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

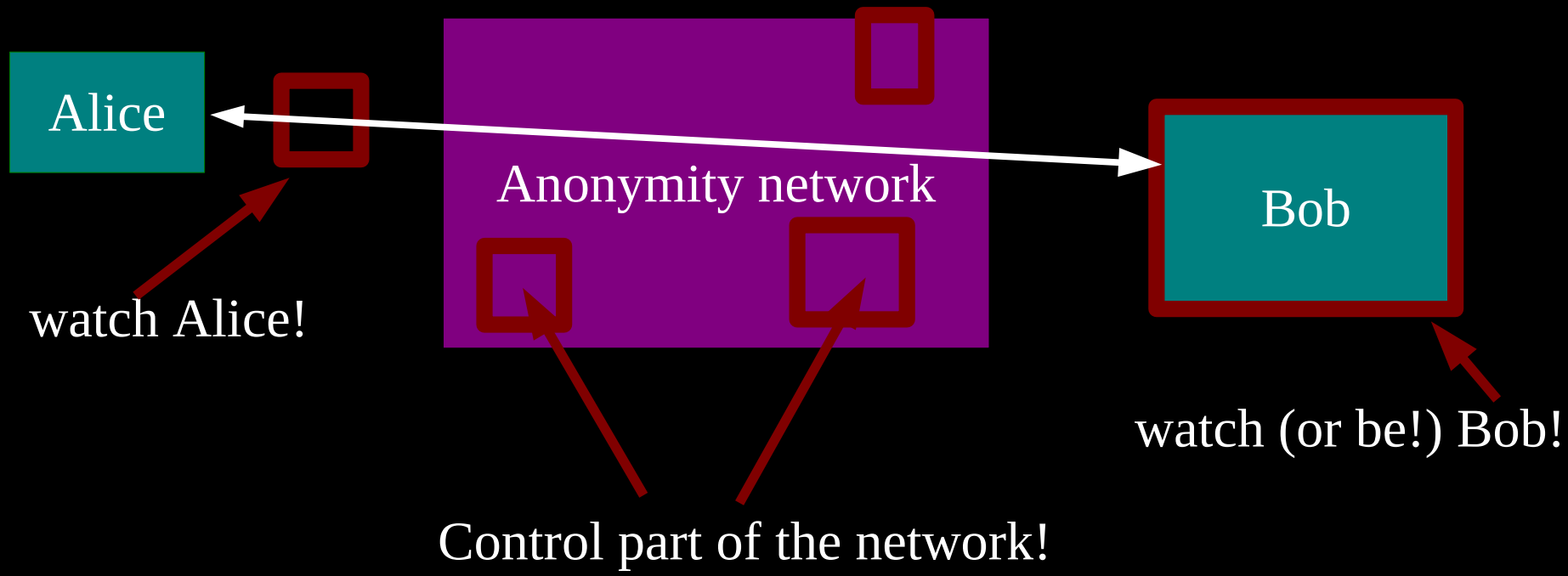
Funding from US DoD, Electronic Frontier Foundation, Voice of America, Google, NLnet, Human Rights Watch, NSF, US State Dept, SIDA, Knight Foundation, ...

The Tor Project, Inc.

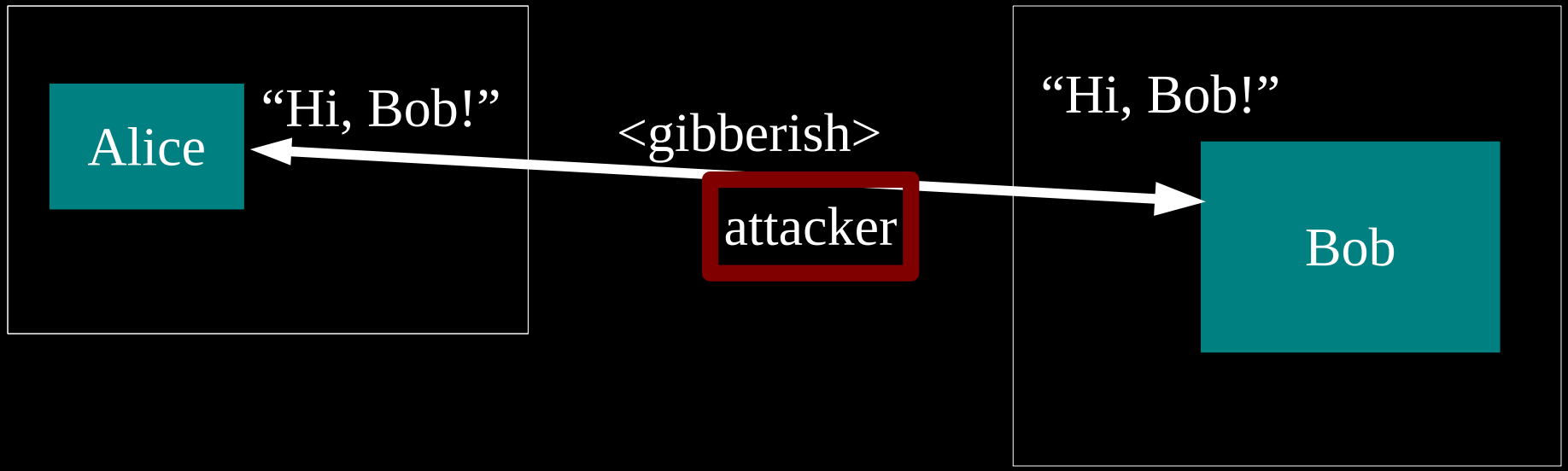
501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy


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!”

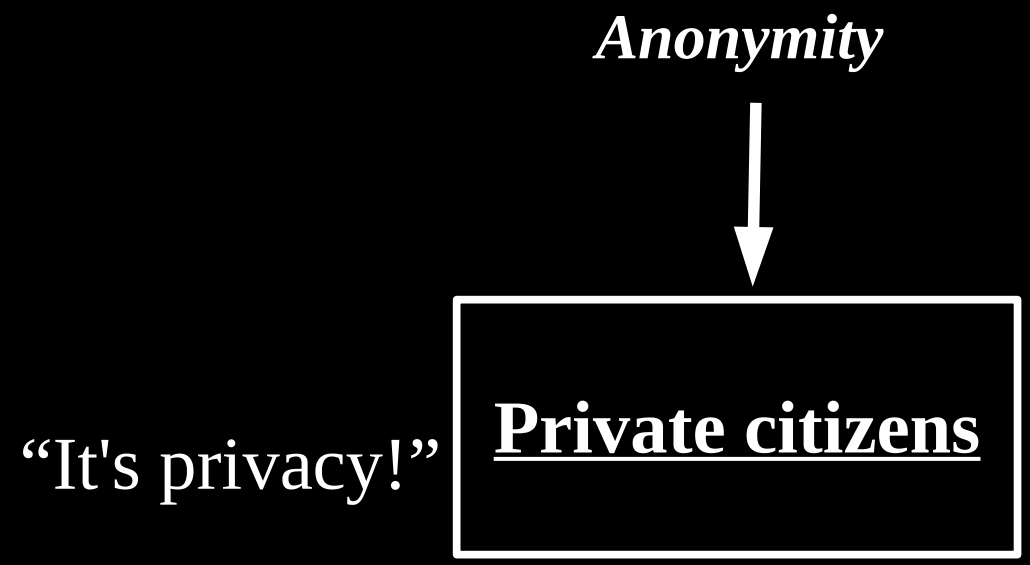
“Promise you won't remember!”

“Promise you won't tell!”

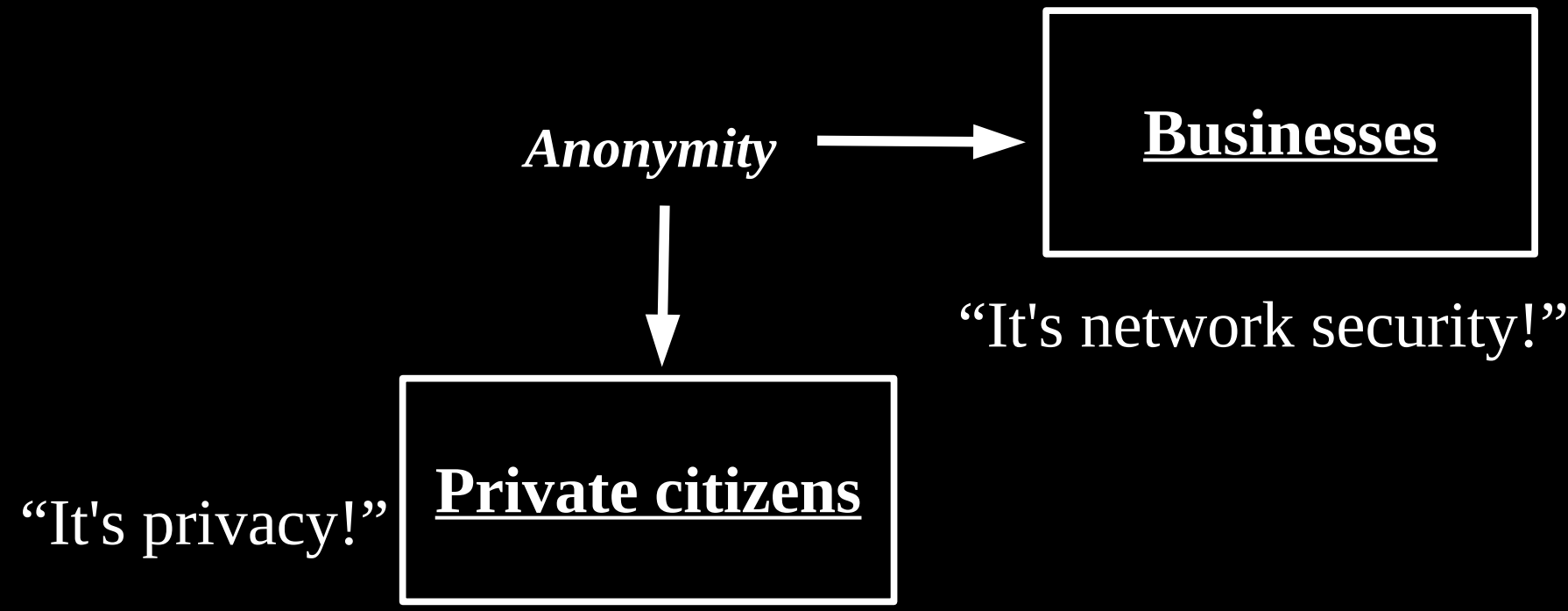
“I didn't write my name on it!”

“Isn't the Internet already anonymous?”

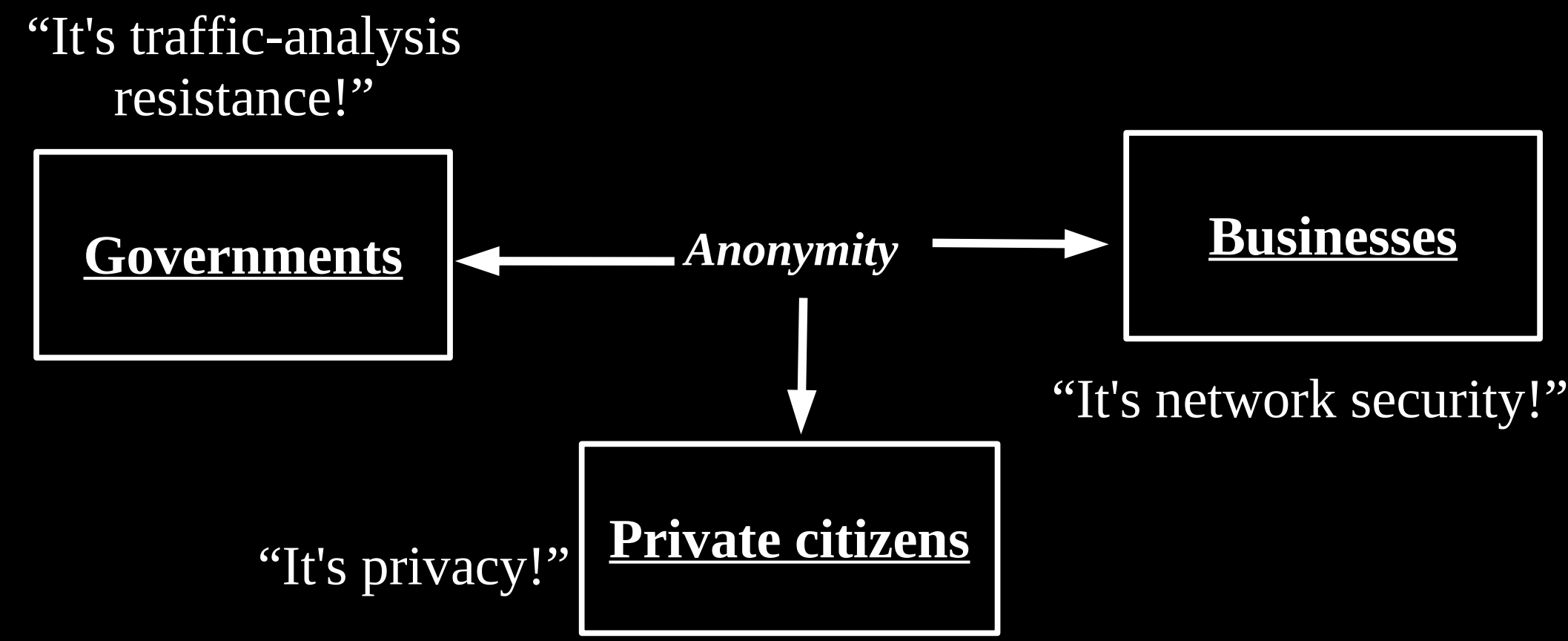
Anonymity serves different interests for different user groups.



