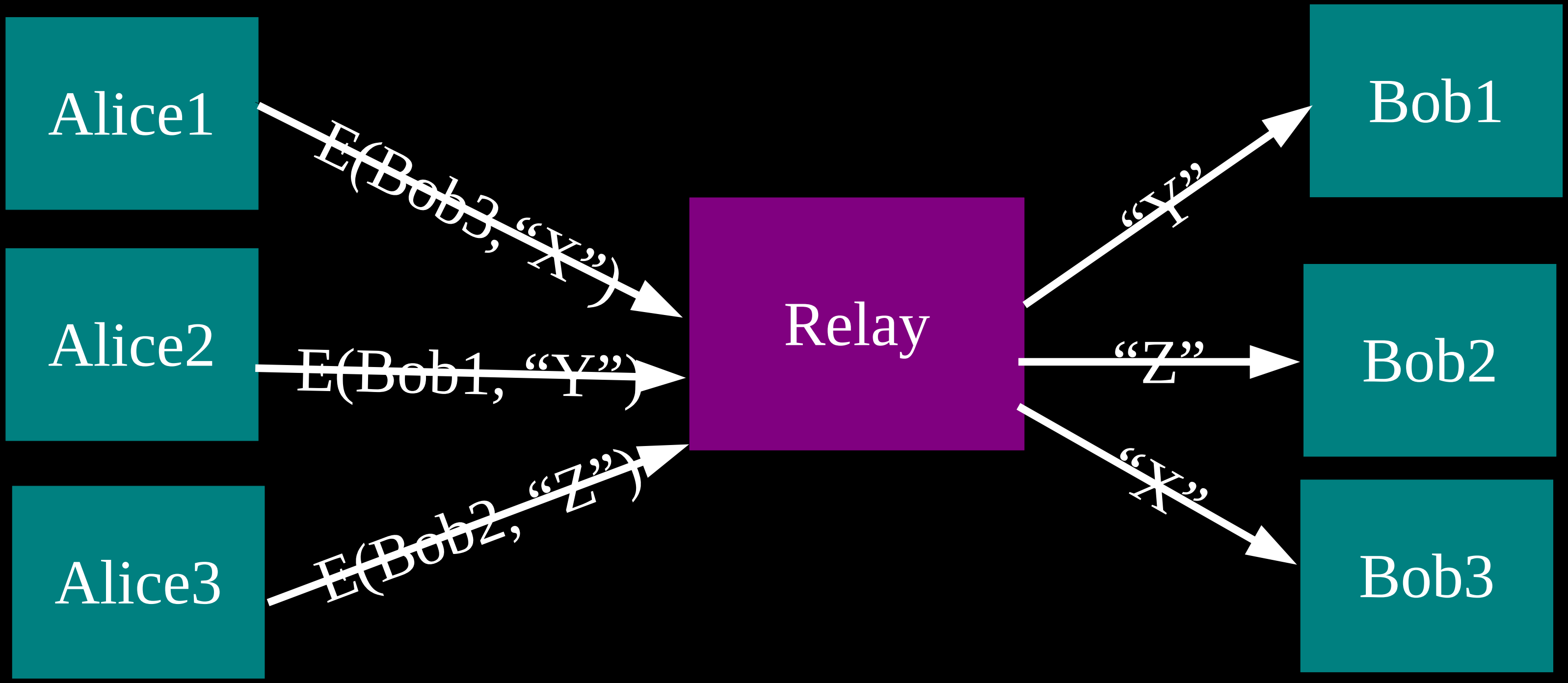
Botnets
Zombies

Espionage
DDoS
Extortion

Spam

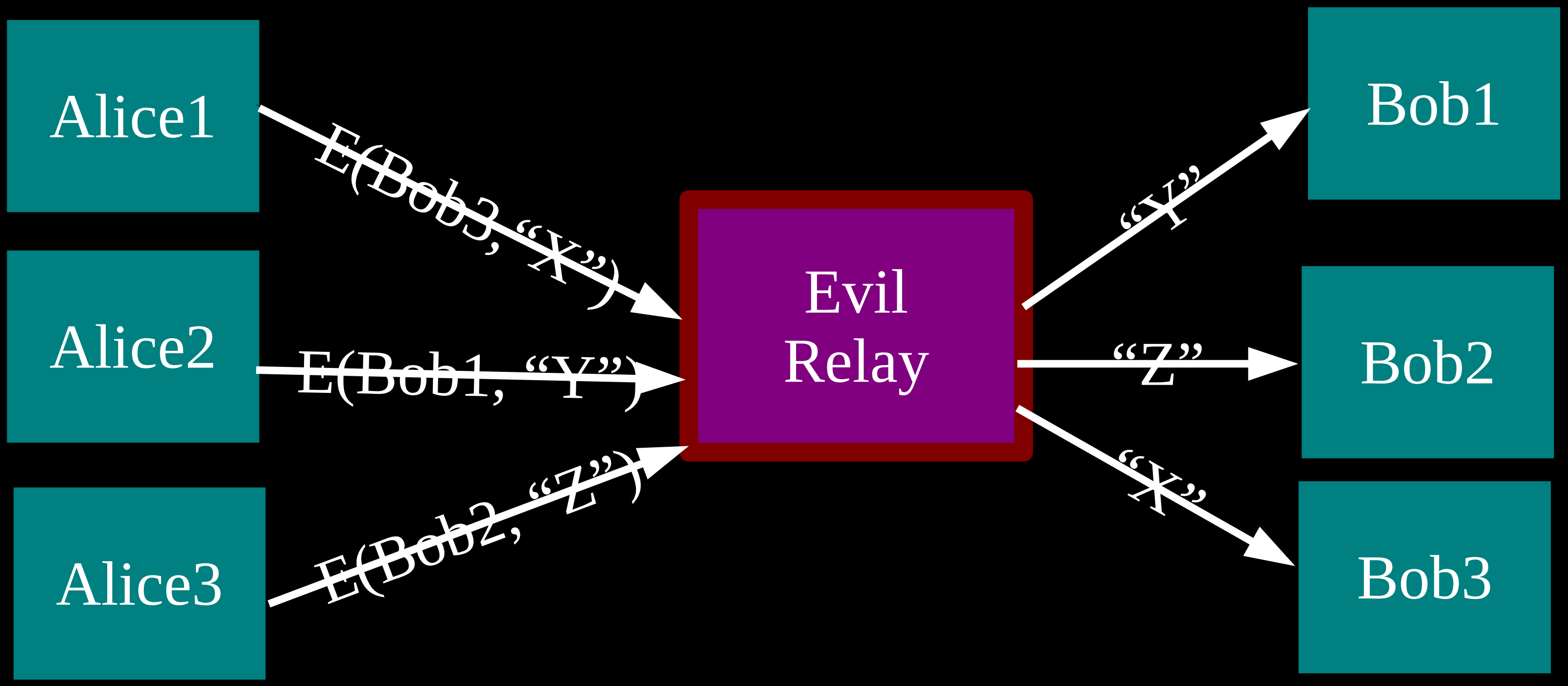
Phishing

The simplest designs use a single relay to hide connections.

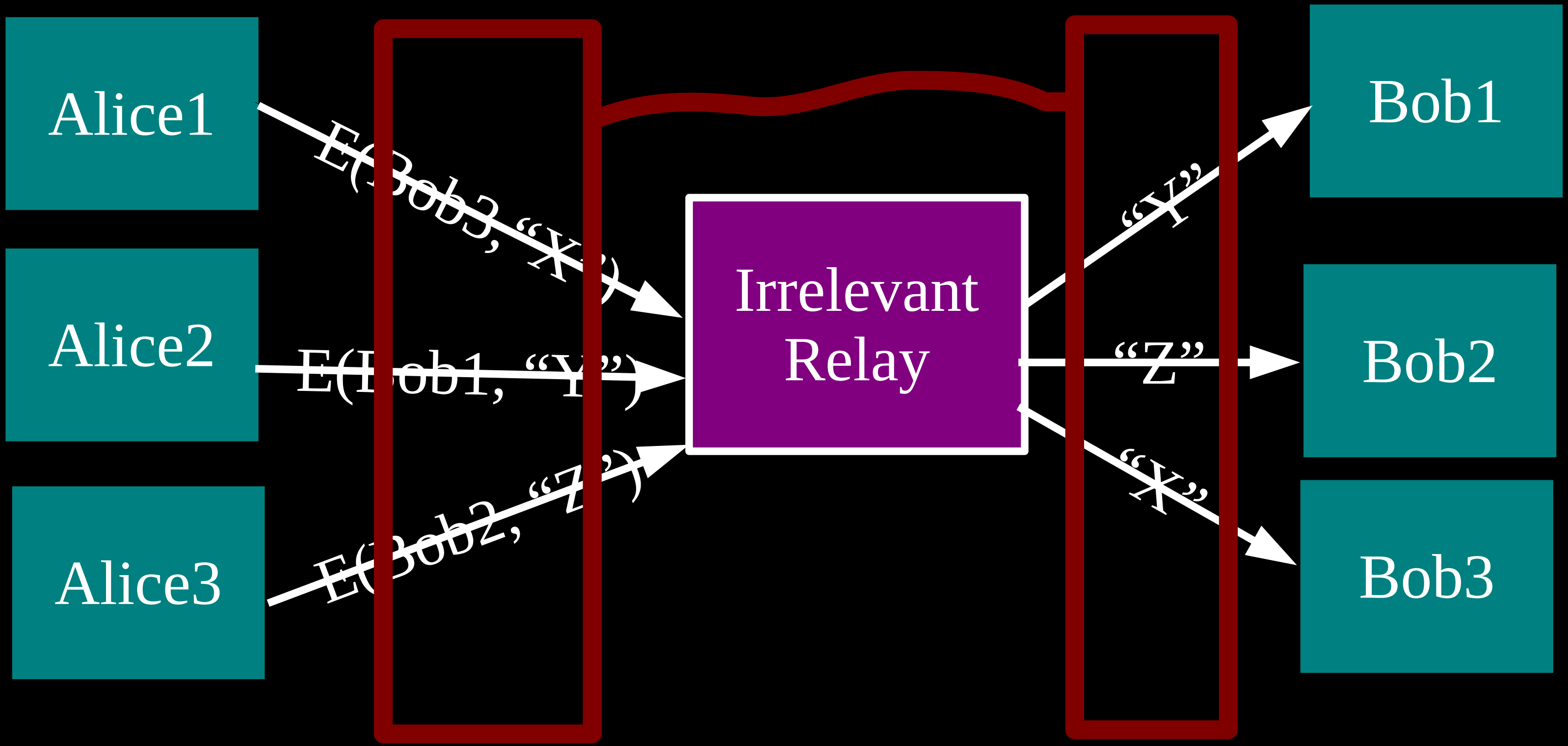


(example: some commercial proxy providers)

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

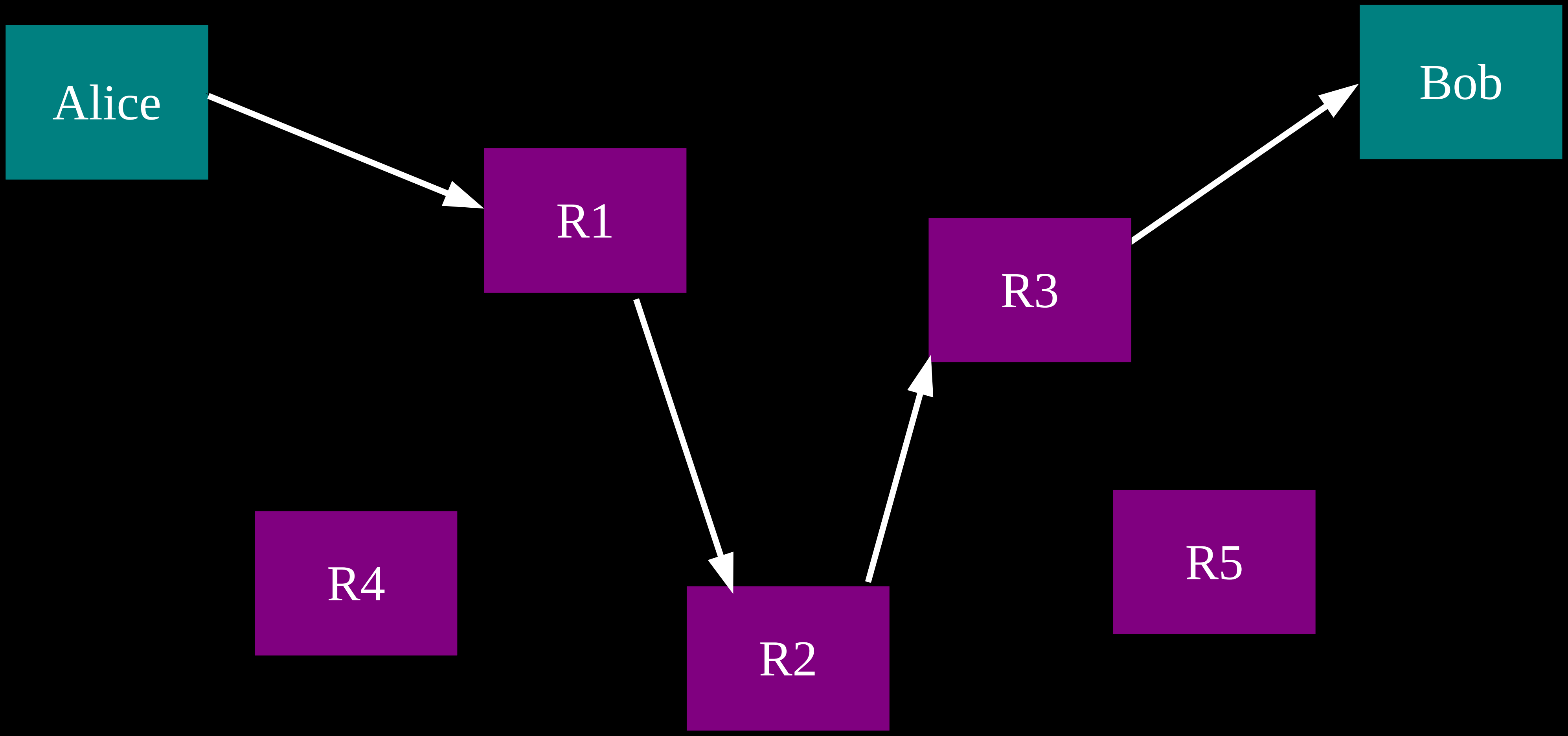


... or a single point of bypass.