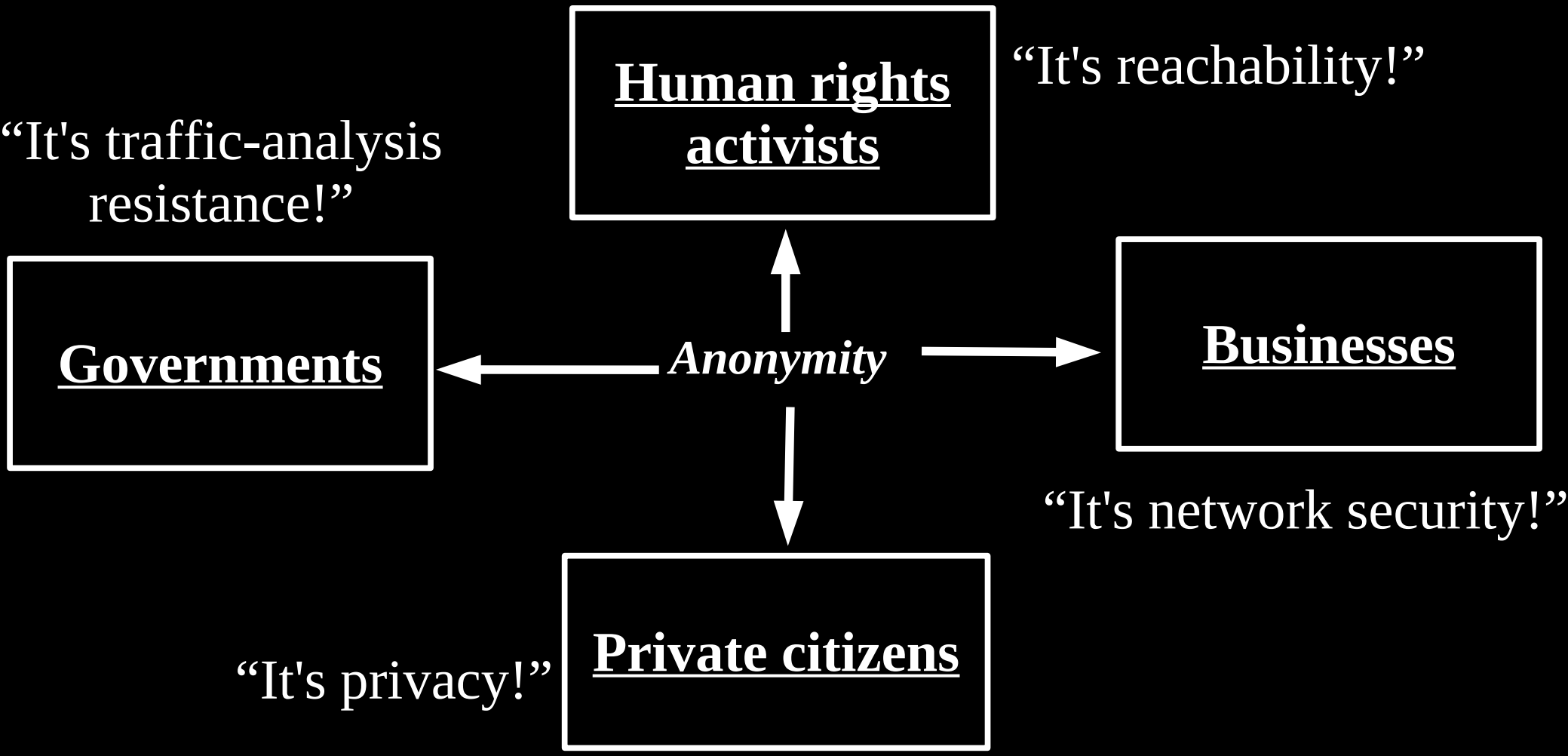
Anonymity serves different interests for different user groups.



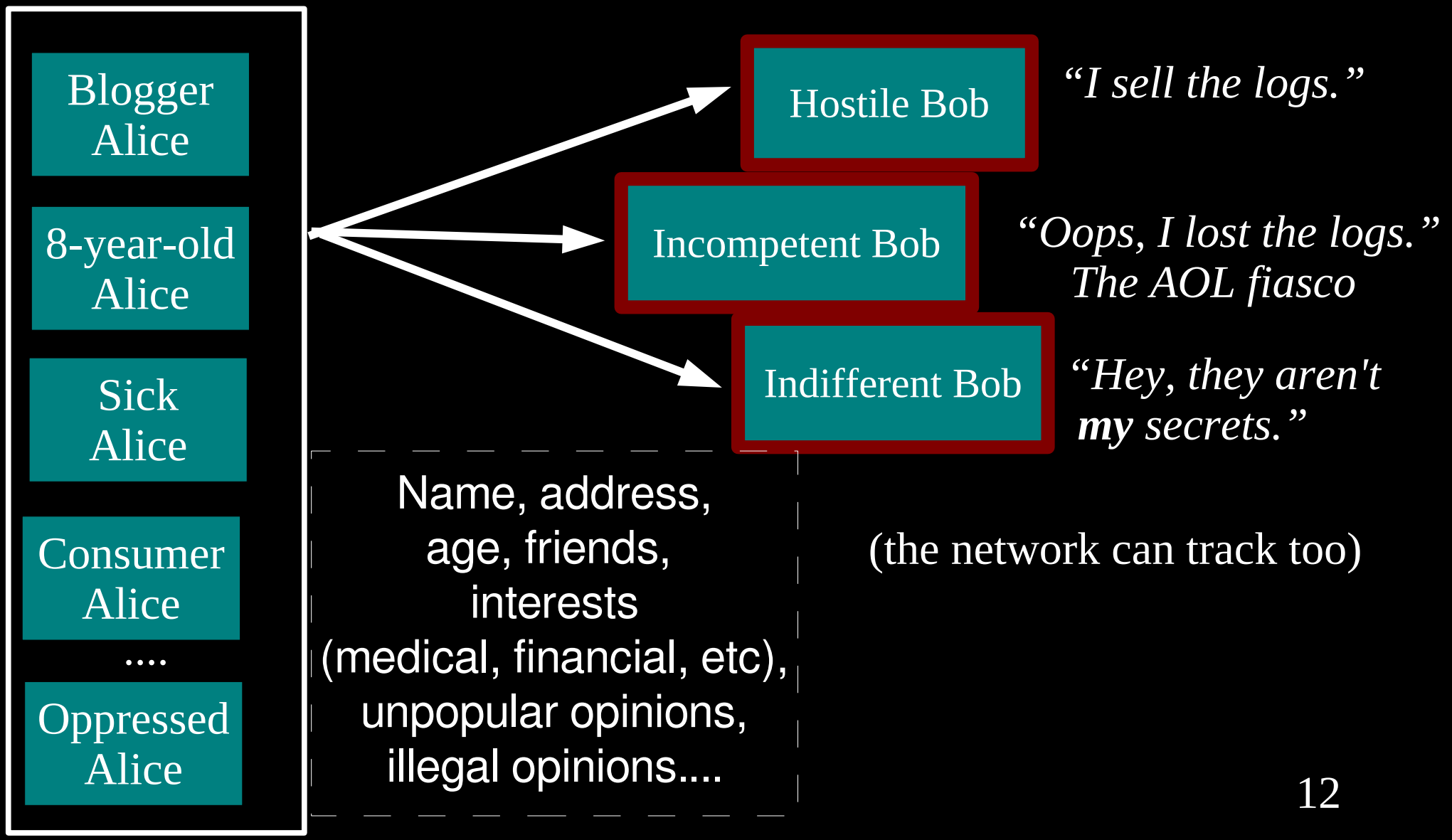
Anonymity serves different interests for different user groups.



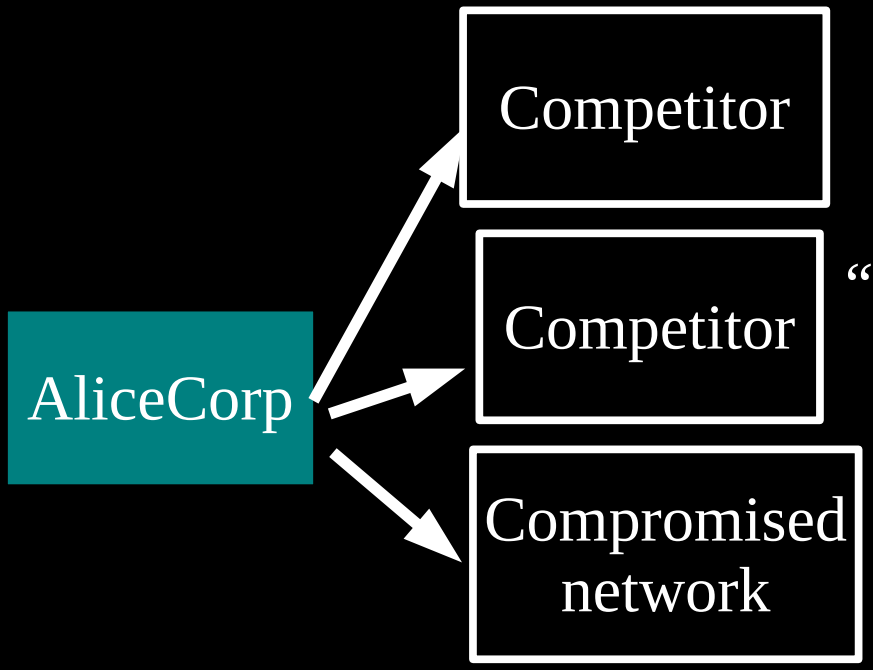
Anonymity serves different interests for different user groups.



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



Businesses need to keep trade secrets.



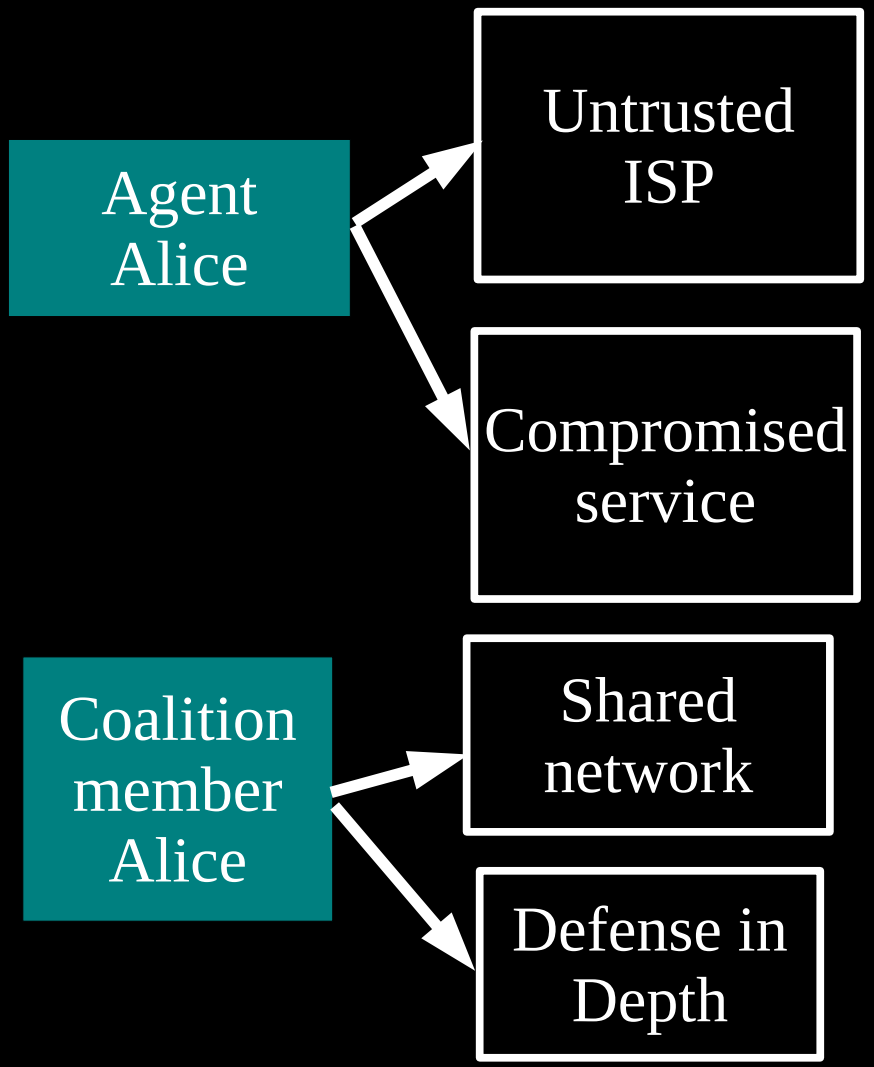
“Oh, your employees are reading our patents/jobs page/product sheets?”

“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.

Governments need anonymity for their security



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

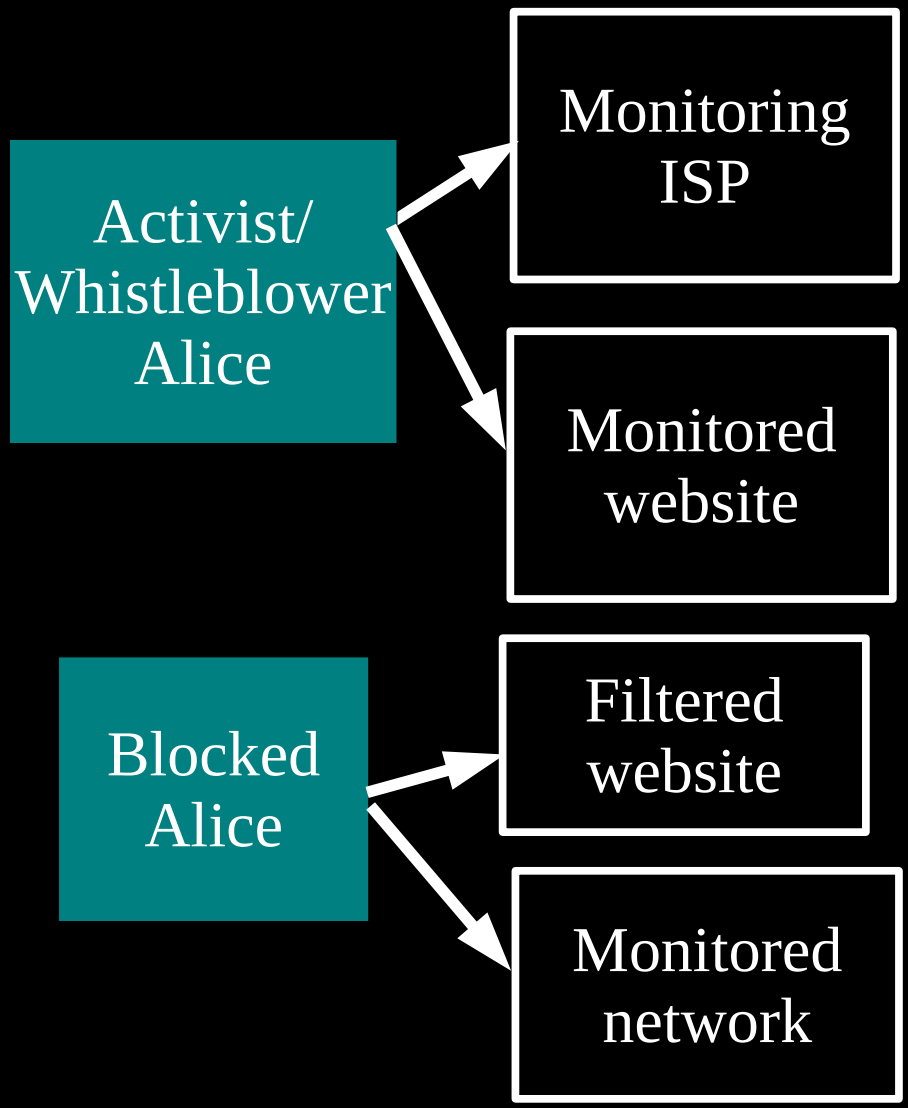
"Somebody in that hotel room just checked his Navy.mil mail!"

"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



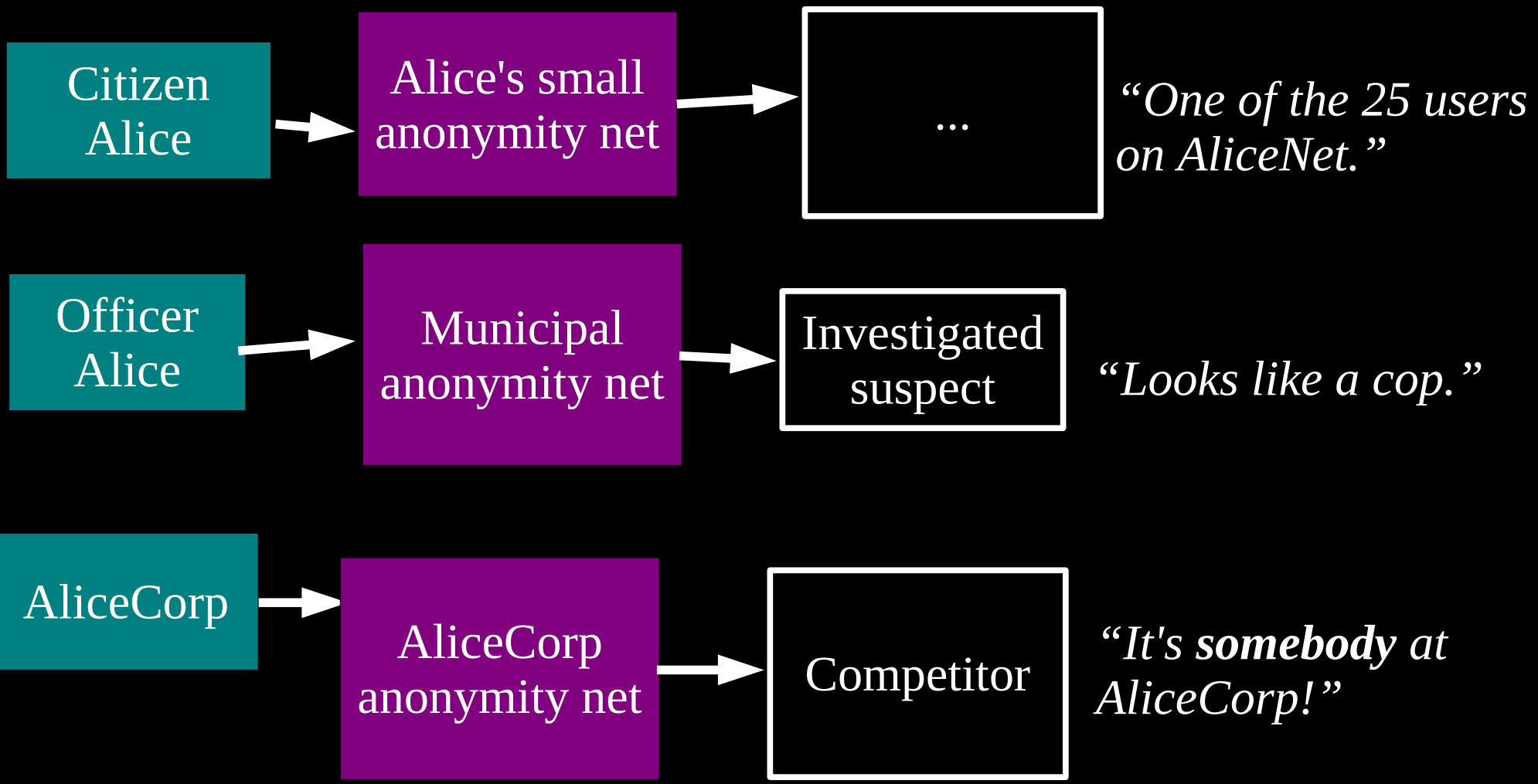
"Did you just post to that website?"

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

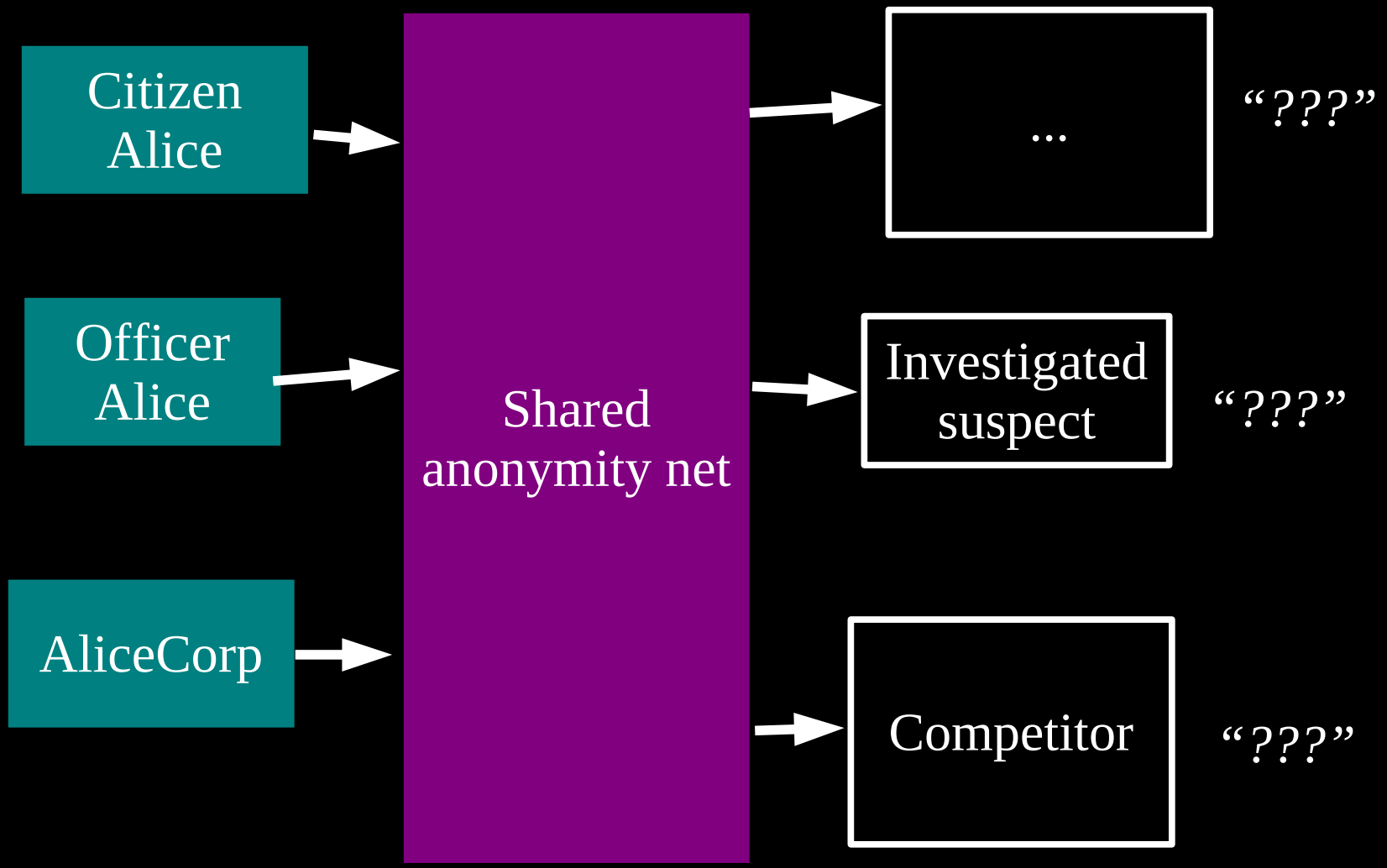
"What does the Global Voices website say today?"
"I want to tell people what's going on in my country"

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

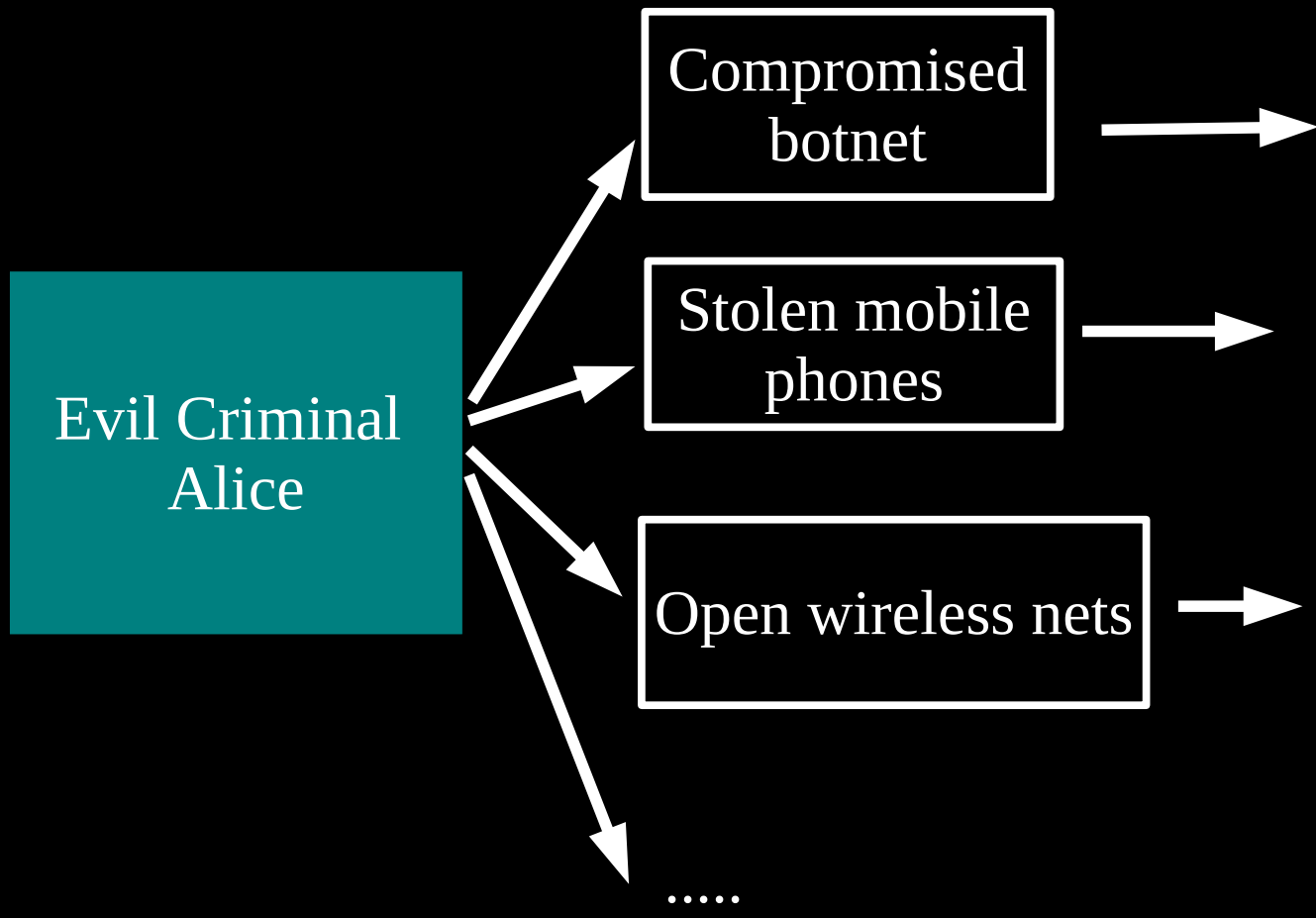
You can't get anonymity on your own: private solutions are ineffective...