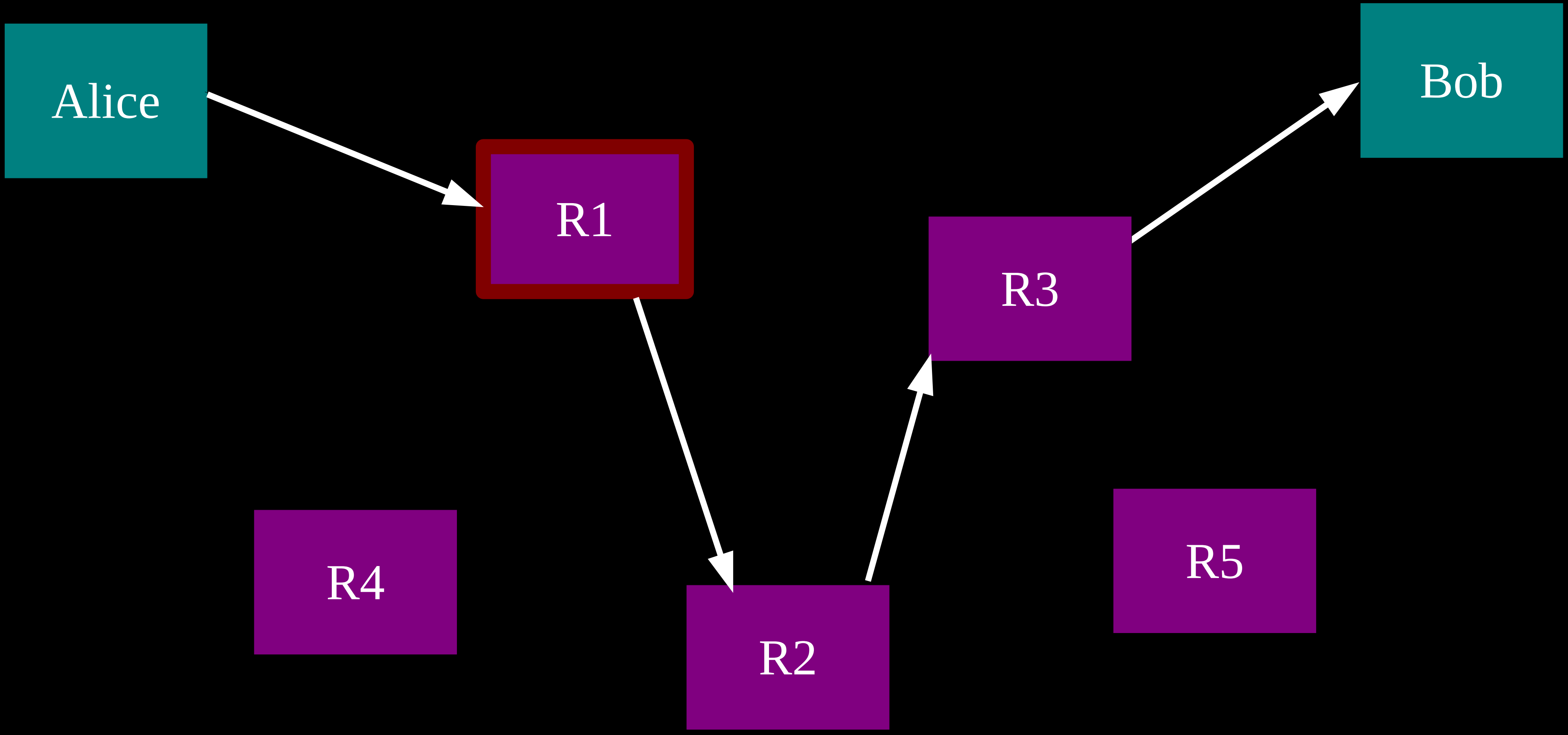


Timing analysis bridges all connections through relay ⇒ An attractive fat target

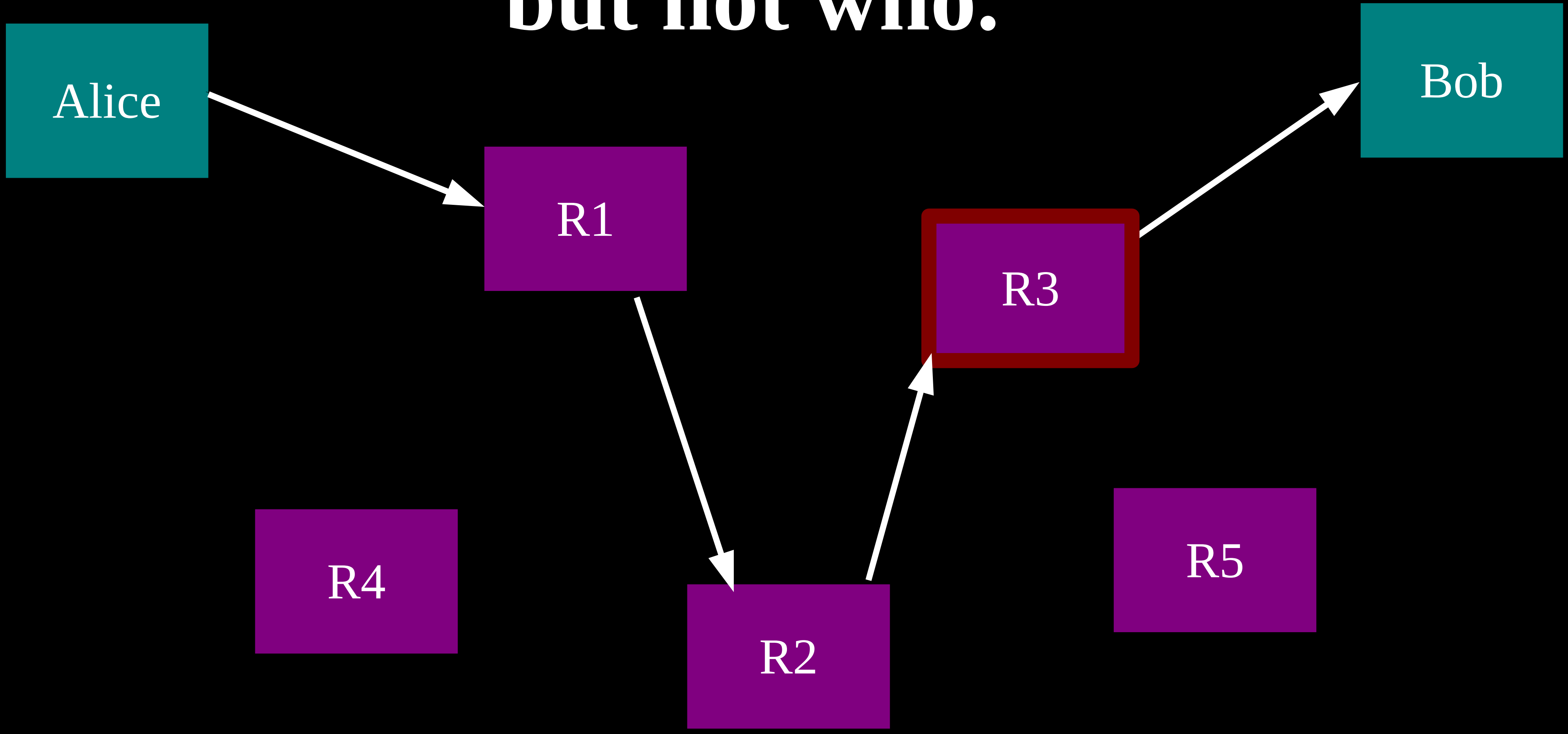
So, add multiple relays so that no single one can betray Alice.



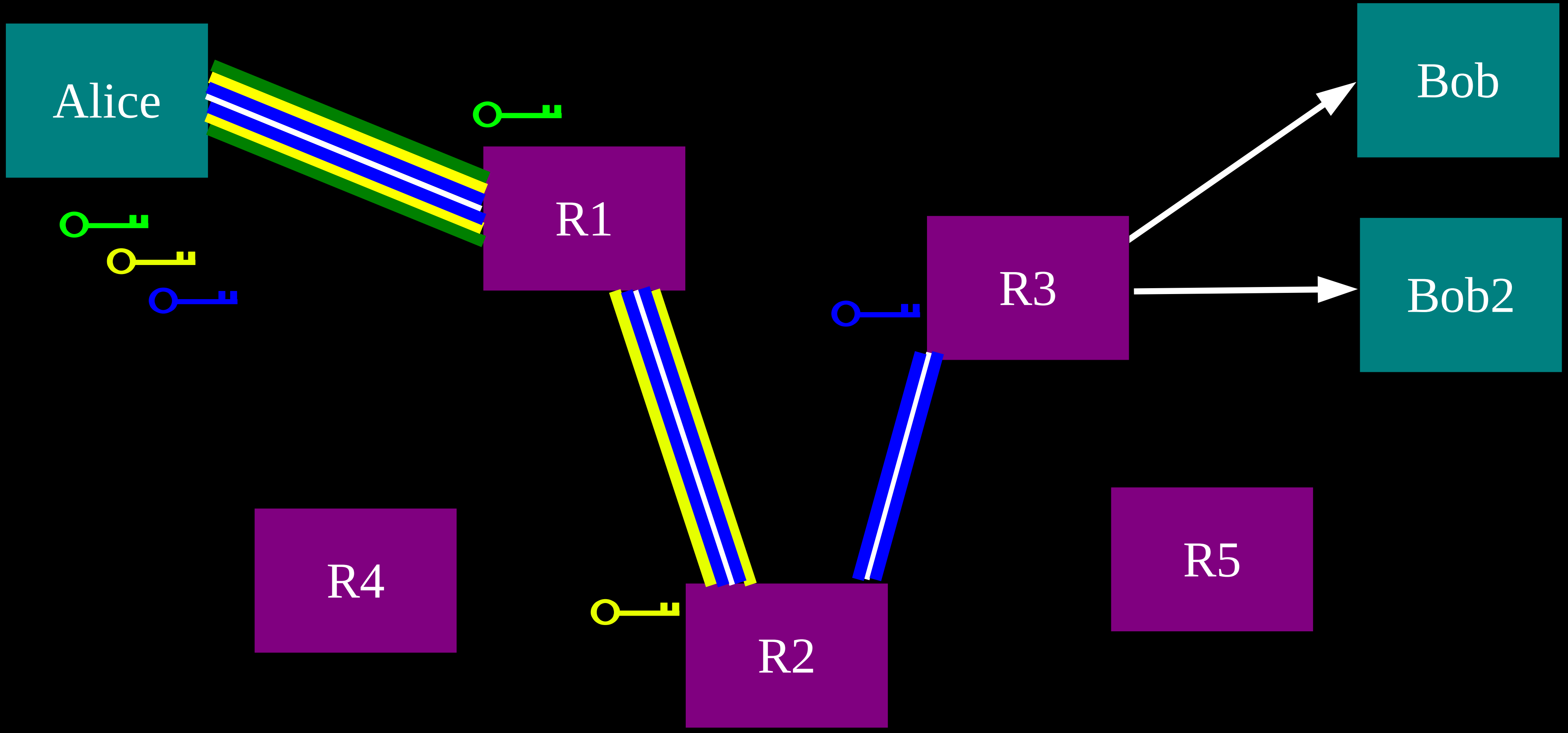
A corrupt first hop can tell that Alice is talking, but not to whom.



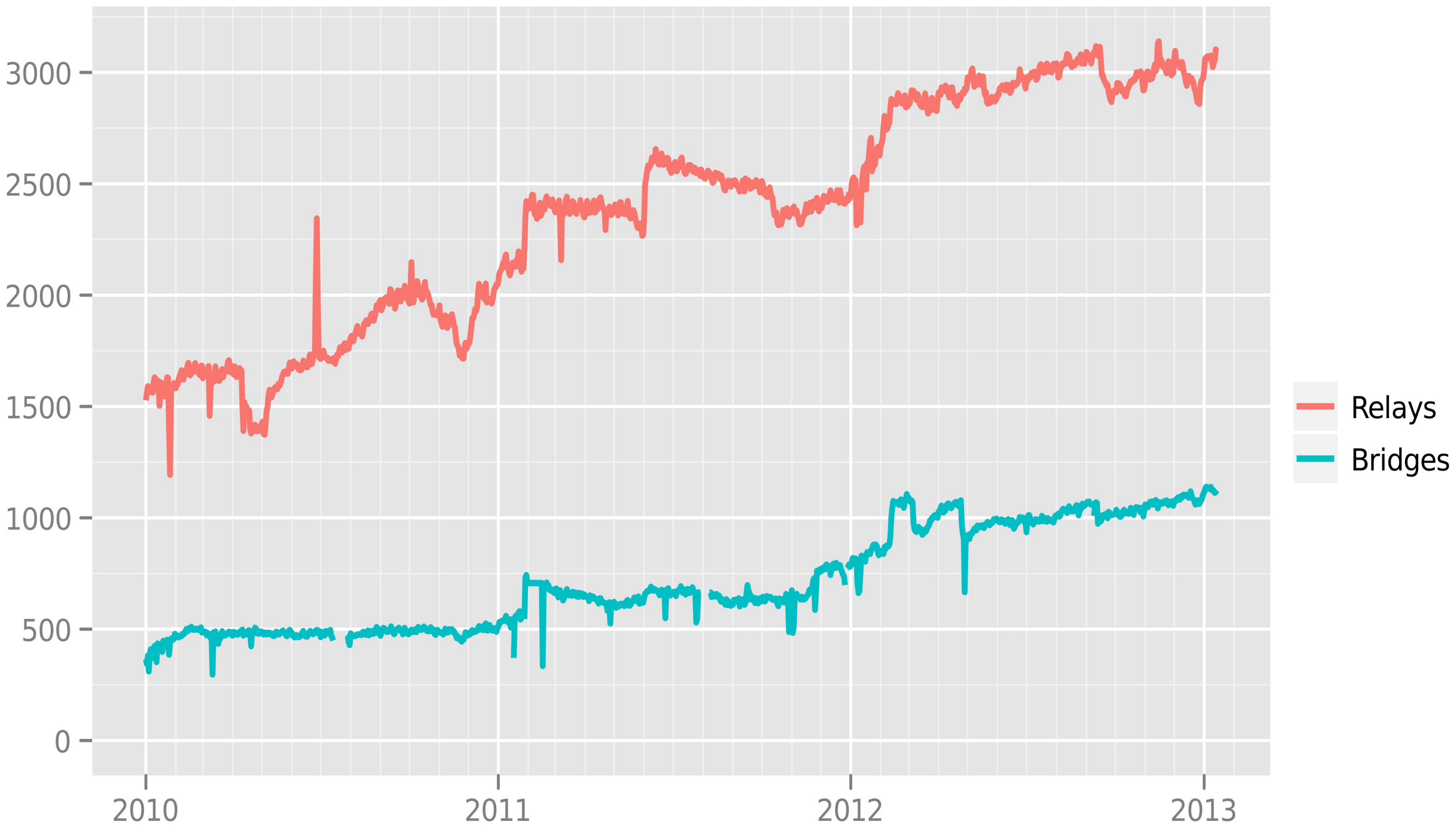
A corrupt final hop can tell that somebody is talking to Bob, but not who.



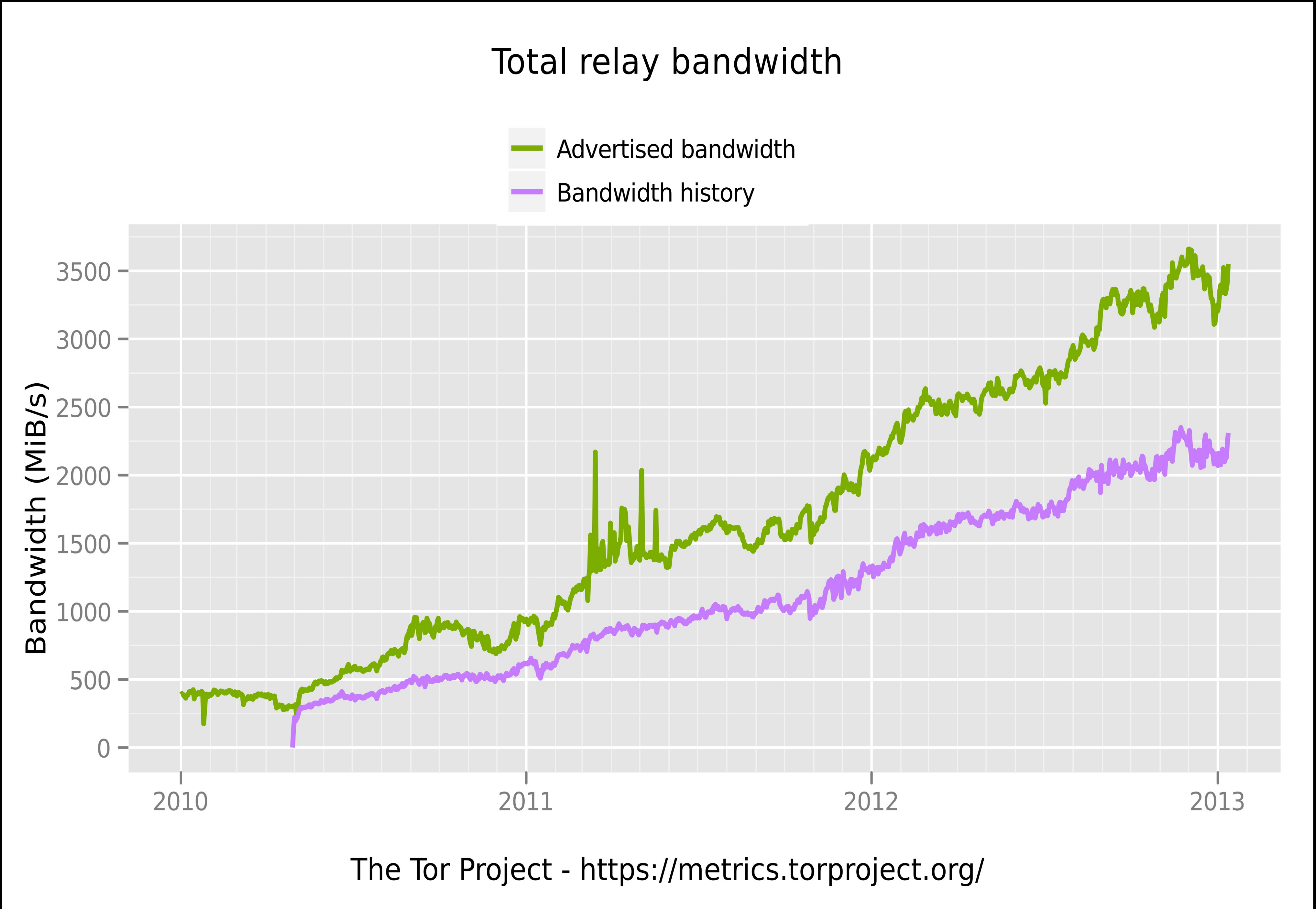
Alice makes a session key with R1
...And then tunnels to R2...and to R3