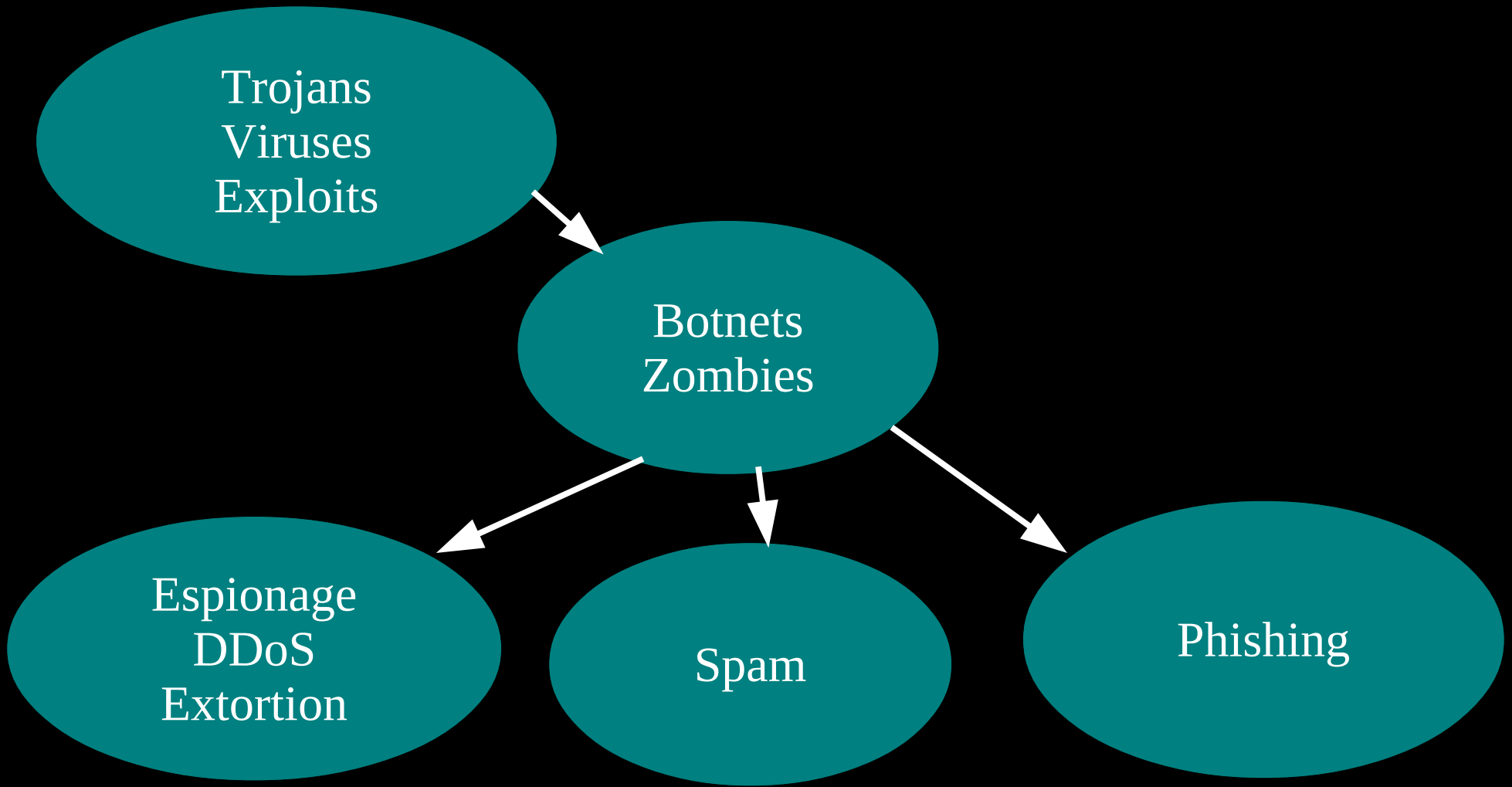
... so, anonymity loves company!



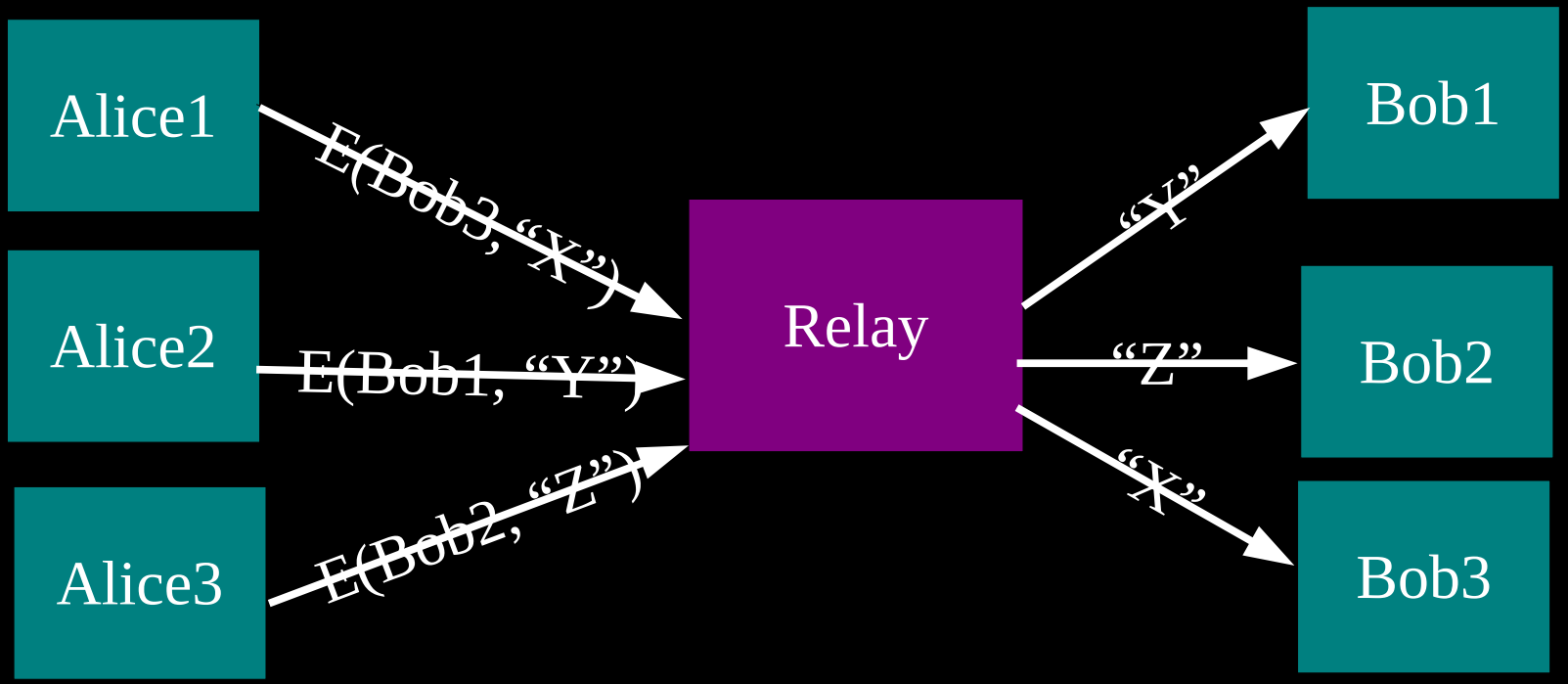
Yes, bad people need anonymity too. But they are *already* doing well.



Current situation: Bad people on the Internet are doing fine

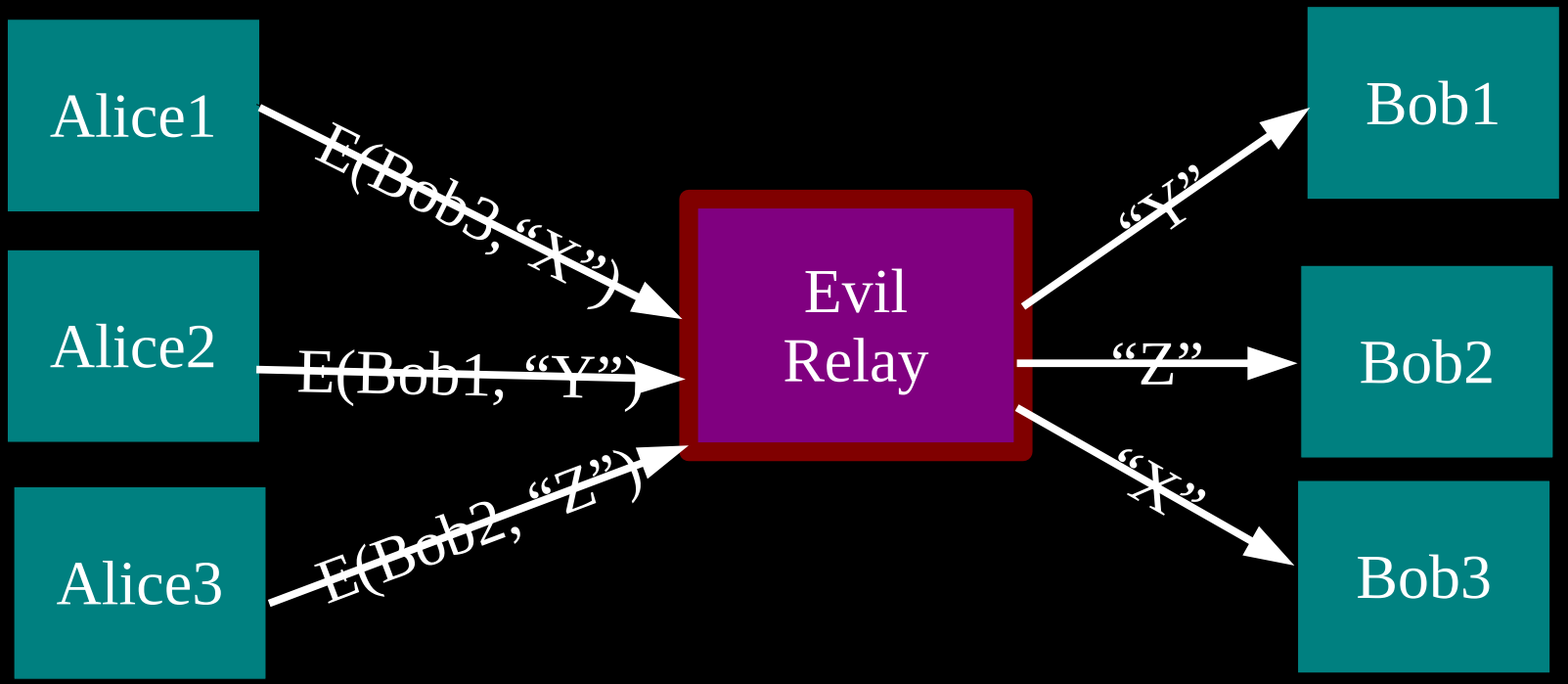


The simplest designs use a single relay to hide connections.

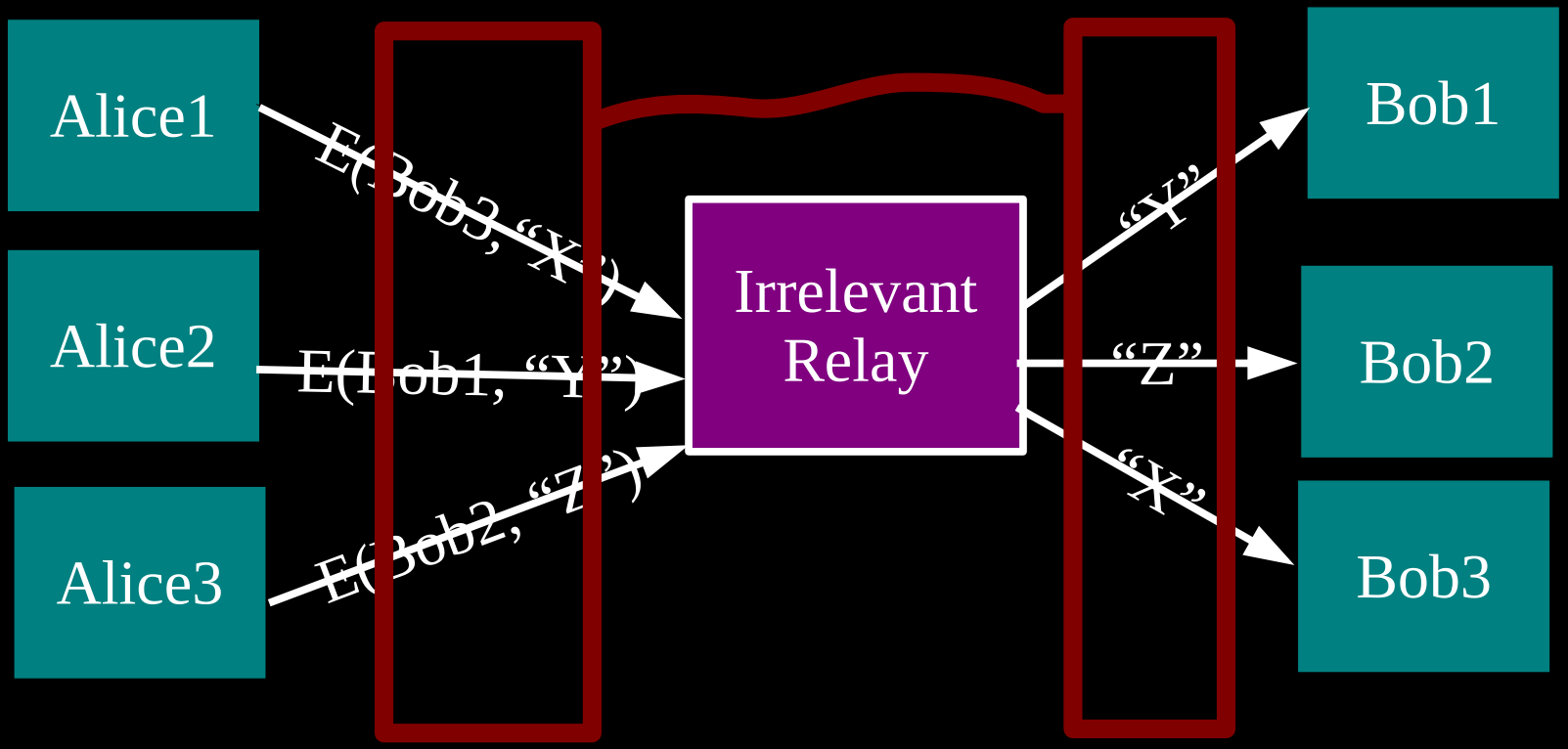


(example: some commercial proxy providers)