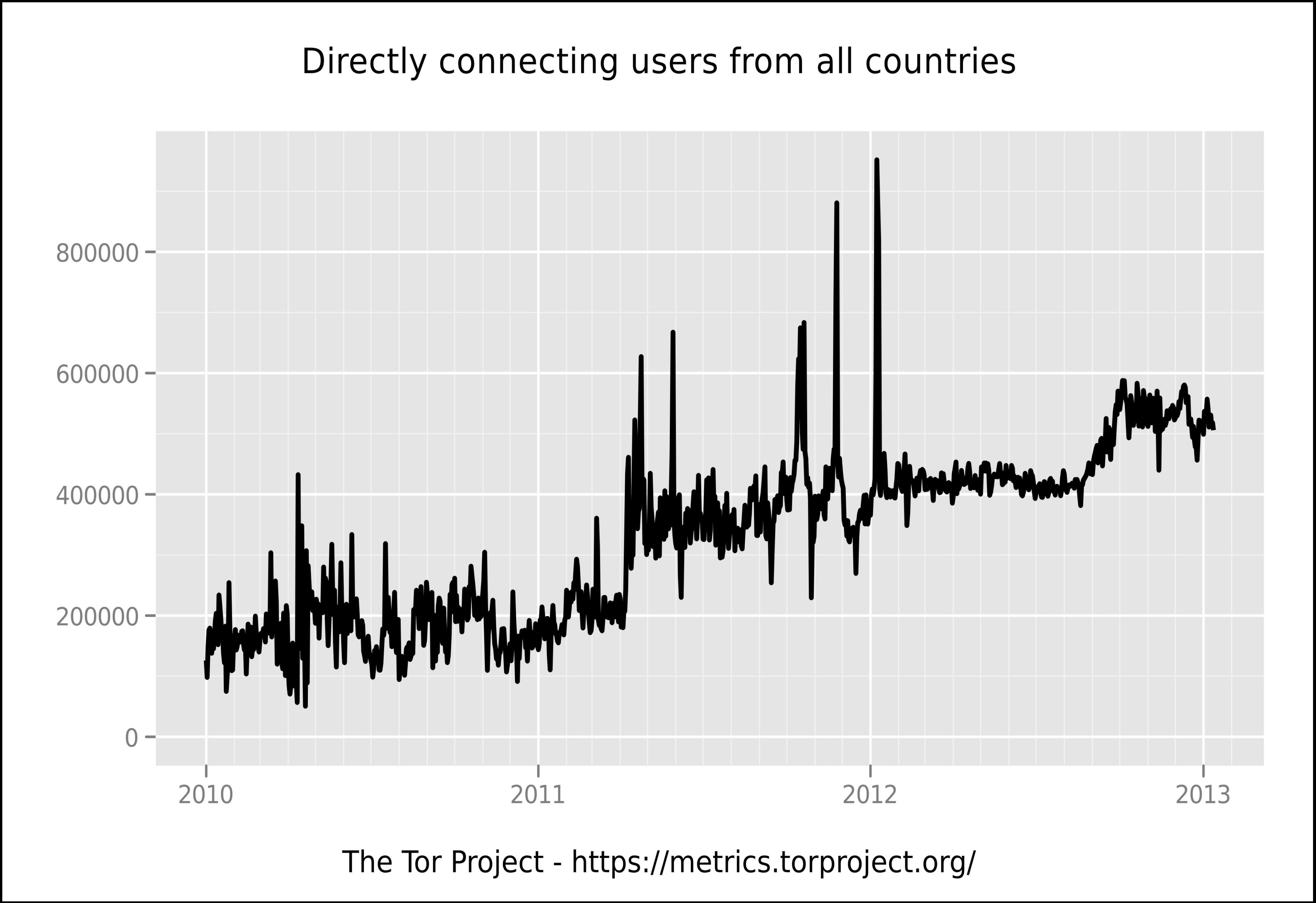


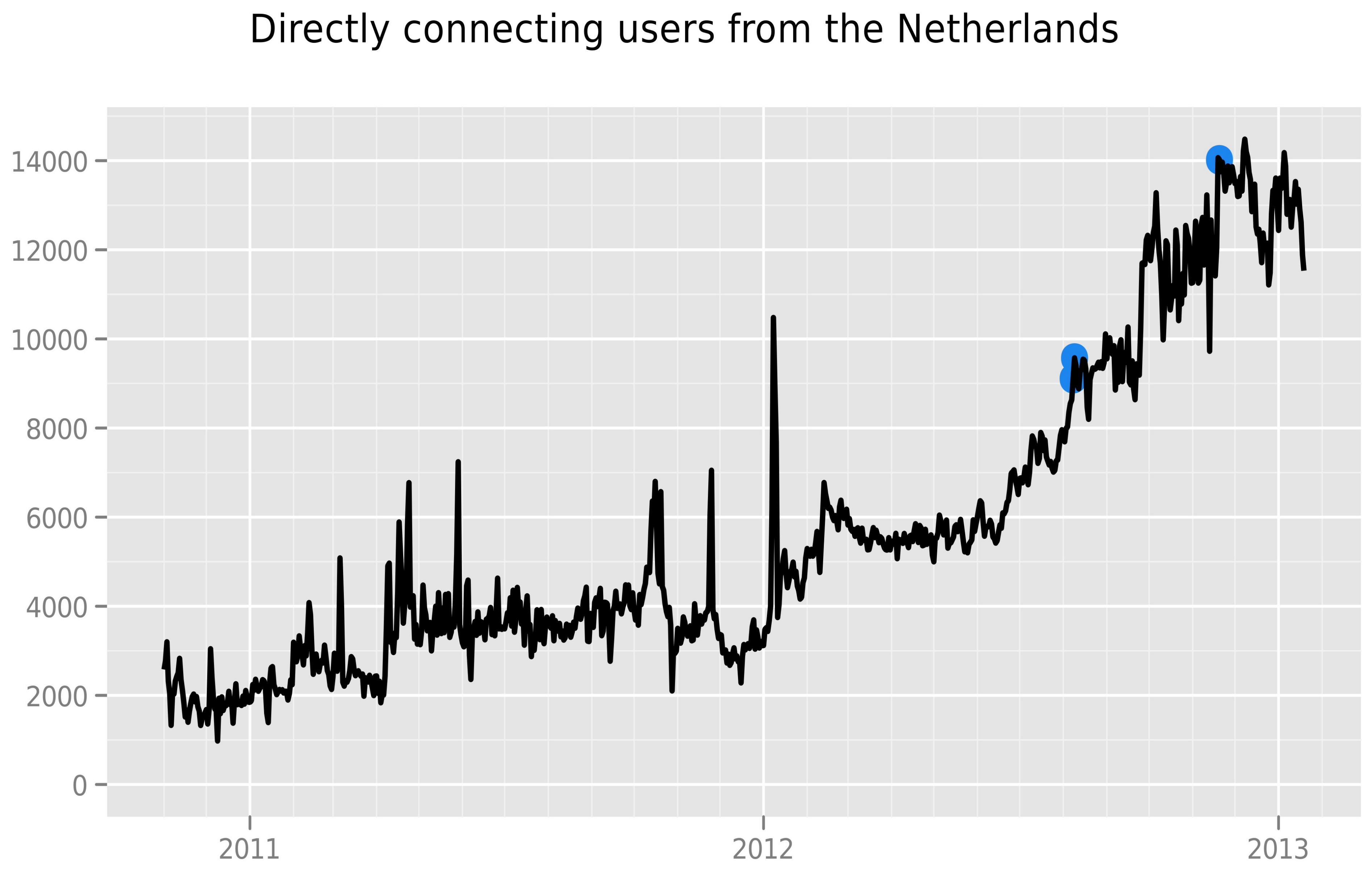
Number of relays



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

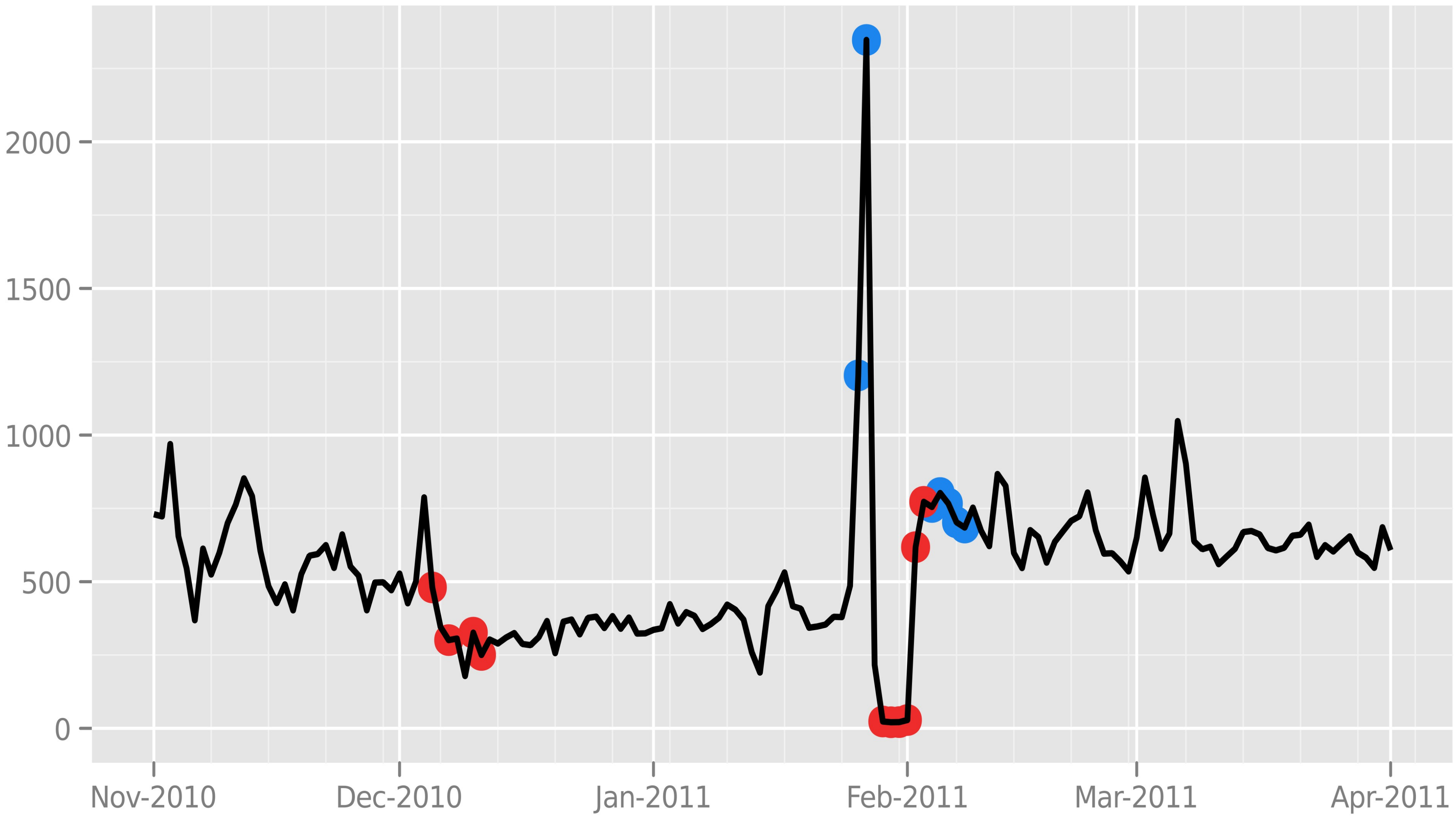

Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
3500
3000
2500
2000
1500
1000
500
0
2010
2011
2012
2013
The Tor Project - https://metrics.torproject.org/


Directly connecting users from all countries
800000
600000
400000
200000
0
2010
2011
2012
2013
The Tor Project - https://metrics.torproject.org/



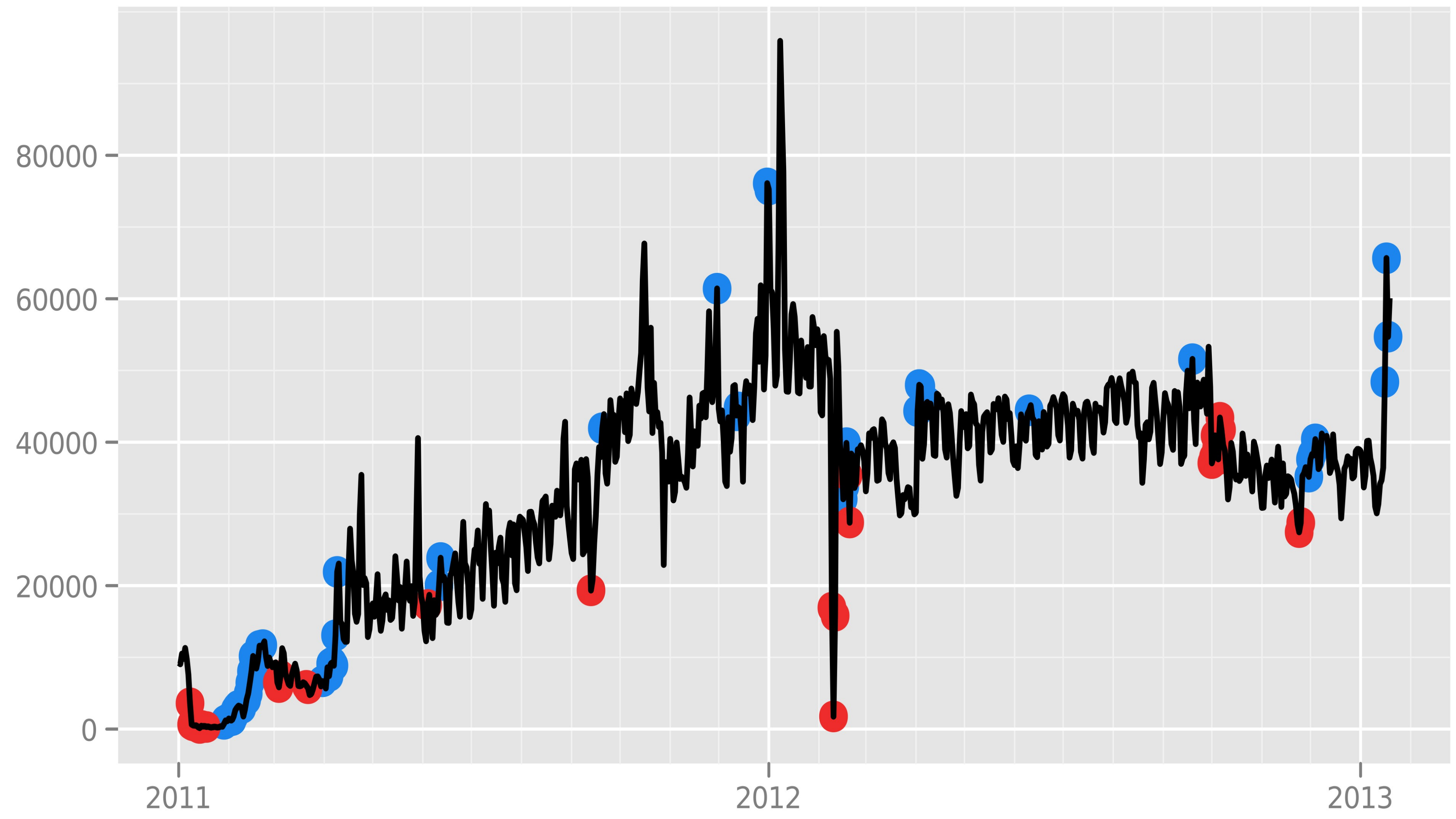
The Tor Project - https://metrics.torproject.org/

Directly connecting users from Egypt



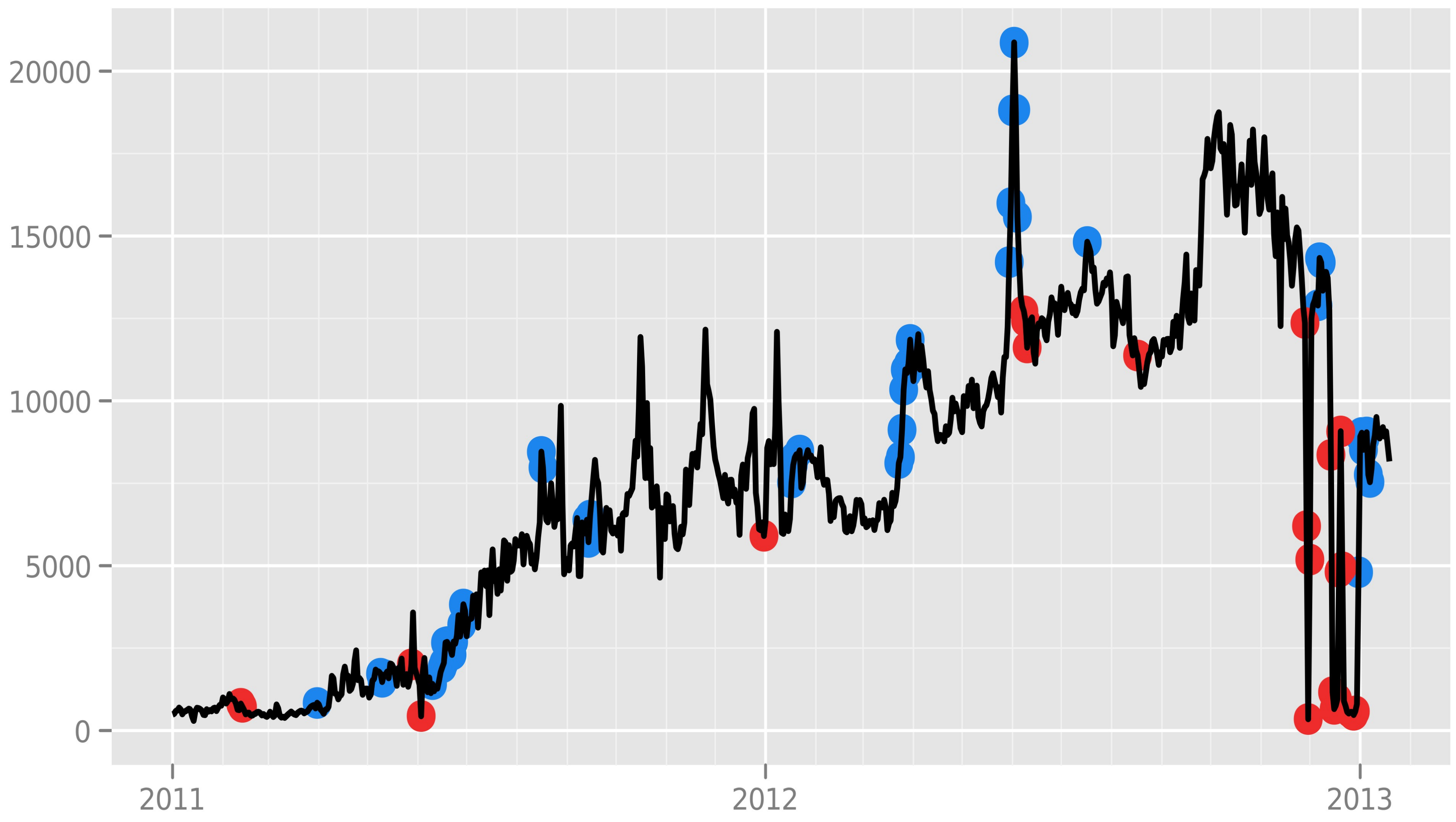
The Tor Project - https://metrics.torproject.org/

Directly connecting users from Iran

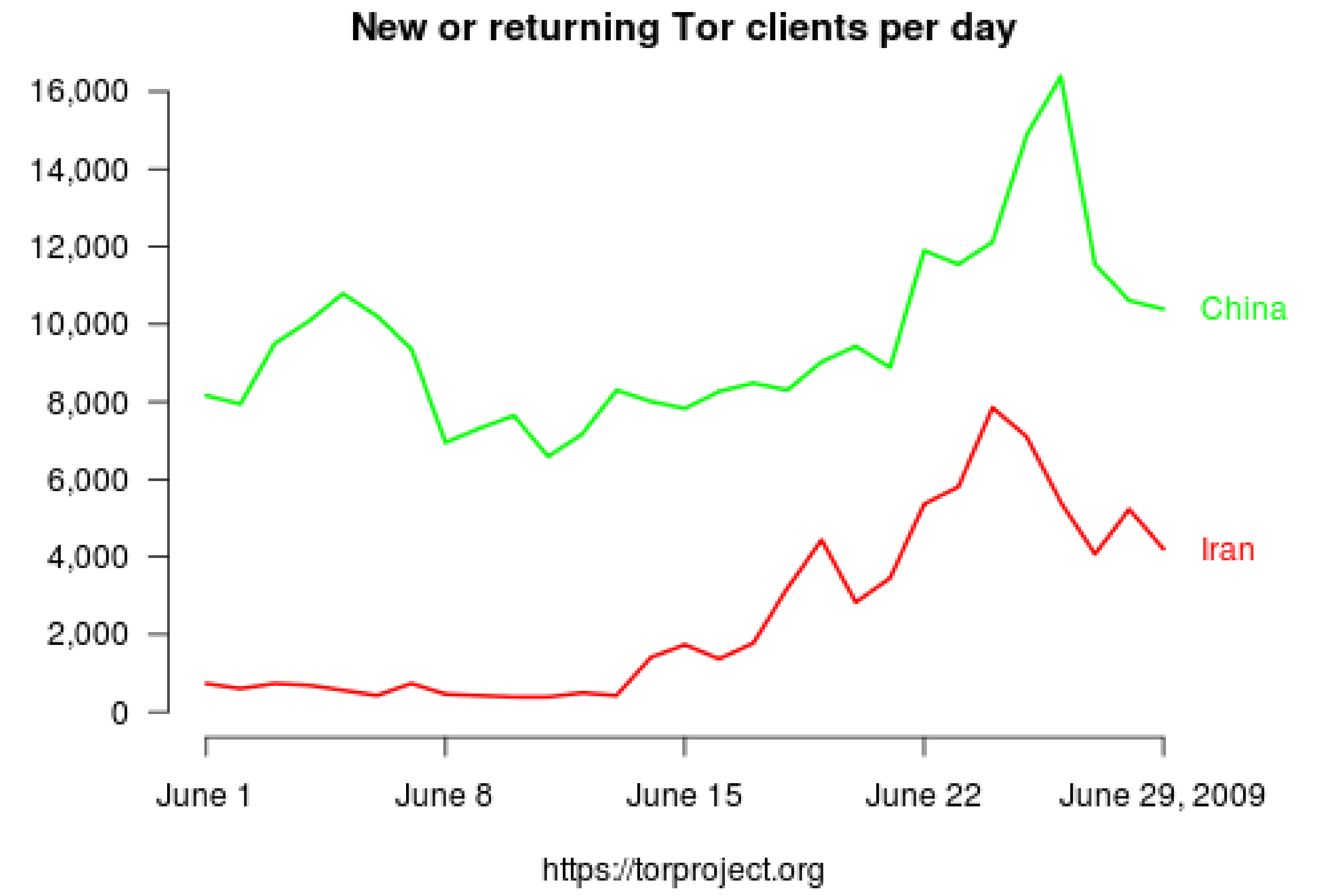


The Tor Project - https://metrics.torproject.org/

Directly connecting users from the Syrian Arab Republic



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


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

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.

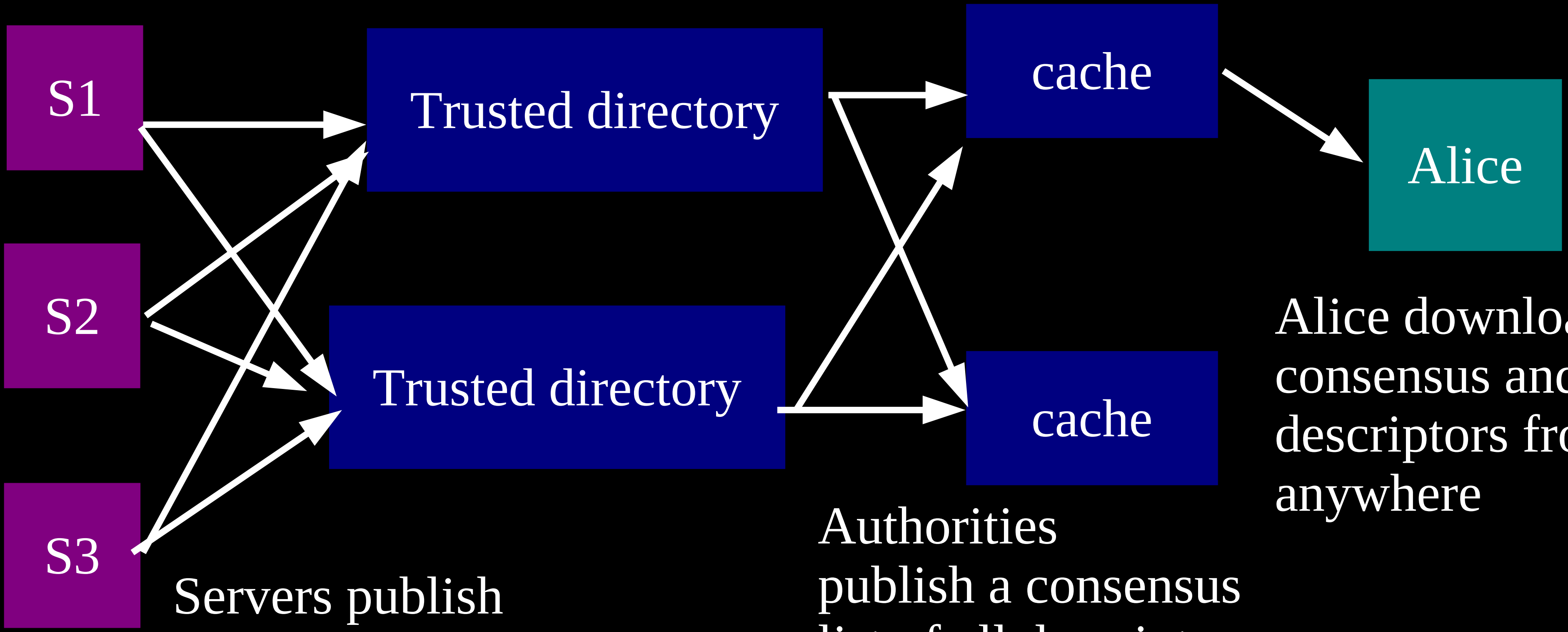
Relay versus Discovery

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

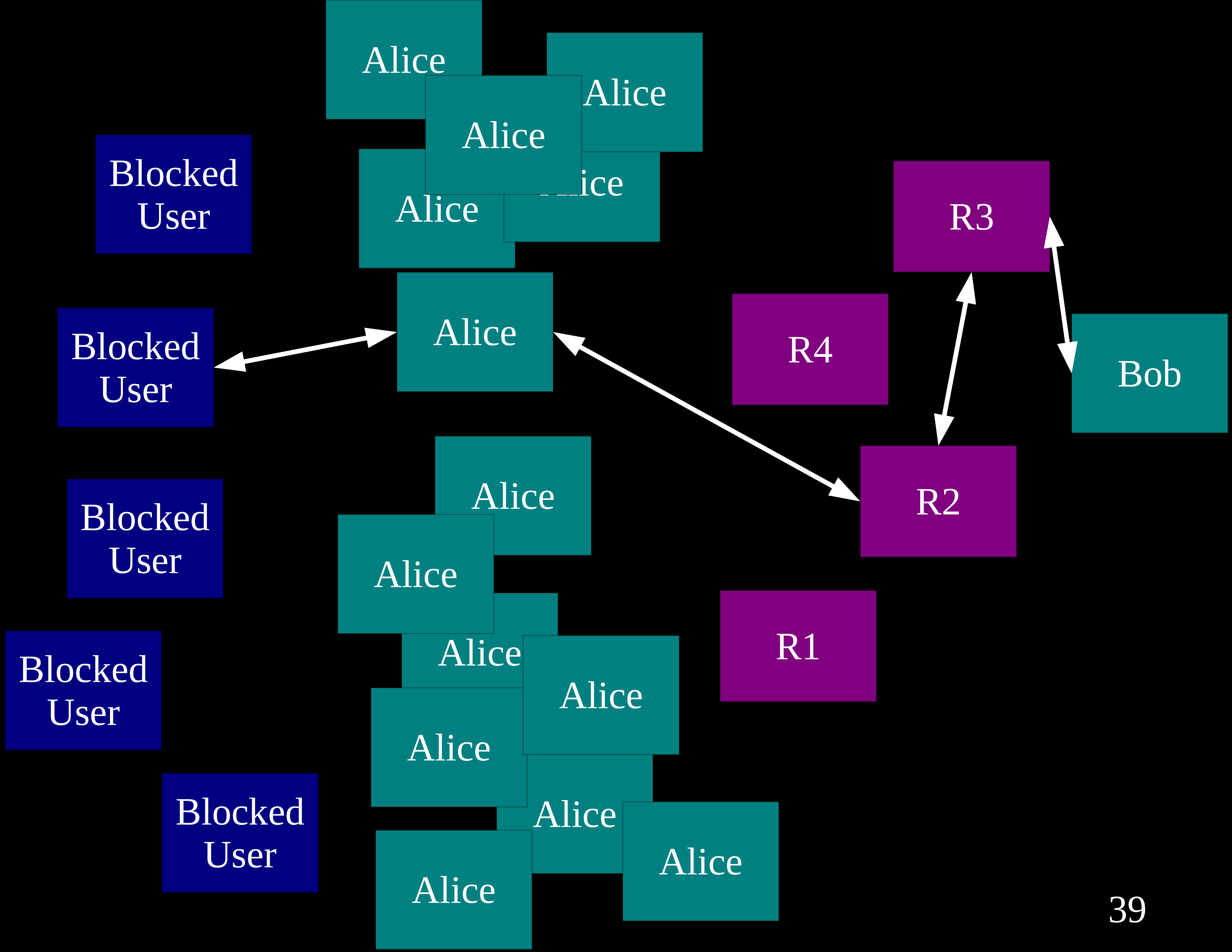
The basic Tor design uses a simple centralized directory protocol.



Servers publish self-signed descriptors.

Authorities publish a consensus list of all descriptors

Alice downloads consensus and descriptors from anywhere


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

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

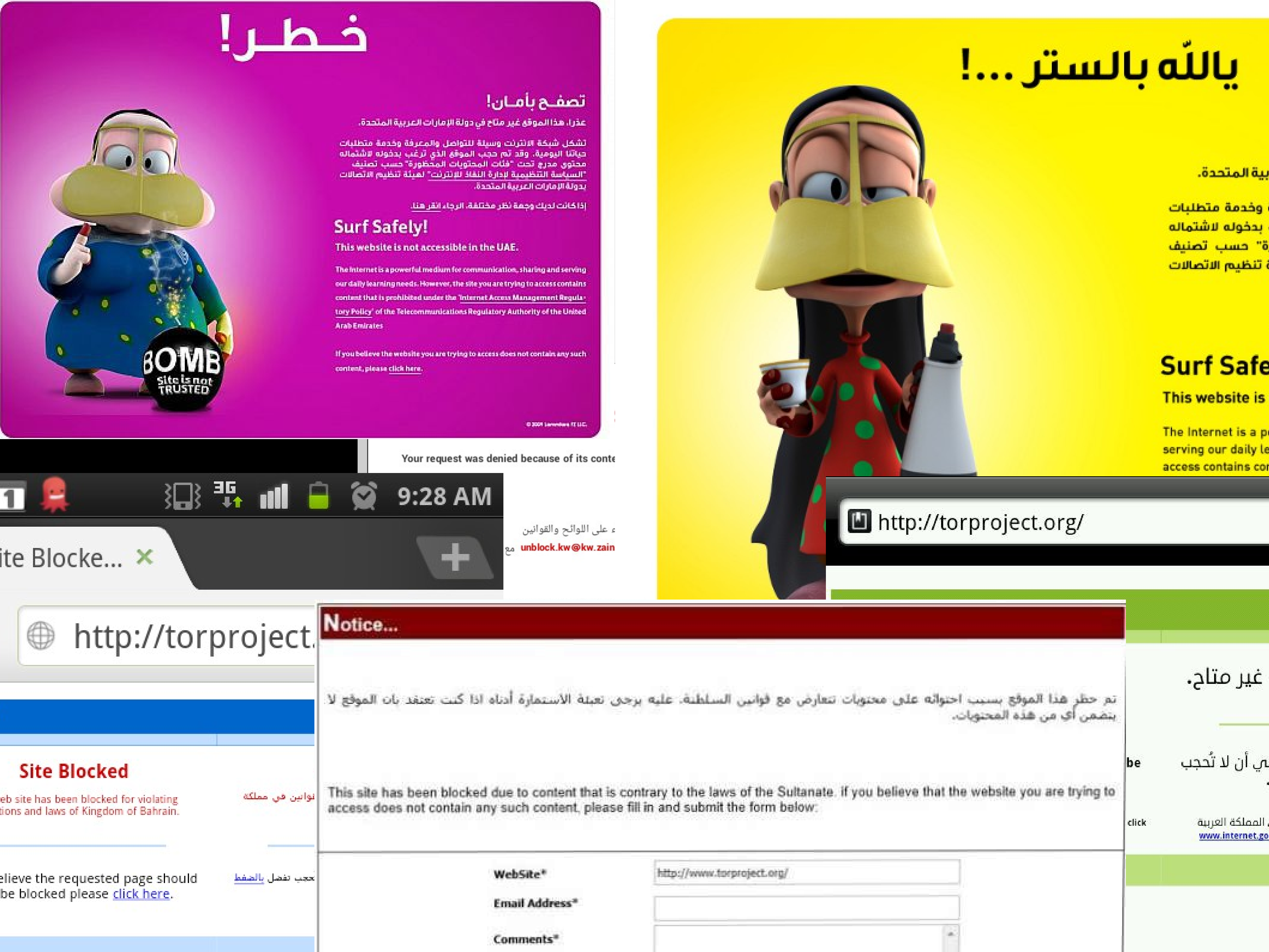
Attackers can block users from connecting to the Tor network

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)



خـطـر!