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

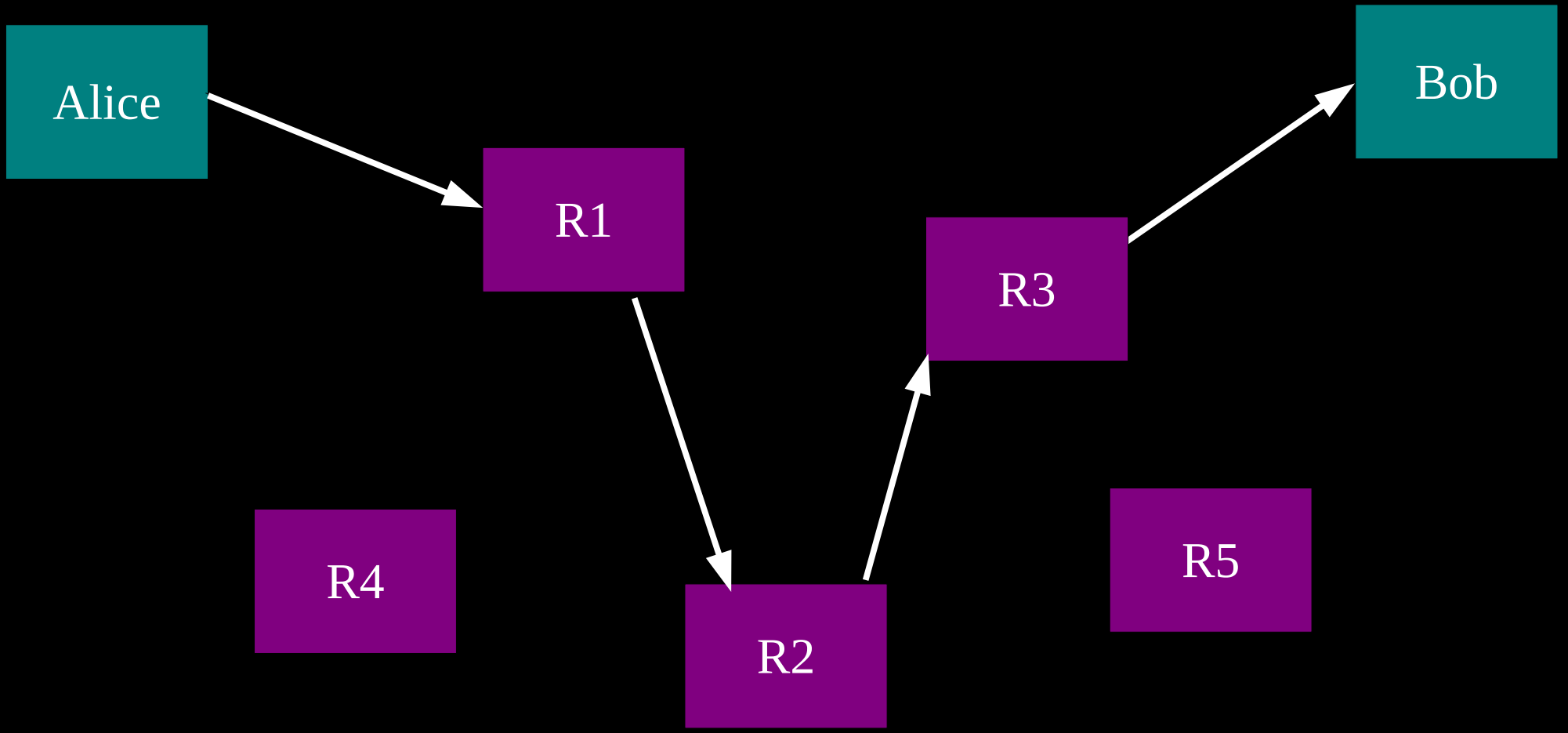


... or a single point of bypass.

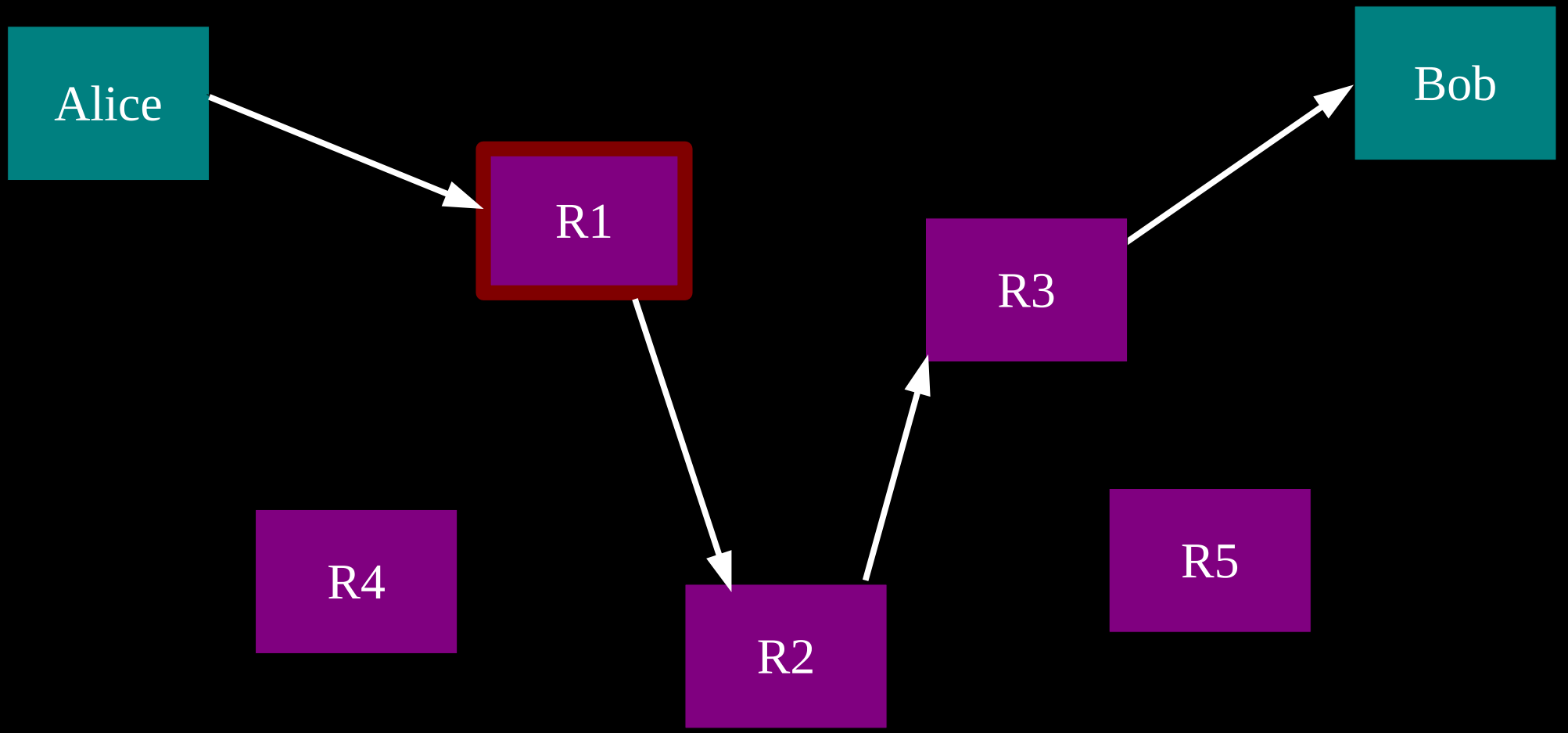


Timing analysis bridges all connections through relay ⇒ An attractive fat target

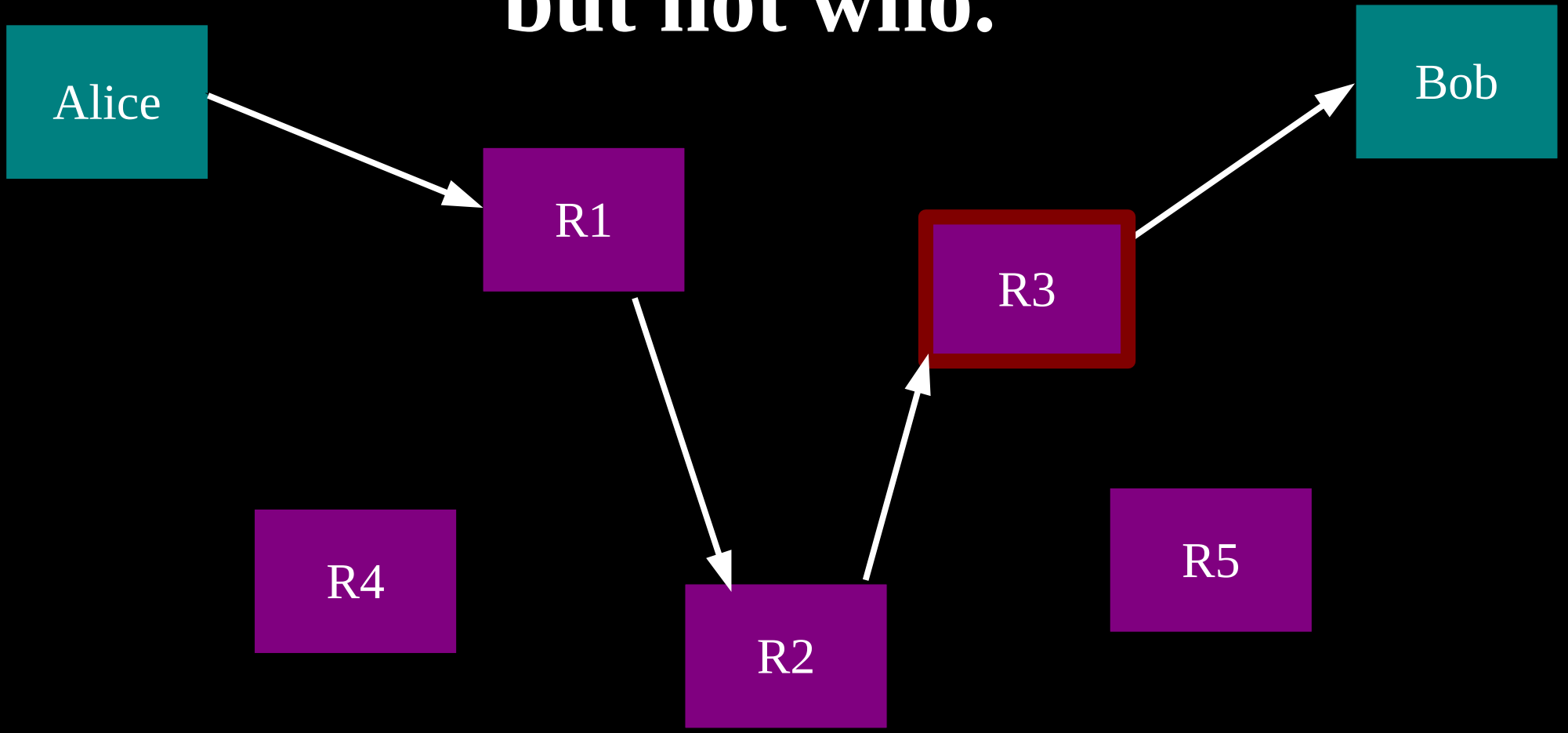
So, add multiple relays so that no single one can betray Alice.