تصفـح بأمـان!

عذرا، هذا الموقع غير متاح في دولة الإمارات العربية المتحدة.

تشكل شبكة الانترنت وسيلة للتواصل والمعرفة وخدمة متطلبات حياتنا اليومية. وقد تم حجب الموقع الذي ترغب بدخوله لاشتماله محتوى مدرج تحت "فئات المحتويات المحظورة" 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 Lamantara IT LLC.

Your request was denied because of its conte

ء على اللوائح والقوانين

مع unblock.kw@kw.zain

يالله بالستر ...!

بية المتحدة.

وخدمة متطلبات
بدخوله لاشتماله
ة" حسب تصنيف
ة تنظيم الاتصالات

Surf Safe

This website is

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

http://torproject.org/

9:28 AM

ite Blocke... ×

http://torproject.

Site Blocked

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

وانين في مملكة

elieve the requested page should
be blocked please click here.

حجب تفضل بالضغط

Notice...

تم حظر هذا الموقع بسبب احتوائه على محتويات تتعارض مع قوانين السلطنة. عليه يرجى تعبئة الأستمارة 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*	http://www.torproject.org/
Email Address*	
Comments*	

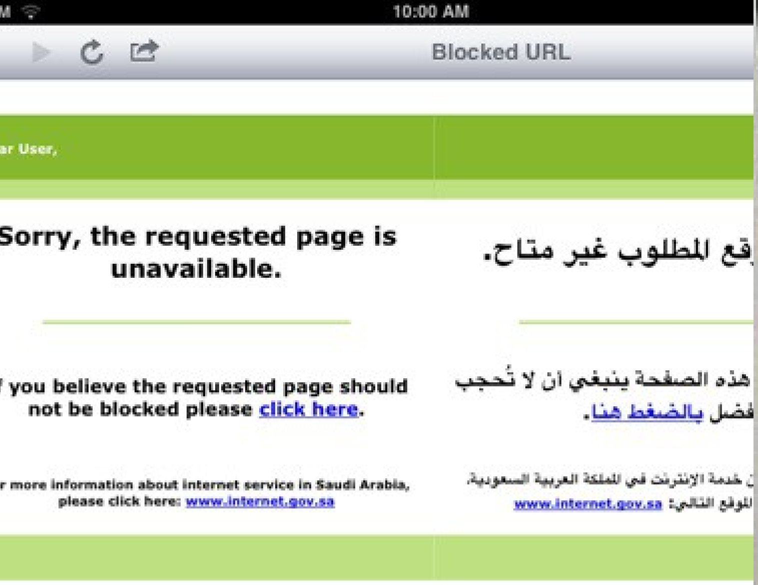
غير متاح.

be

ي أن لا تُحجب

click

المملكة العربية
www.internet.go



ar User,

Sorry, the requested page is unavailable.

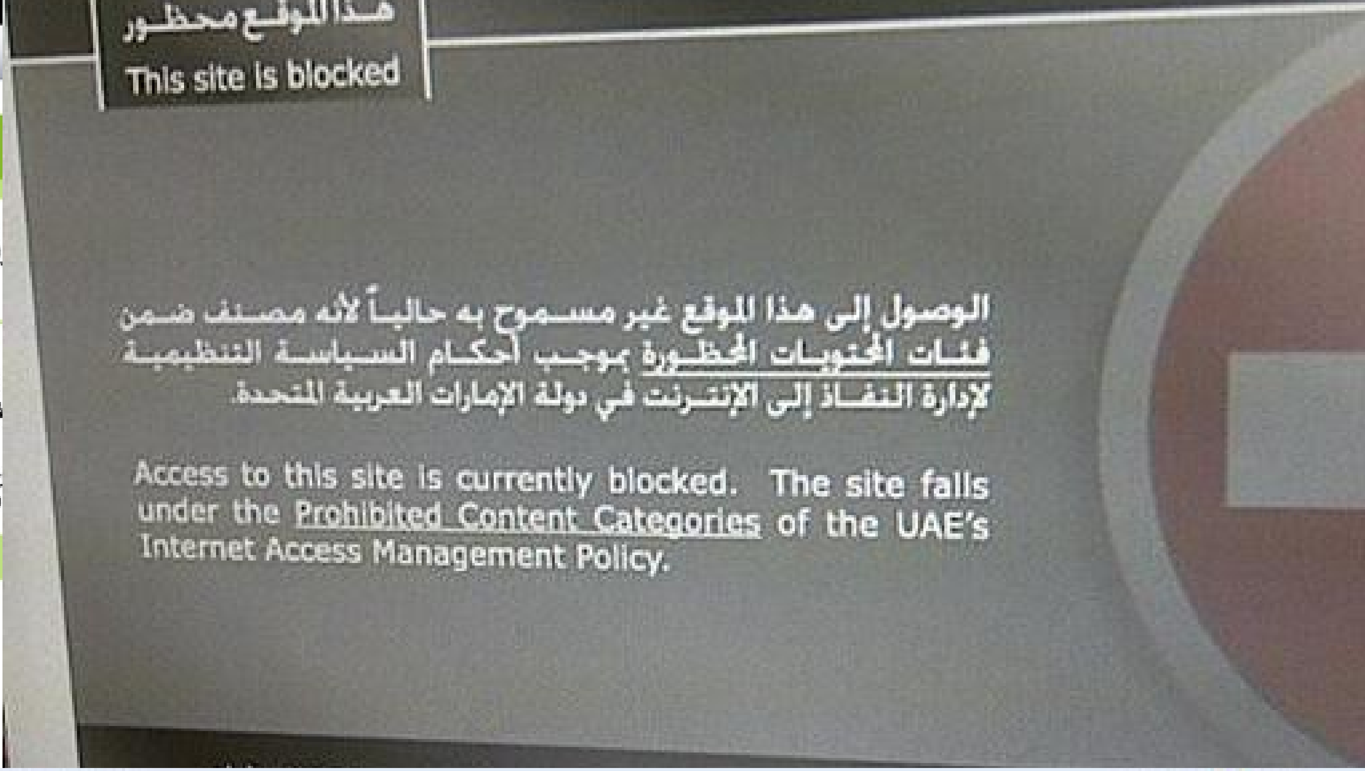
قع المطلوب غير متاح.

you believe the requested page should not be blocked please click here.

هذه الصفحة ينبغي ان لا تُحجب
فضل بالضغط هنا.

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

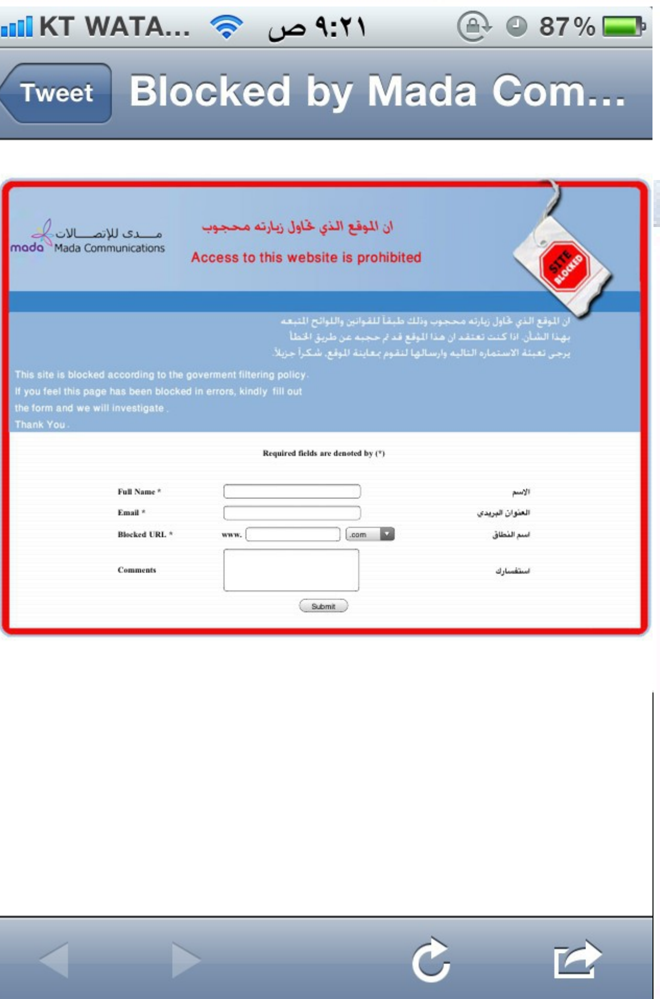
خدمة الإنترنت في المملكة العربية السعودية،
الموقع التالي: www.internet.gov.sa


هـذا الموقـع محظـور

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.



ان الموقع الذي تحاول زيارته محجوب

Access to this website is prohibited

ان الموقع الذي تحاول زيارته محجوب وذلك طبقاً للقوانين واللوائح المتبعه
بهذا الشأن. اذا كنت تعتقد ان هذا الموقع قد تم حجبه عن طريق الخطأ
يرجى تعبئة الاستماره التاليه وارسالها لنقوم بمعاينة الموقع. شكراً جزيلاً.

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 (*)

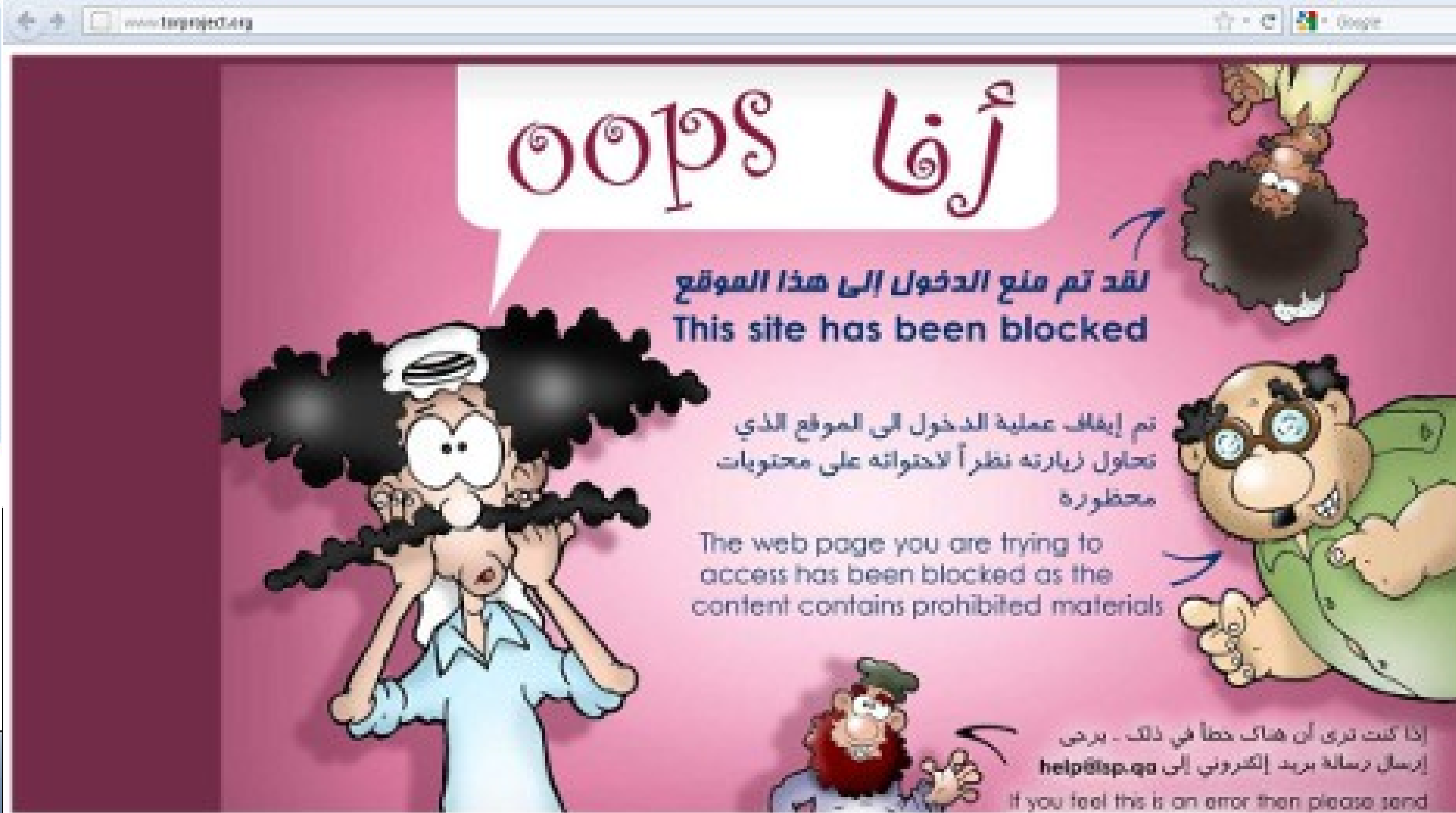
Full Name * ____ الإسم

Email * ____ العنوان البريدي

Blocked URL * www. ____ .com اسم النطاق

Comments ____ استفسارك

Submit



لقد تم منع الدخول إلى هذا الموقع

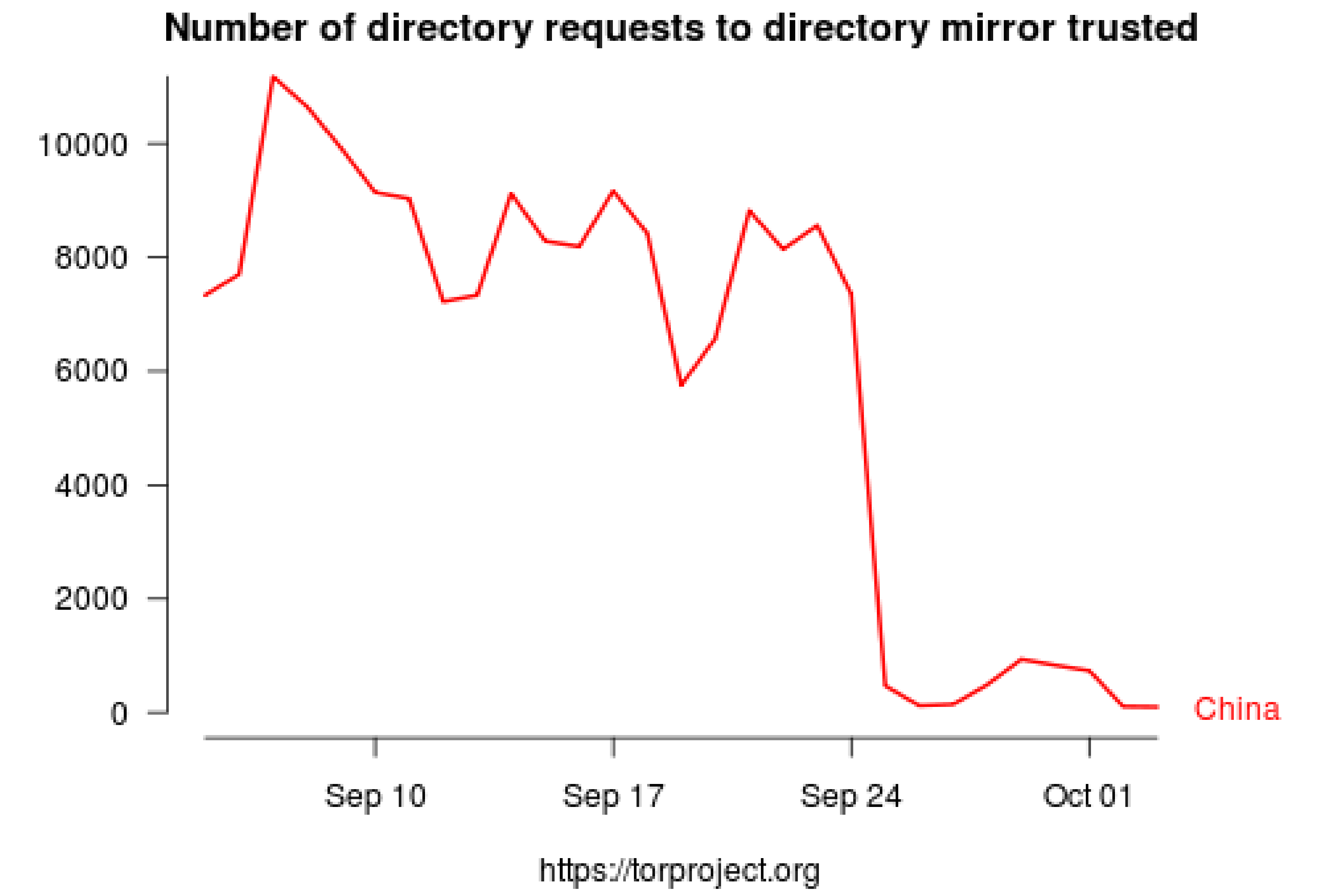
This site has been blocked

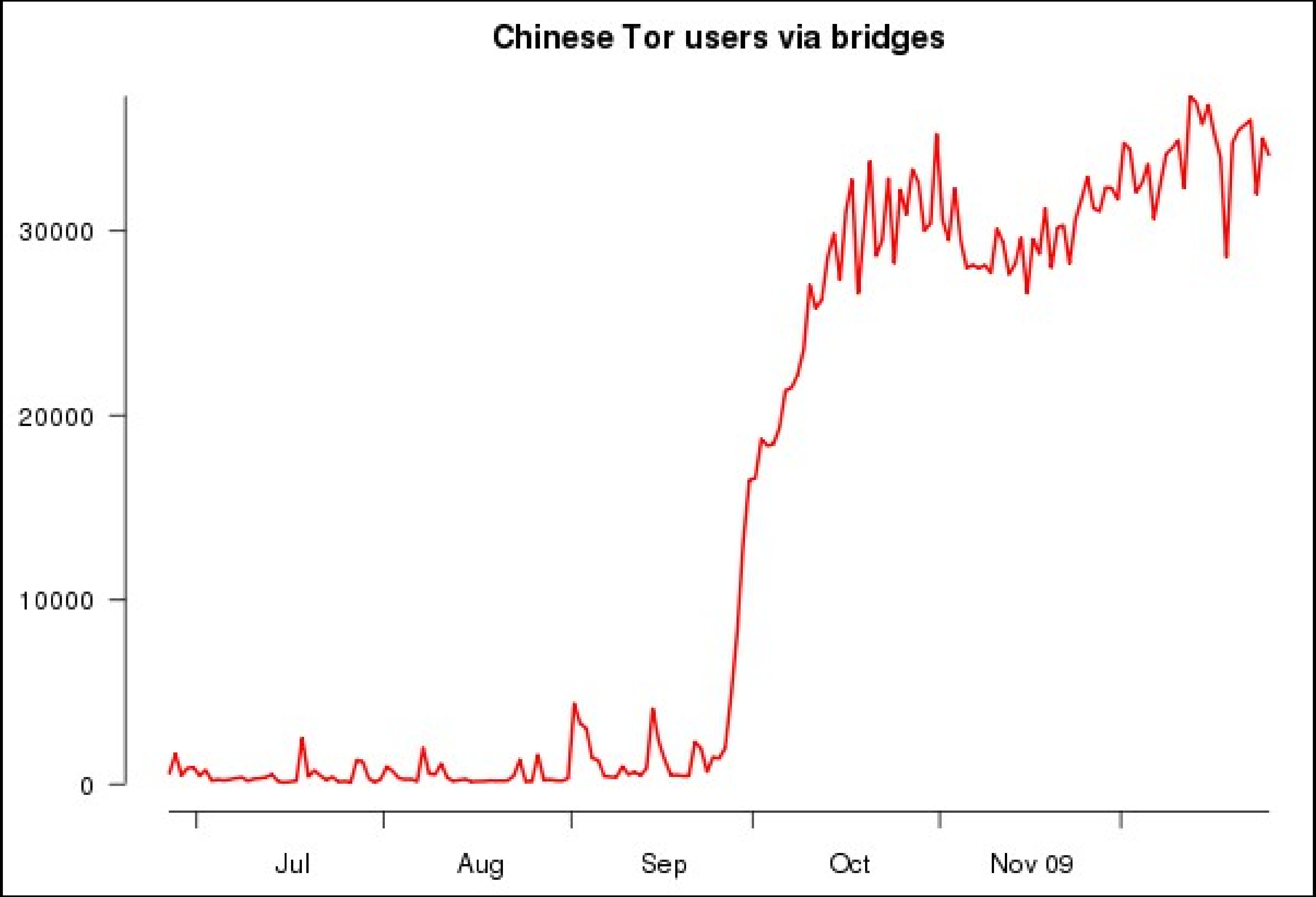
تم إيقاف عملية الدخول الى الموقع الذي تحاول زيارته نظراً لاحتوائه على محتويات محظورة

The web page you are trying to access has been blocked as the content contains prohibited materials

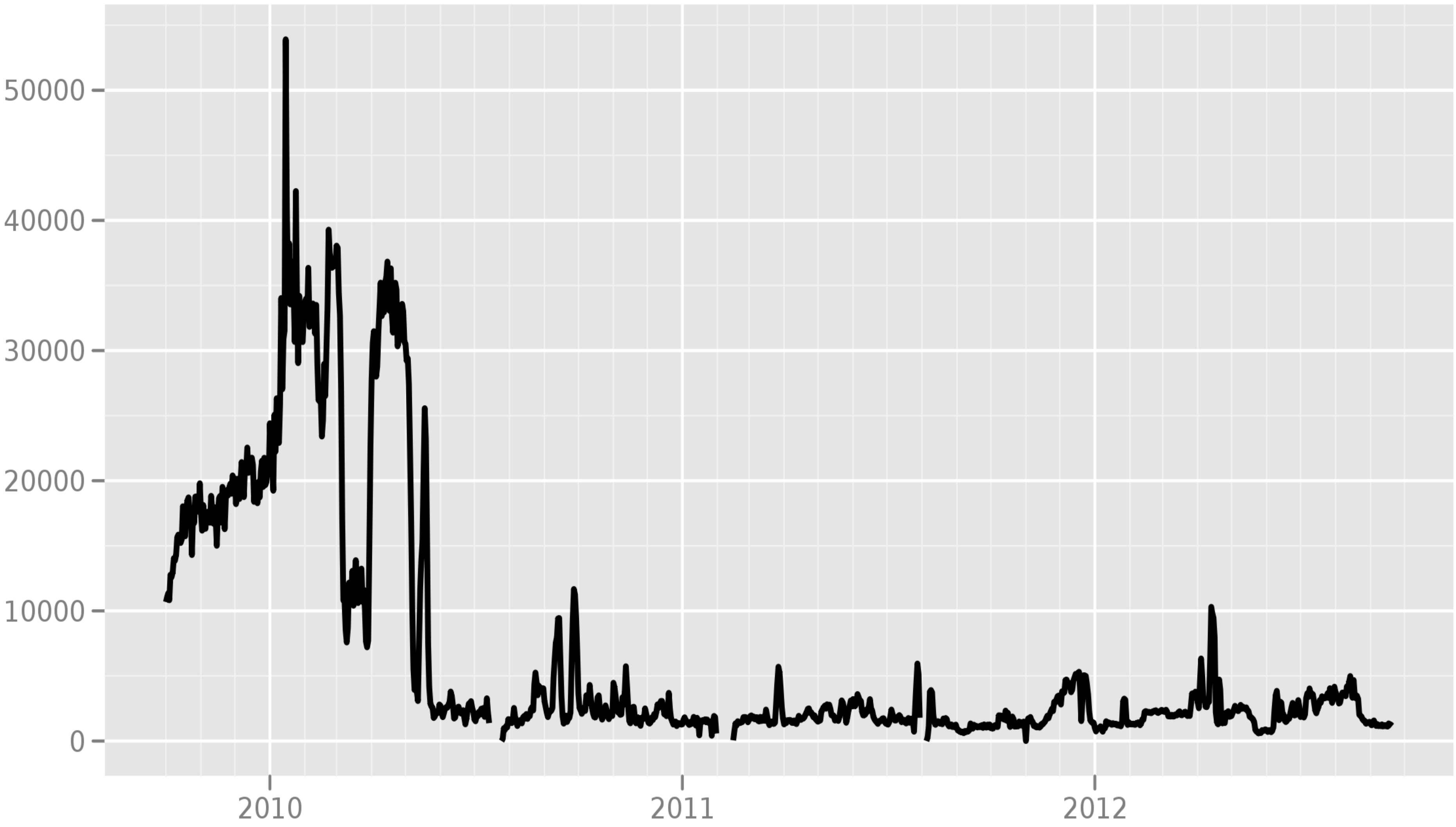
إذا كنت ترى أن هناك خطأ في ذلك ، يرجى
إرسال رسالة بريد إلكتروني إلى help@isp.qa

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

Bridge users from China



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

What we spend our time on

Performance and scalability

Maintaining the whole software ecosystem

Blocking-resistance (circumvention)

Basic research on anonymity

Reusability and modularity

Advocacy, education, and trainings around the world

Metrics, data, and analysis

Javascript, cookies, history, etc

Javascript refresh attack

Cookies, History, browser window size, user-agent, language, http auth, ...

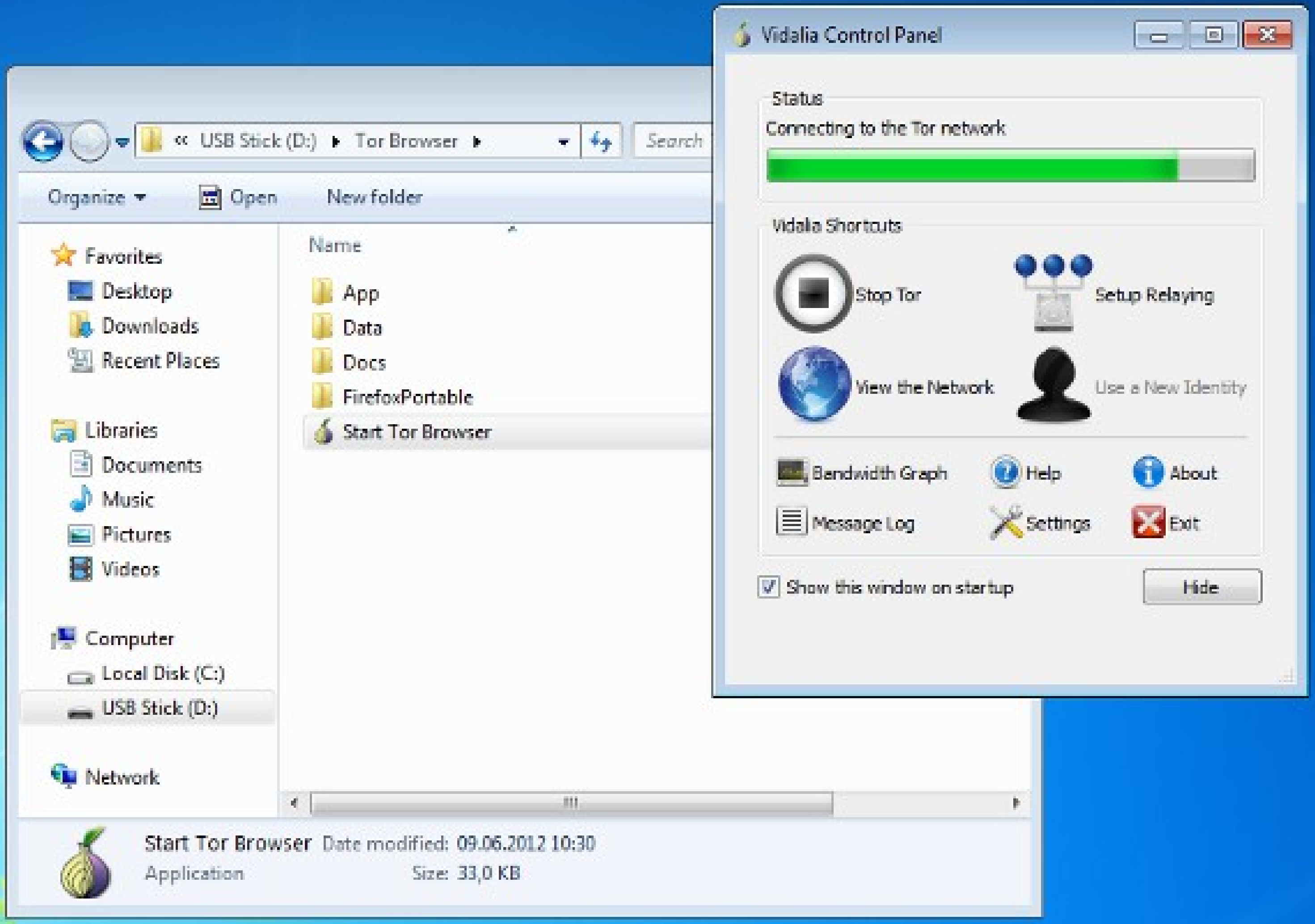
Our Torbutton Firefox extension tackles many of these

Flash is dangerous too

Some apps are bad at obeying their proxy settings.

Adobe PDF plugin. Flash. Other plugins. Extensions. Especially Windows stuff: did you know that Microsoft Word is a network app?

Tor Browser Bundle (TBB)