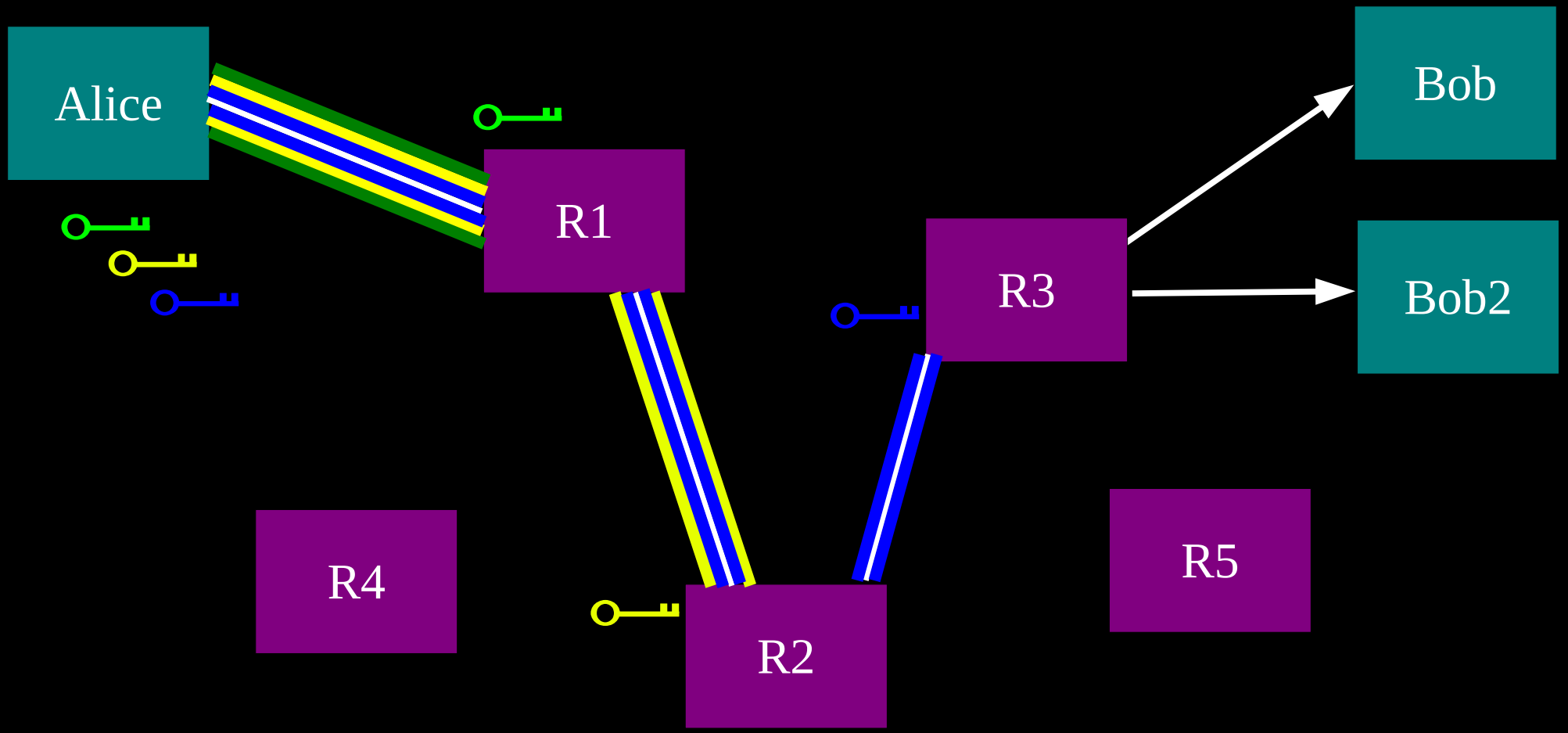
A corrupt first hop can tell that Alice is talking, but not to whom.

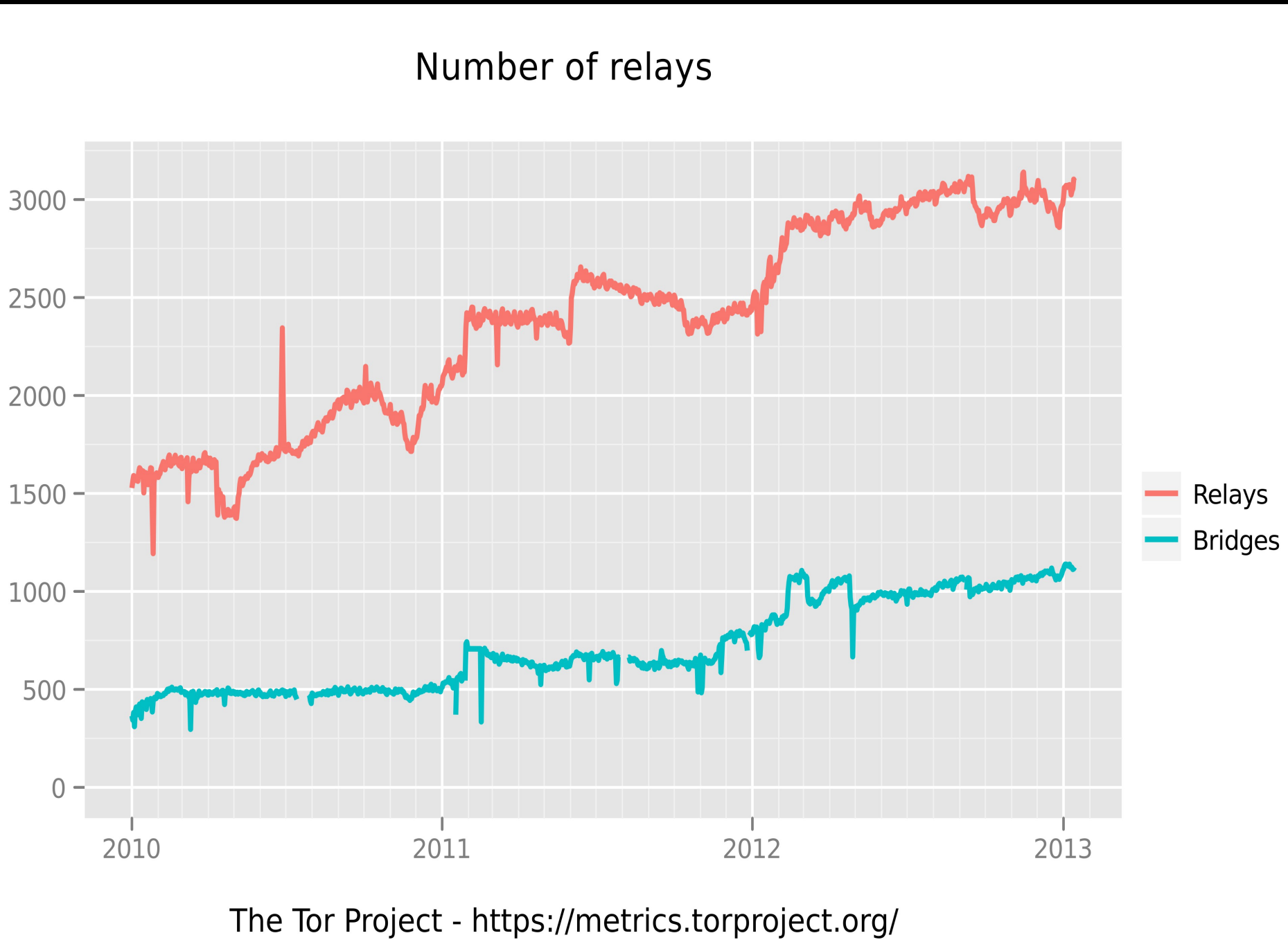


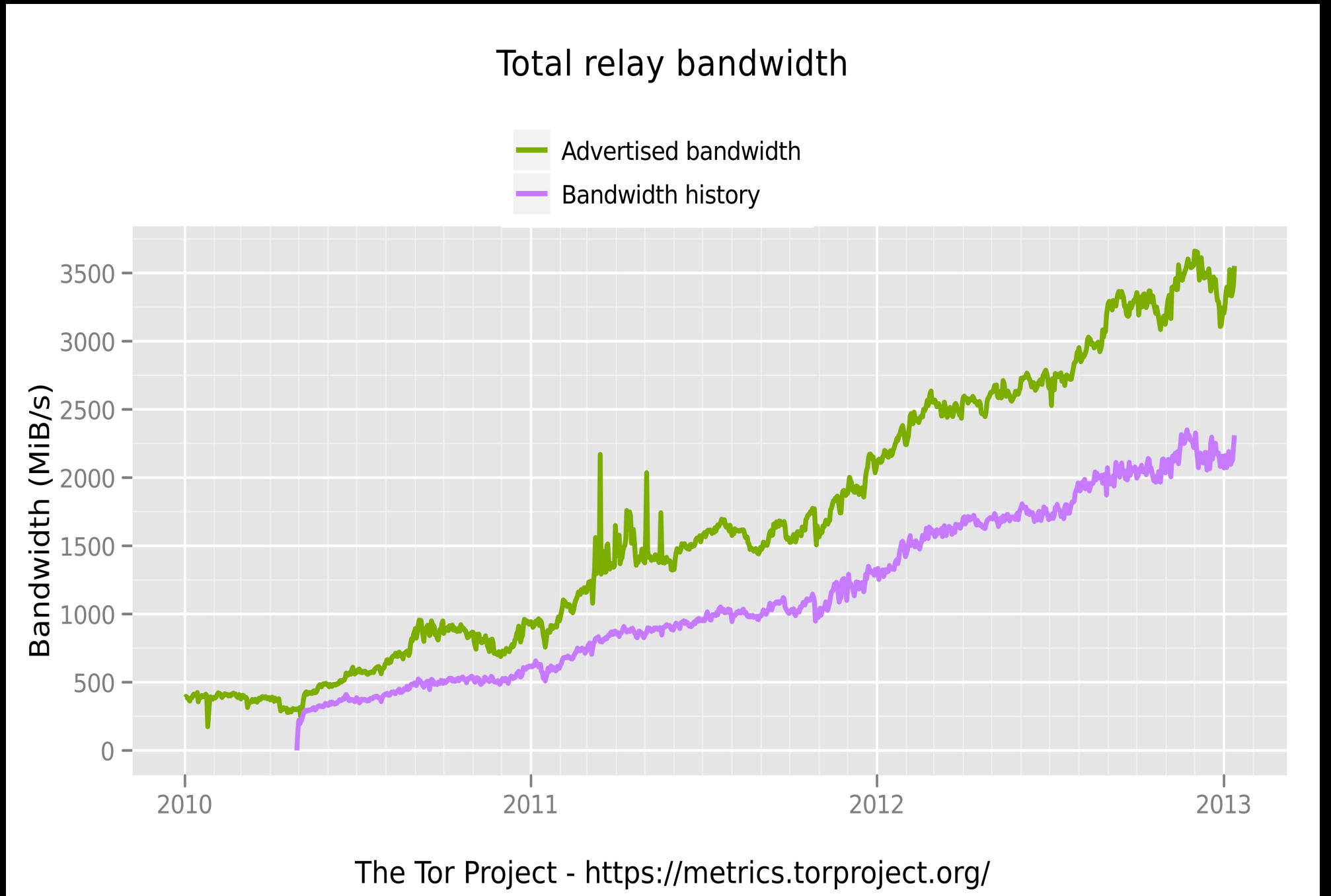
A corrupt final hop can tell that somebody is talking to Bob, but not who.

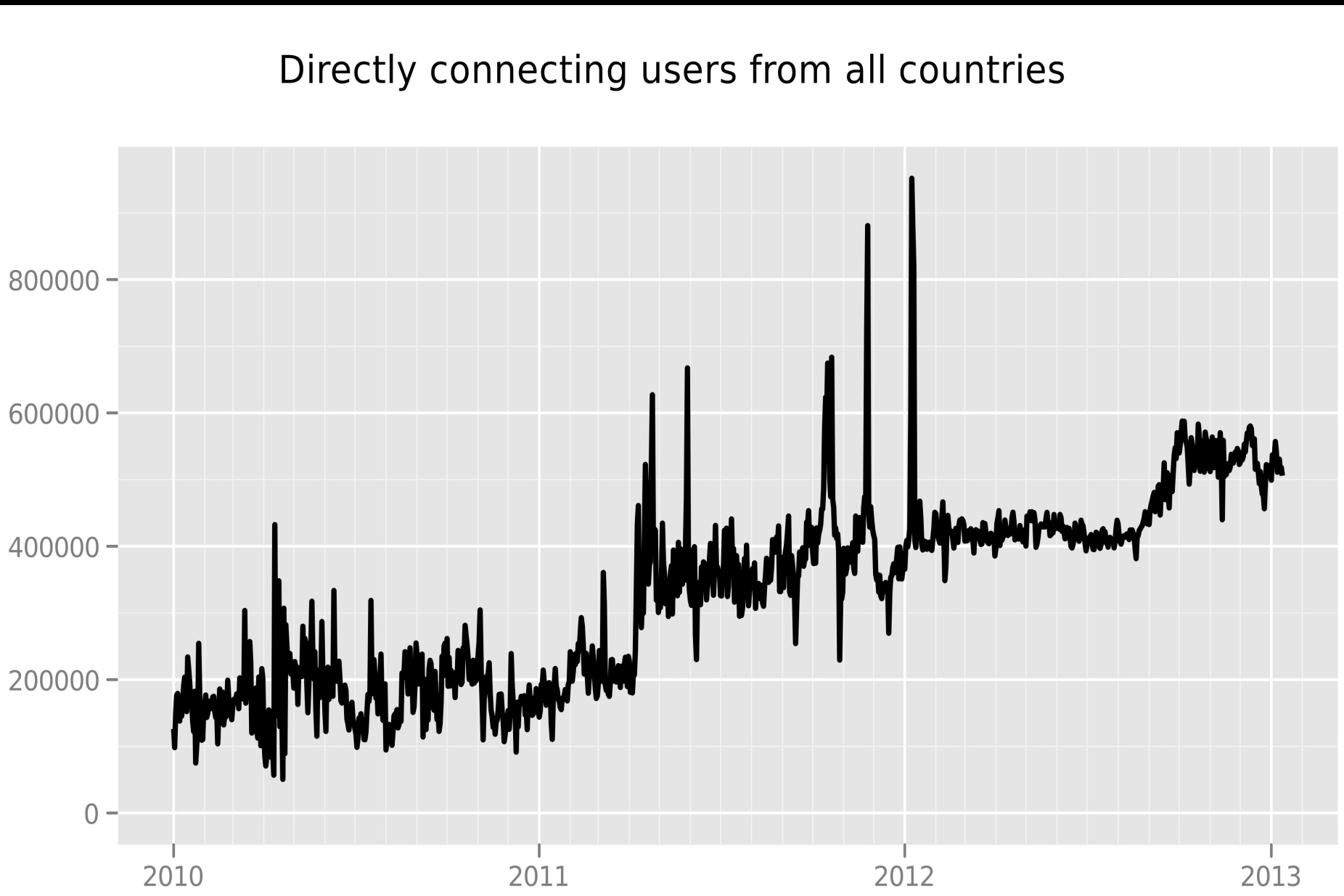


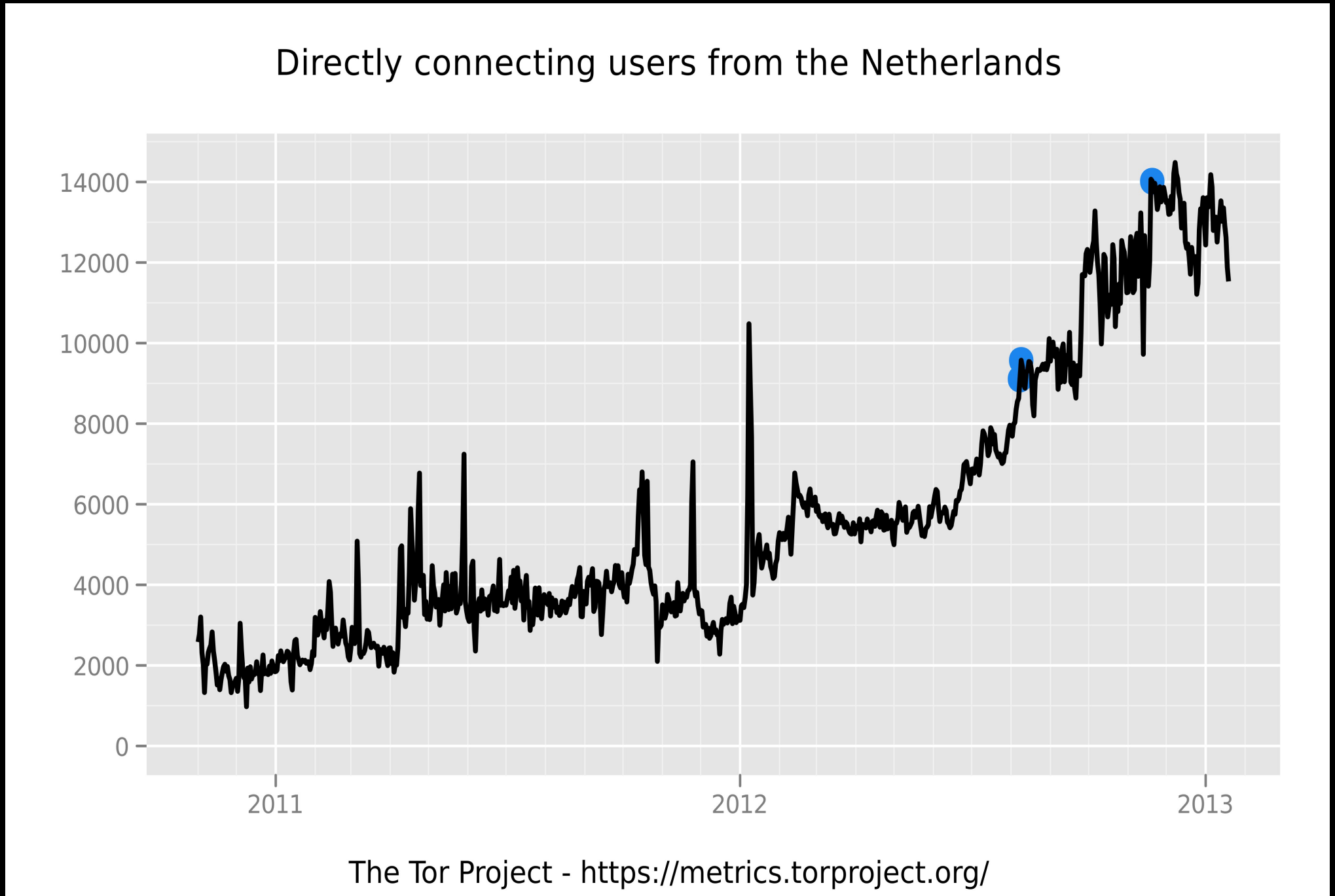
Alice makes a session key with R1 ...And then tunnels to R2...and to R3

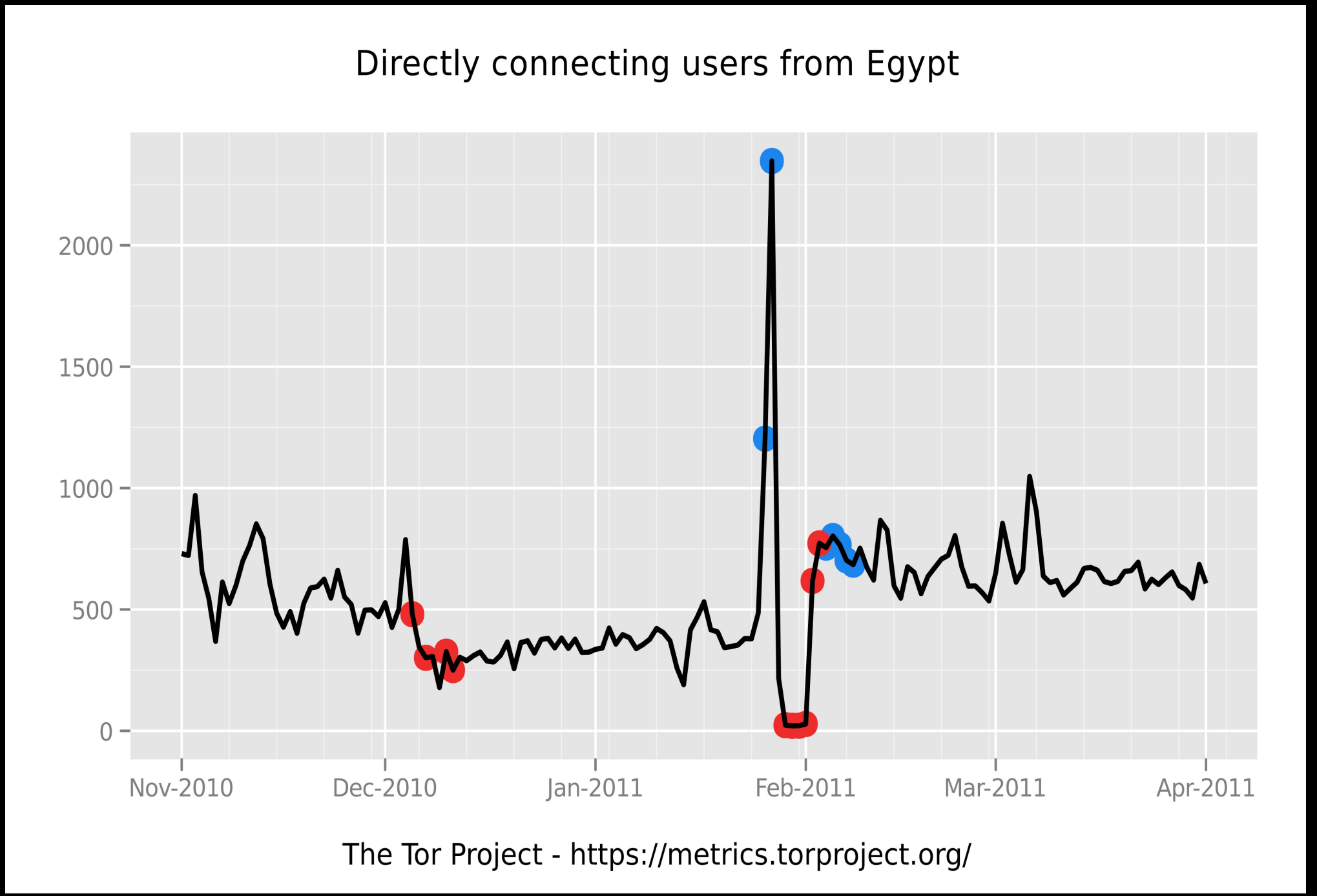


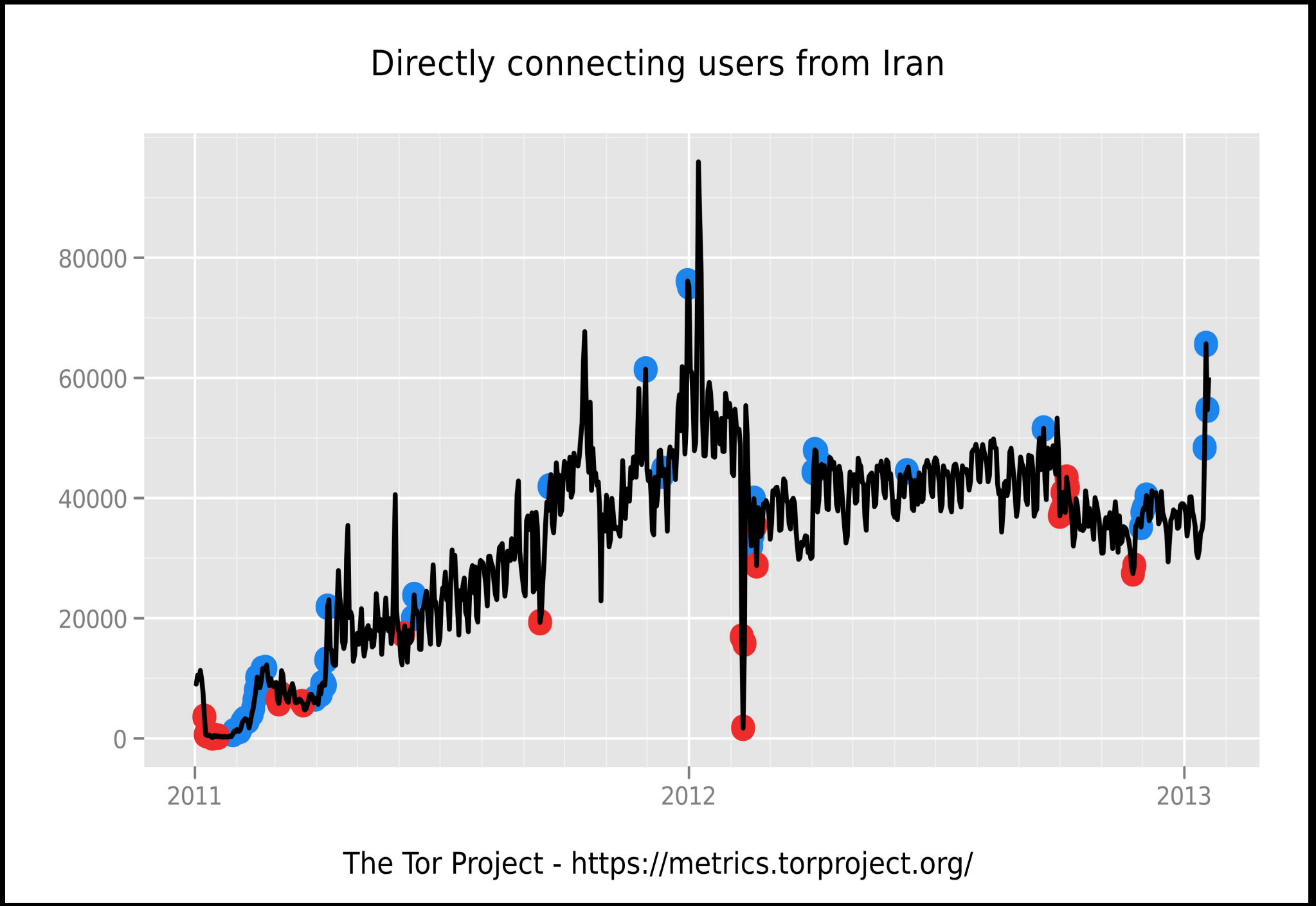

Number of relays
3000
2500
2000
1500
1000
500
0
2010
2011
2012
2013
Relays
Bridges
The Tor Project - https://metrics.torproject.org/

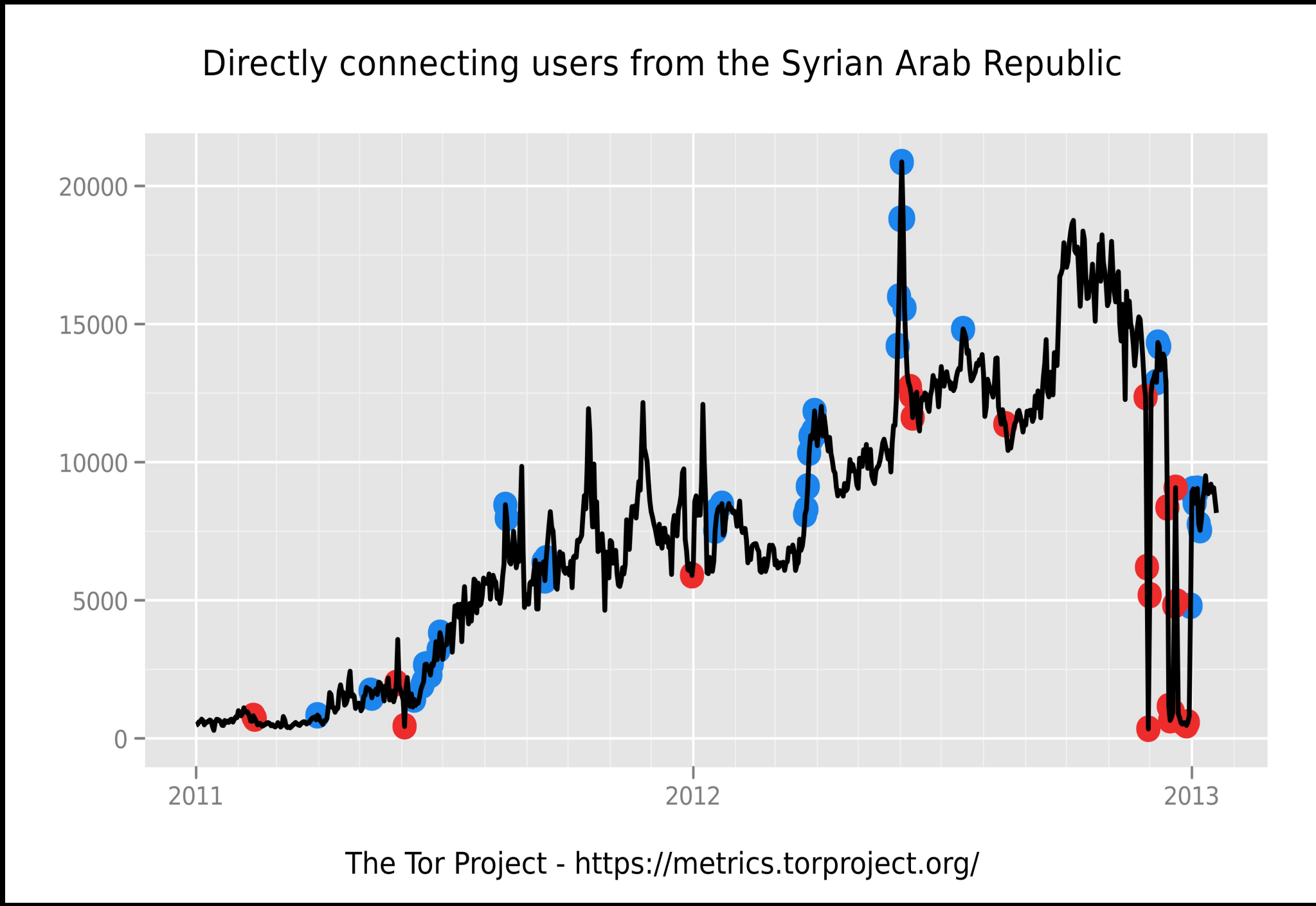

Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
3500
3000
2500
2000
1500
1000
500
0
2010
2011
2012
2013
The Tor Project - https://metrics.torproject.org/