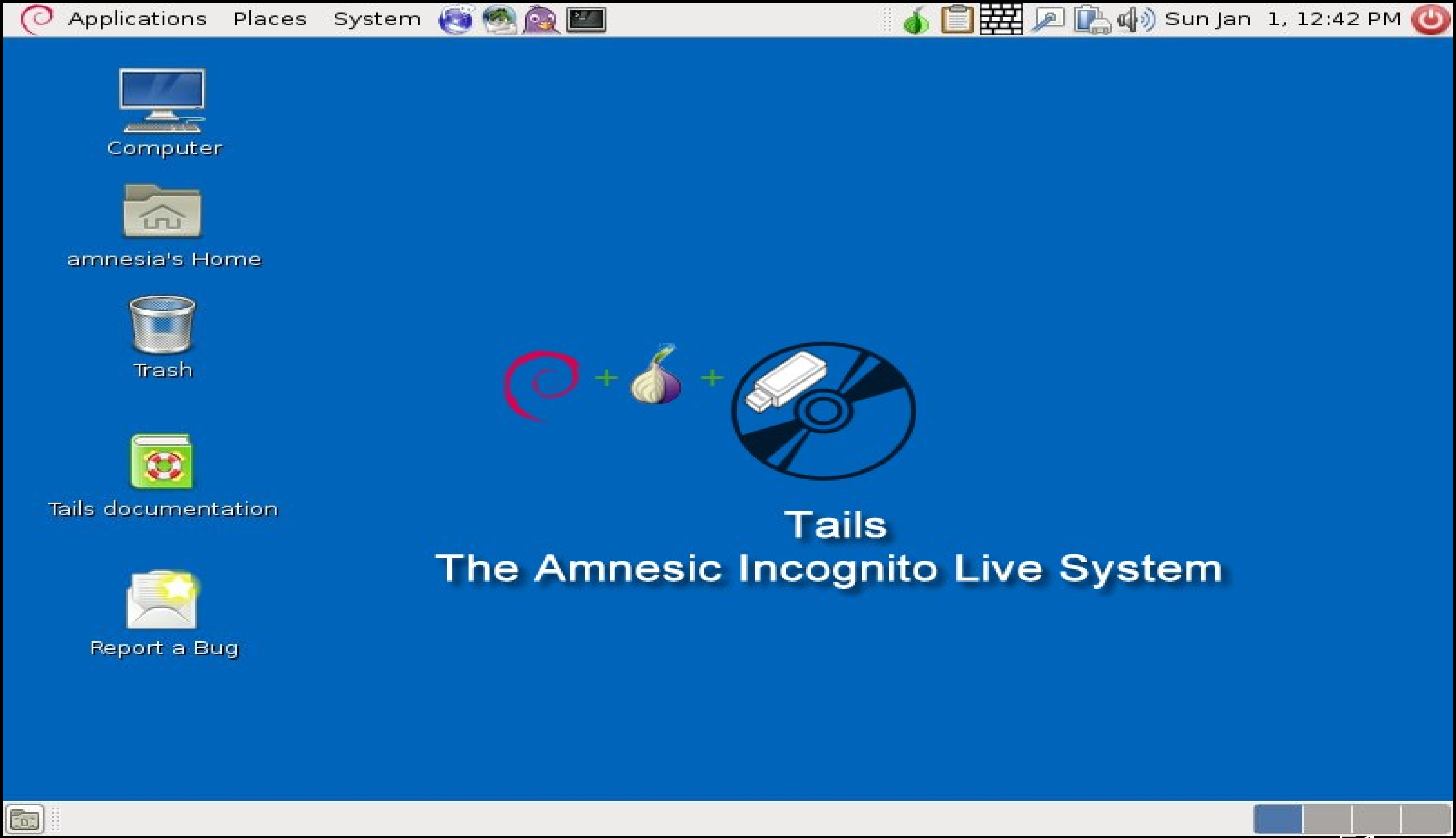
Status

Connecting to the Tor network

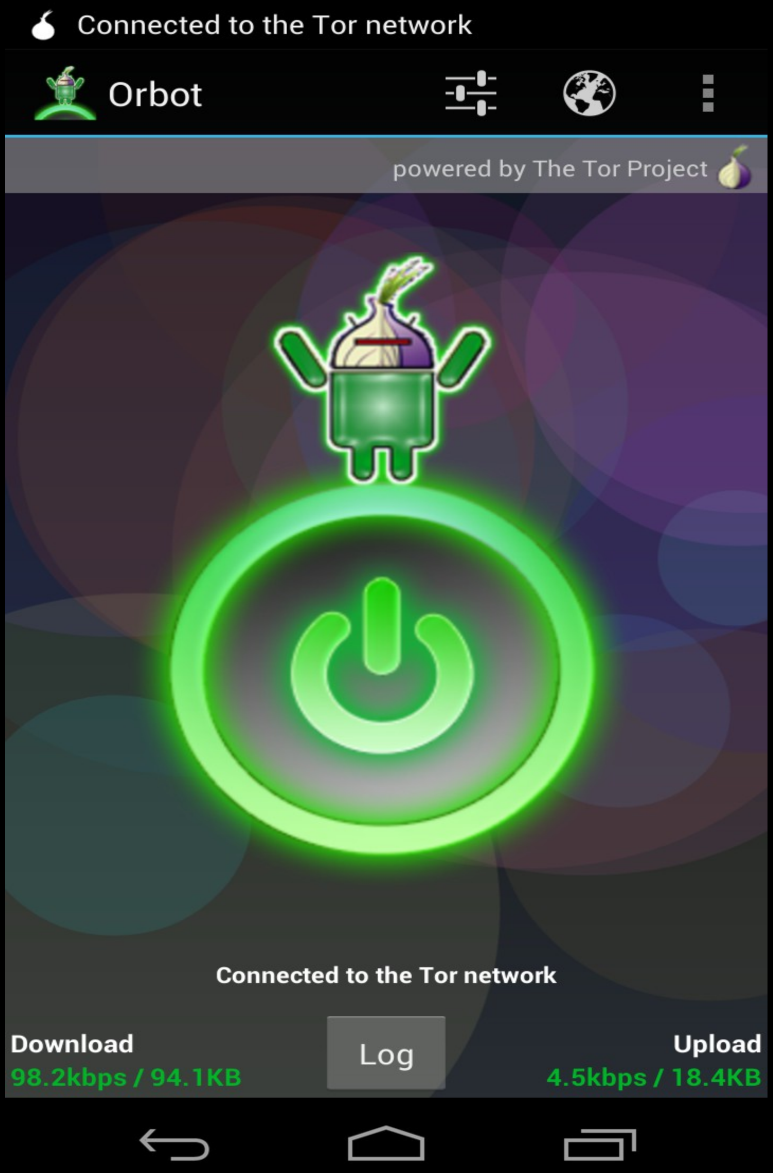
Start Tor Browser Date modified: 09.06.2012 10:30

Application Size: 33,0 KB

Tails (Tor LiveCD)



Orbot (Tor for Android)



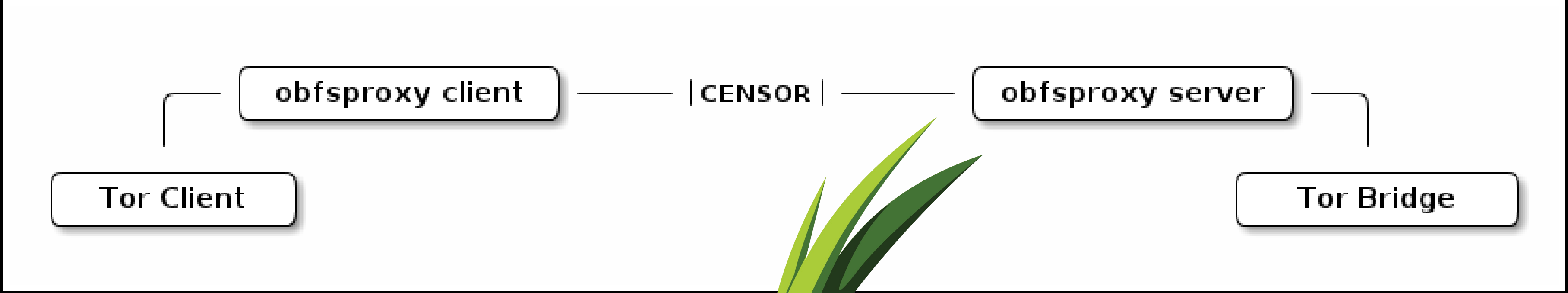
Connected to the Tor network

Connected to the Tor network

Download
98.2kbps / 94.1KB

Upload
4.5kbps / 18.4KB

Tor pluggable transports



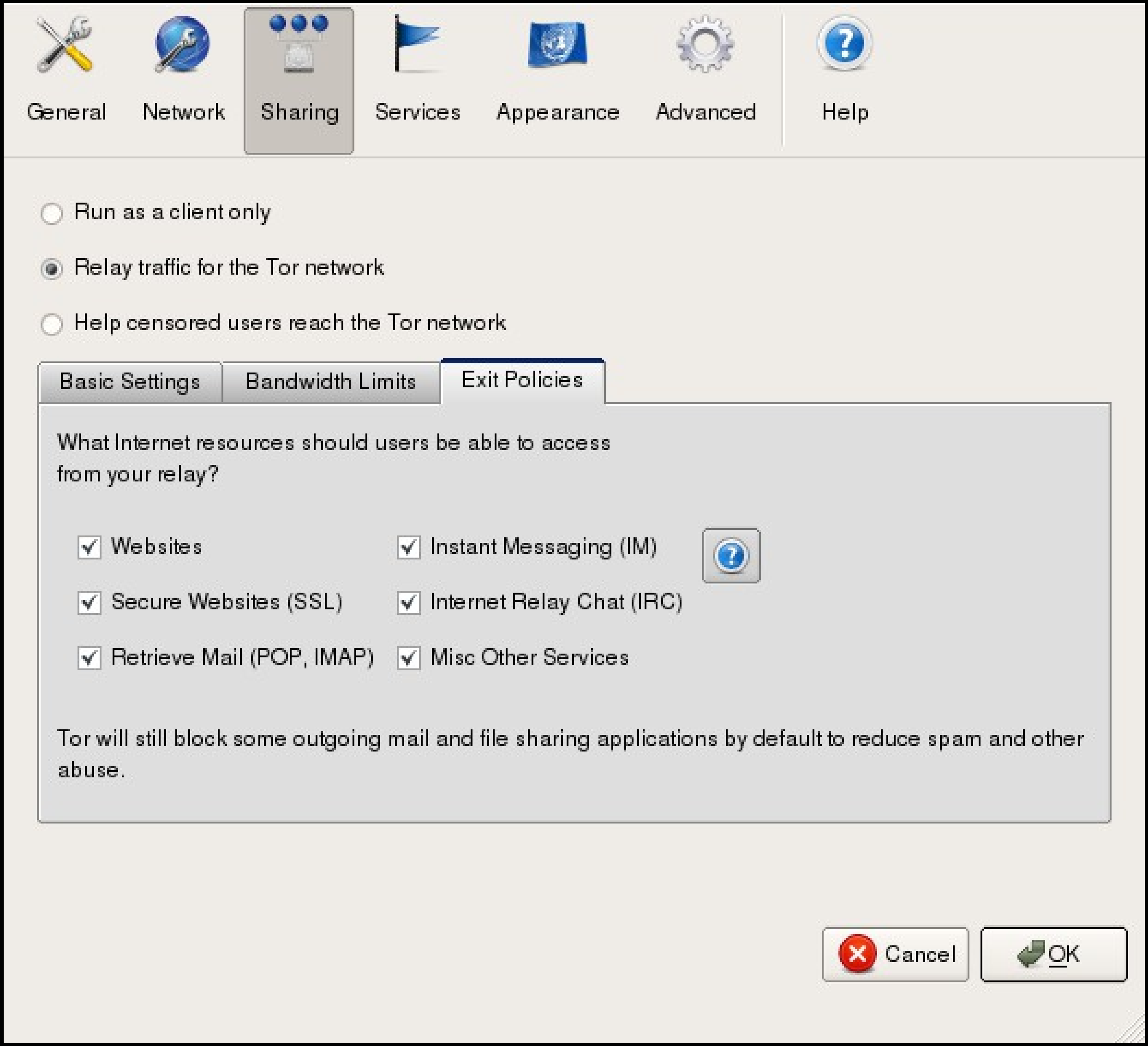
Tor Client

obfsproxy client

|CENSOR|

obfsproxy server

Tor Bridge



○ Run as a client only

● Relay traffic for the Tor network

○ Help censored users reach the Tor network

What Internet resources should users be able to access from your relay?

☑ Websites

☑ Secure Websites (SSL)

☑ Retrieve Mail (POP, IMAP)

☑ Instant Messaging (IM)

☑ Internet Relay Chat (IRC)

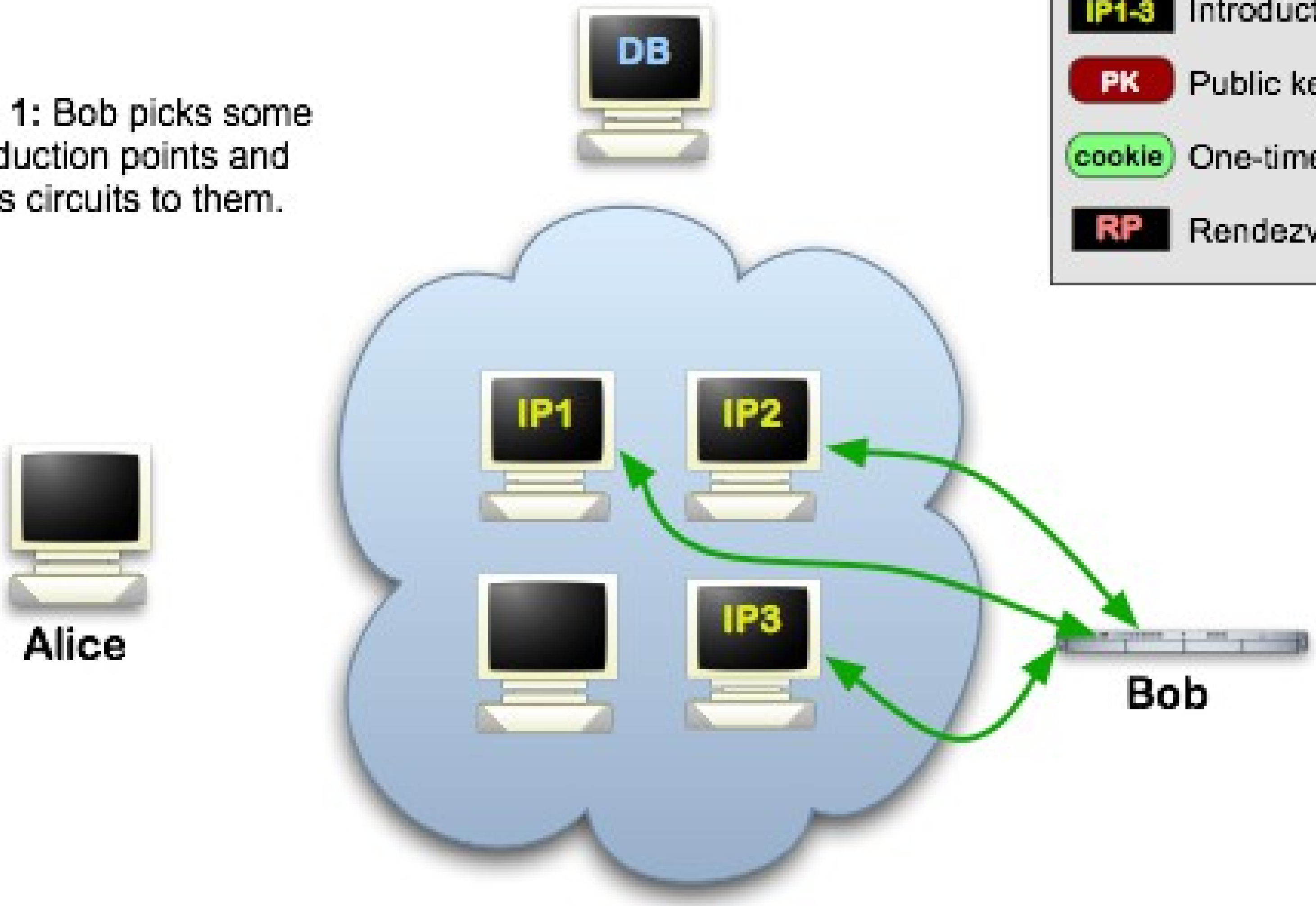
☑ Misc Other Services

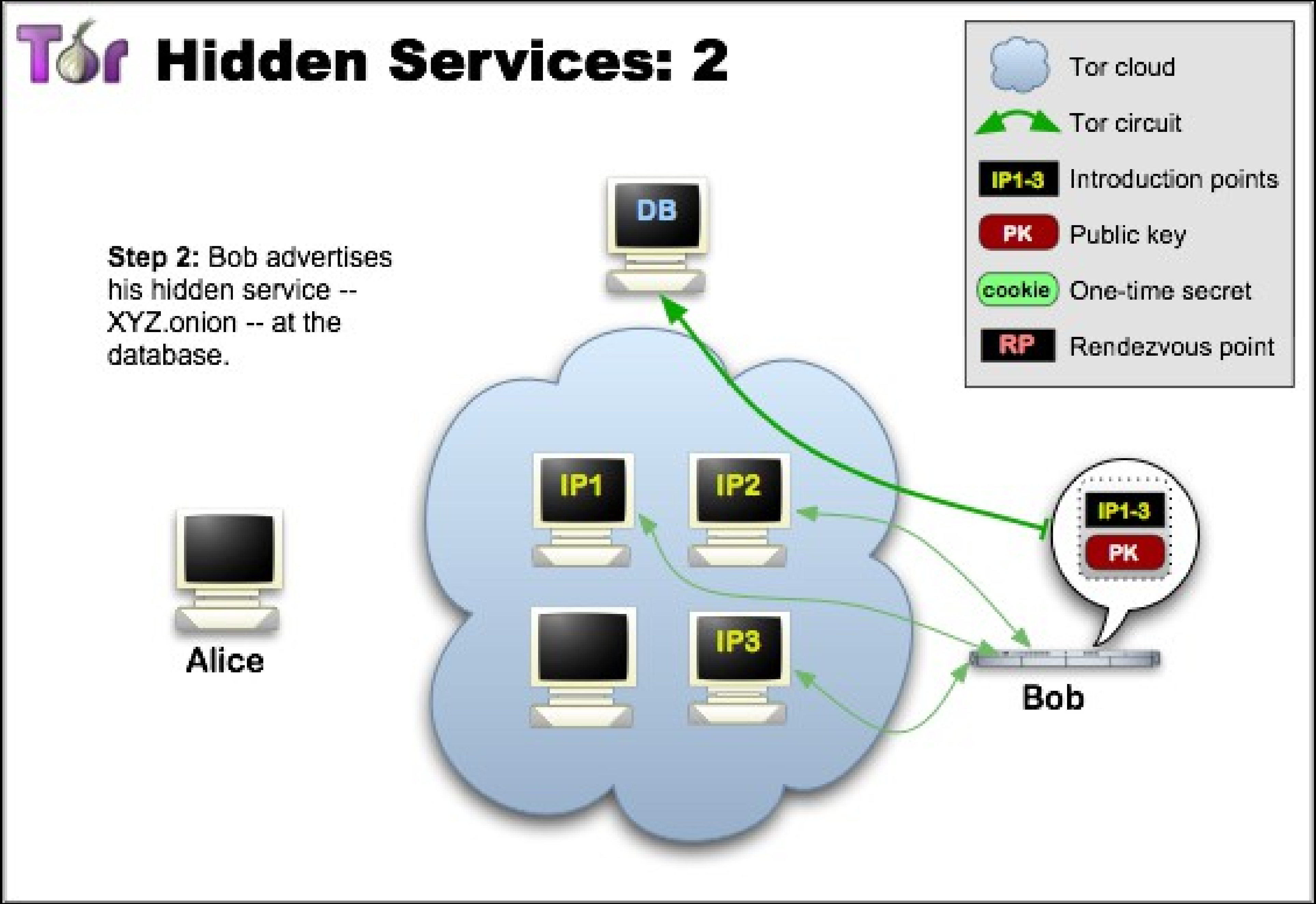
Tor will still block some outgoing mail and file sharing applications by default to reduce spam and other abuse.

Tor Hidden Services: 1

- Tor cloud
- Tor circuit
- IP1-3 Introduction points
- PK Public key
- cookie One-time secret
- RP Rendezvous point

Step 1: Bob picks some introduction points and builds circuits to them.





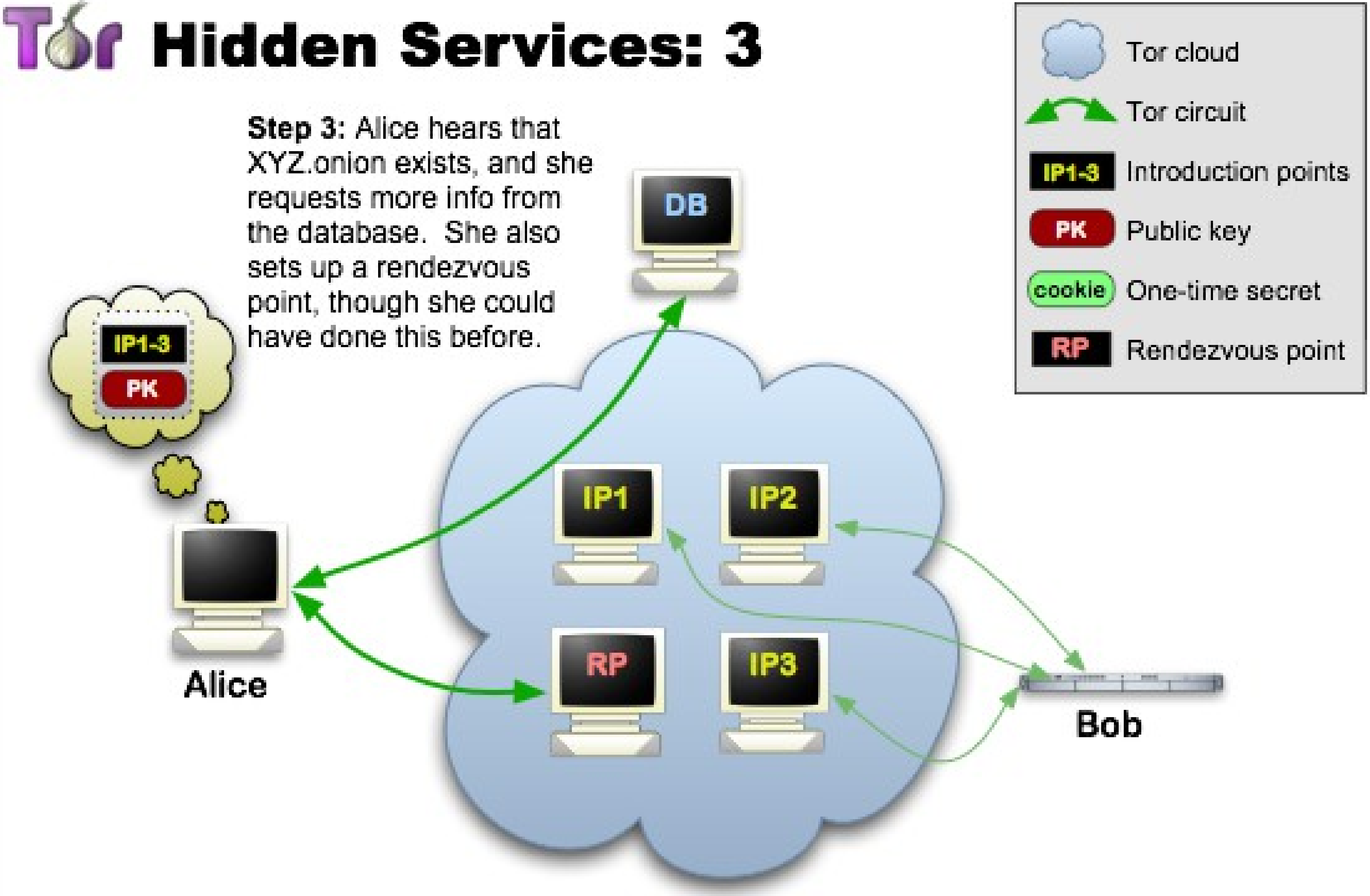
Tor Hidden Services: 2

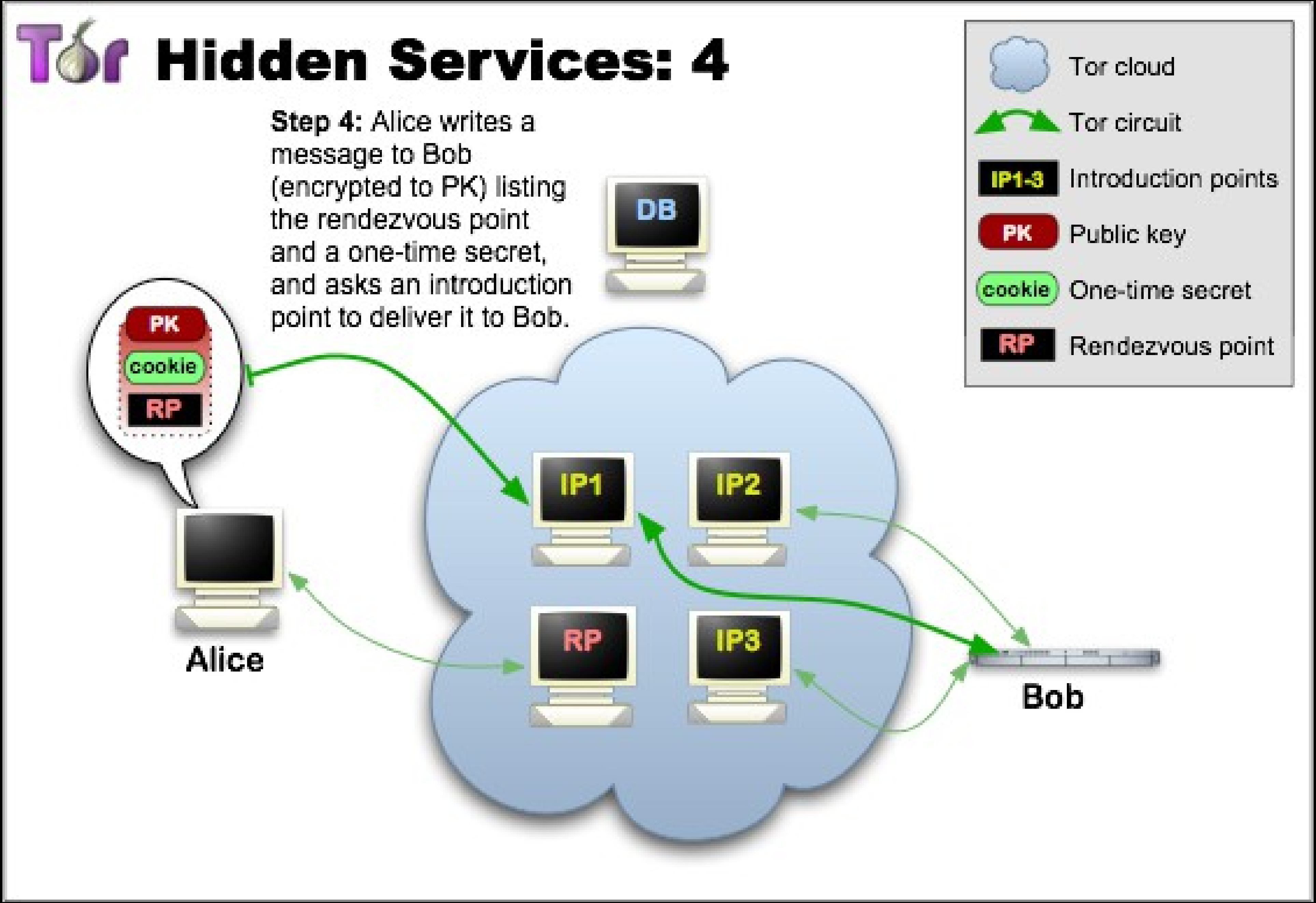
Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.

	Tor cloud
	Tor circuit
IP1-3	Introduction points
PK	Public key
cookie	One-time secret
RP	Rendezvous point

Tor Hidden Services: 3

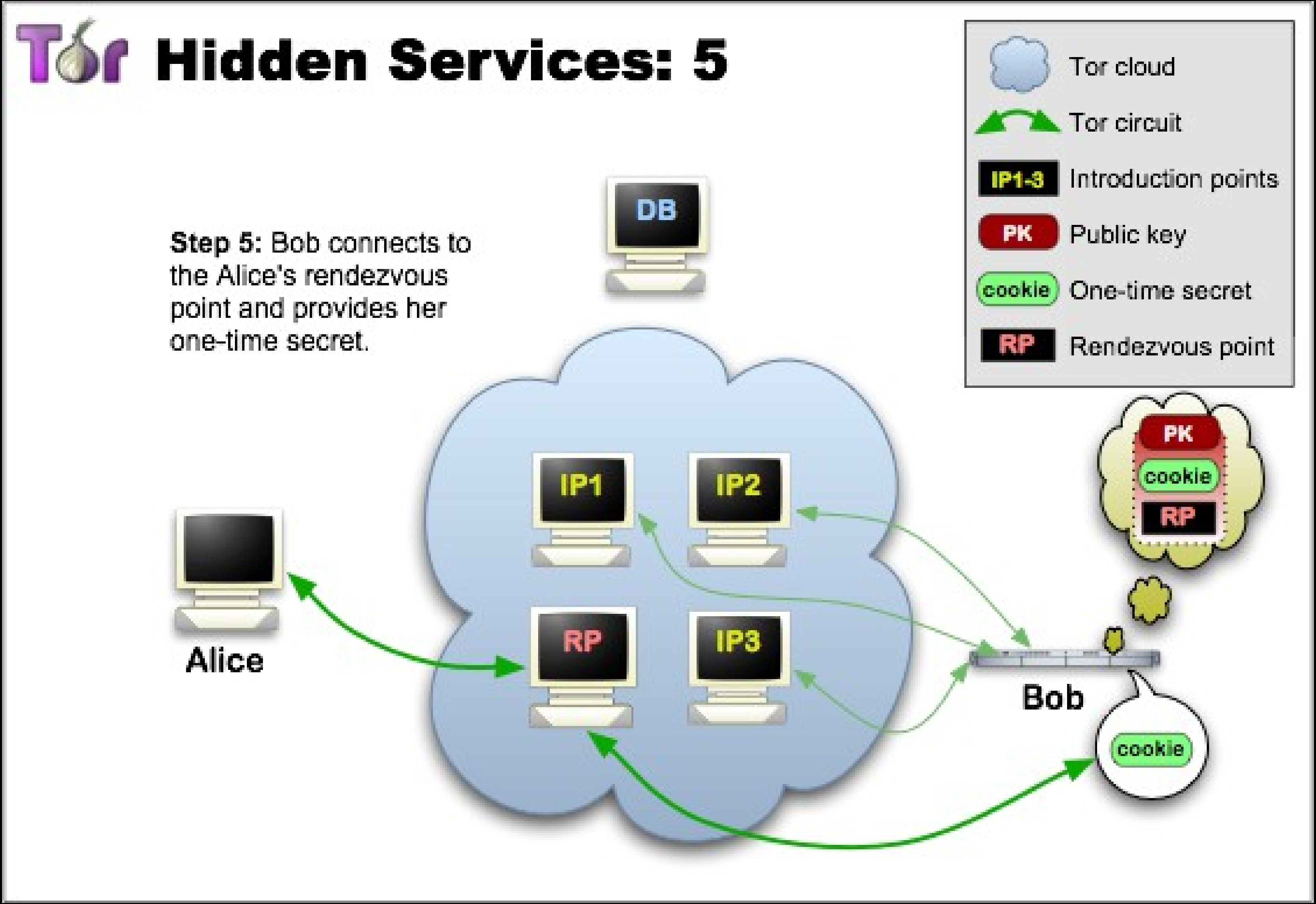
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.





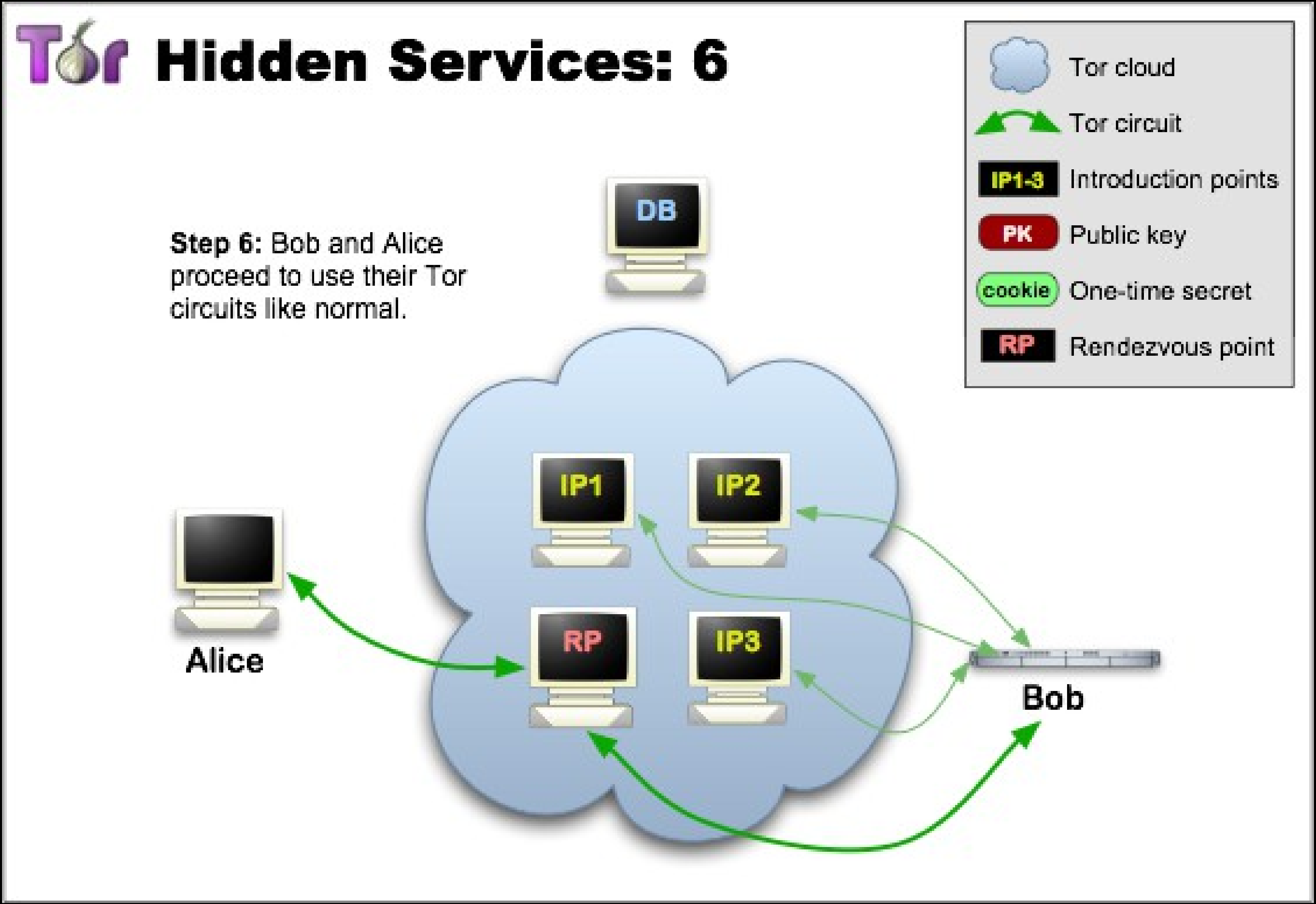
Hidden Services: 4

Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.



Tor Hidden Services: 5

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



Tor Hidden Services: 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.

Tor is 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
- Assume the users can fetch a genuine copy of Tor: from a friend, via PGP signatures, etc.

Advocacy and education

- Unending stream of people (e.g. in DC) who make critical policy decisions without much technical background
- Worse, there's a high churn rate
- Need to teach policy-makers, business leaders, law enforcement, journalists, ...
- Data retention? Internet driver's license?

I CAN HAZ
FREEDOM?
Tor
TorProject.org

Lessons?

- 1) Bad people don't need Tor. They're doing fine.
- 2) Honest people need more security/privacy/anonymity.
- 3) Law enforcement benefits from it too.
- 4) Tor is not unbreakable.