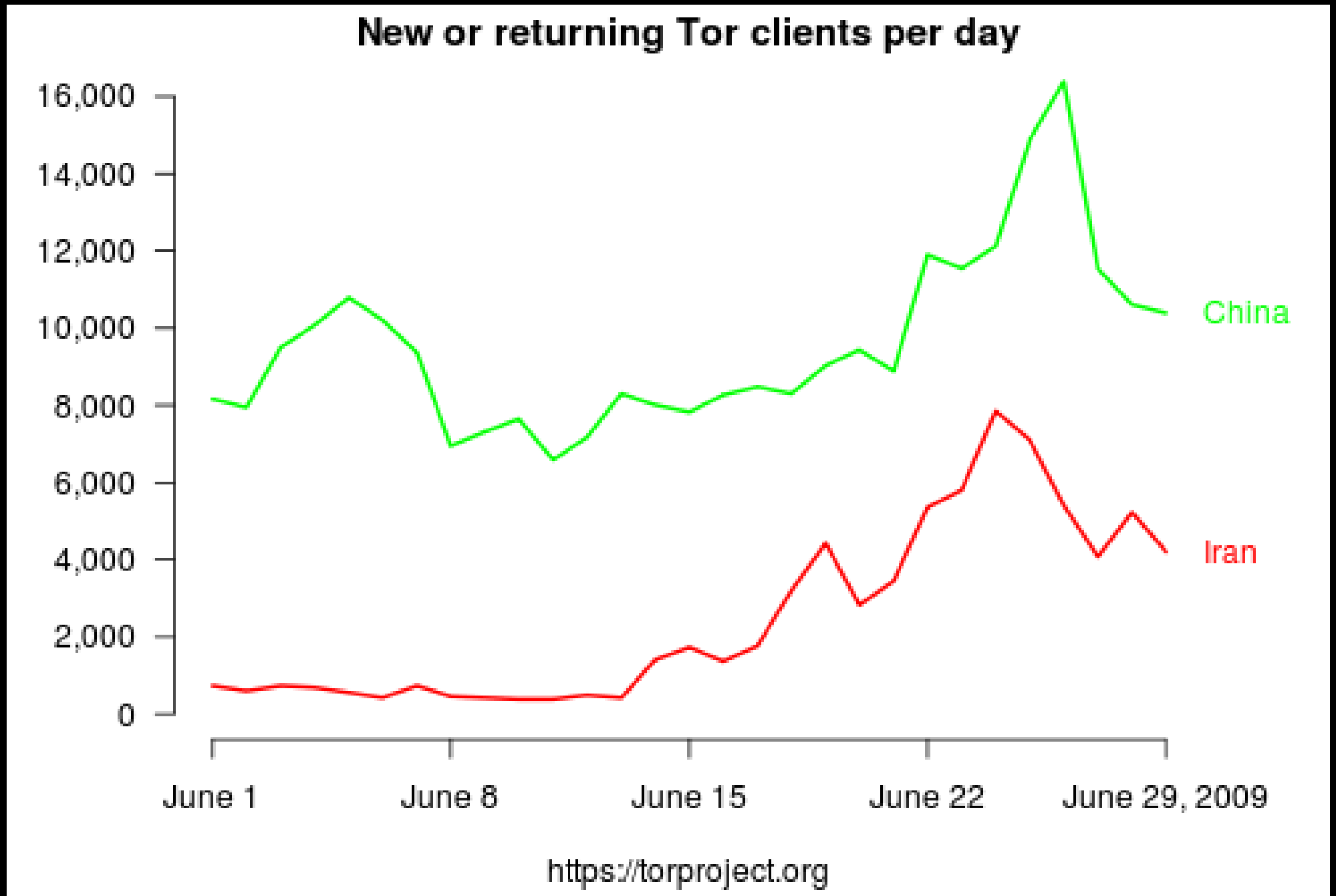

Directly connecting users from all countries
800000
600000
400000
200000
0
2010
2011
2012
2013
The Tor Project - https://metrics.torproject.org/


Directly connecting users from the Netherlands
14000
12000
10000
8000
6000
4000
2000
0
2011
2012
2013
The Tor Project - https://metrics.torproject.org/


Directly connecting users from Egypt
2000
1500
1000
500
0
Nov-2010
Dec-2010
Jan-2011
Feb-2011
Mar-2011
Apr-2011
The Tor Project - https://metrics.torproject.org/


Directly connecting users from Iran
80000
60000
40000
20000
0
2011
2012
2013
The Tor Project - https://metrics.torproject.org/


Directly connecting users from the Syrian Arab Republic
20000
15000
10000
5000
0
2011
2012
2013
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.

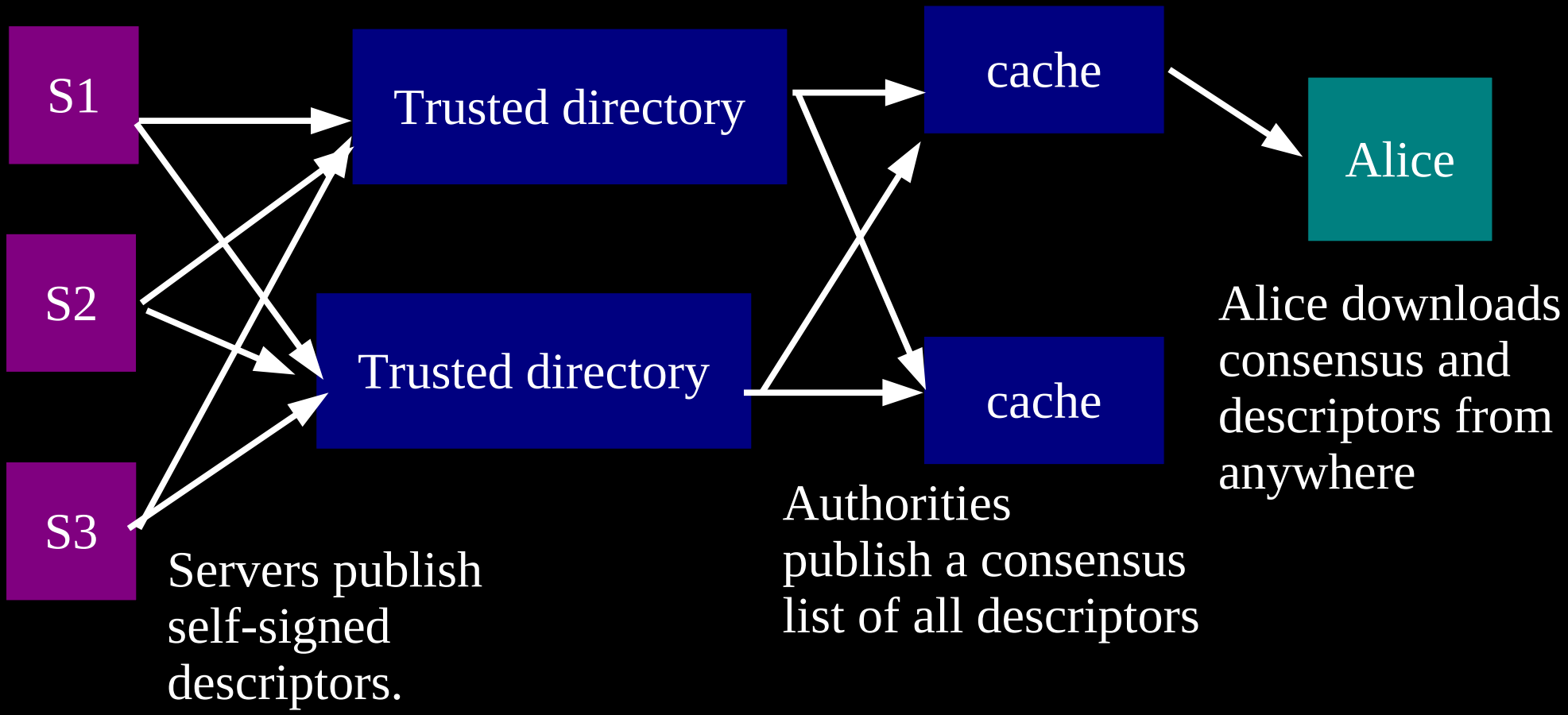
Relay versus Discovery

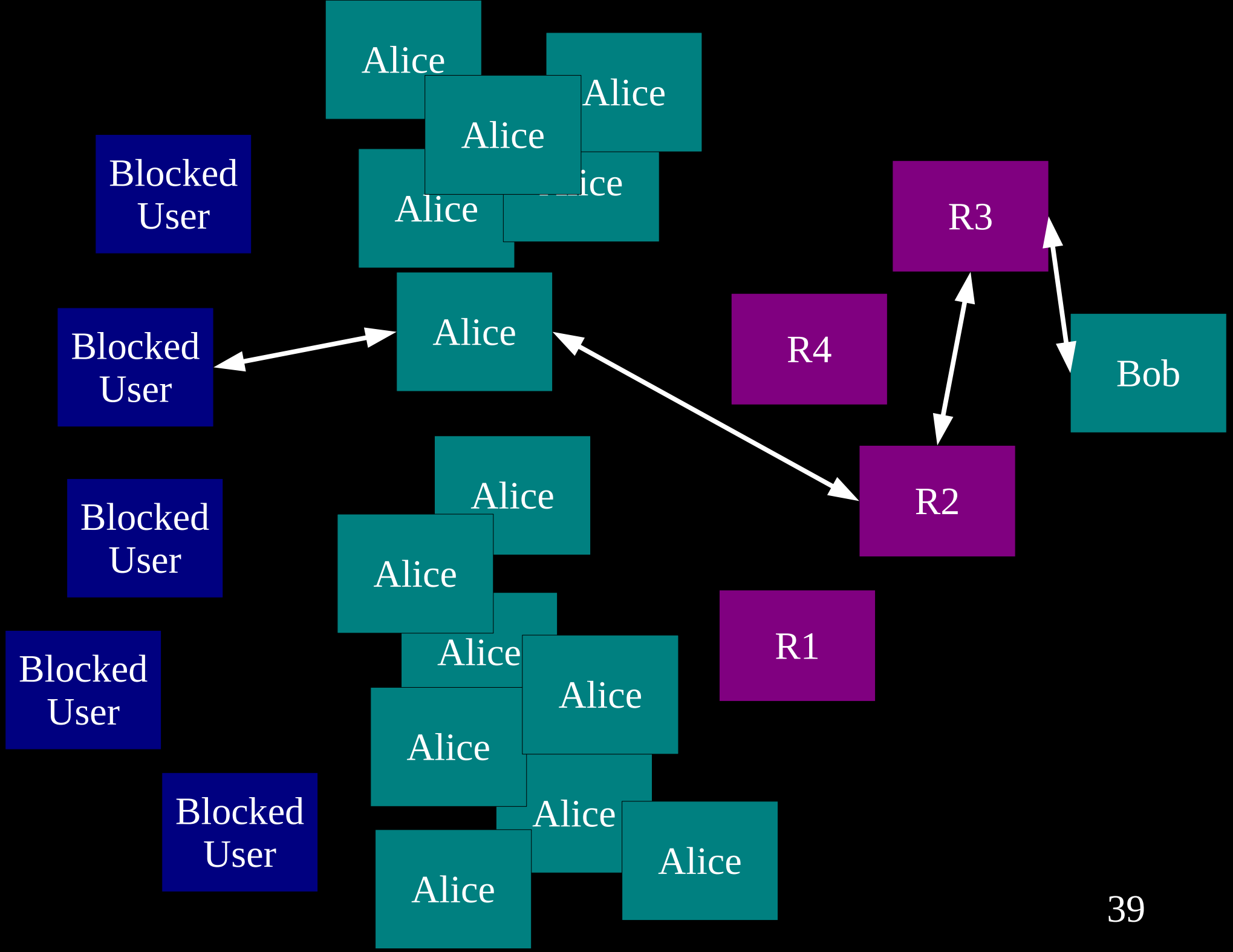
There are two pieces to all these “proxying” schemes:

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.




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

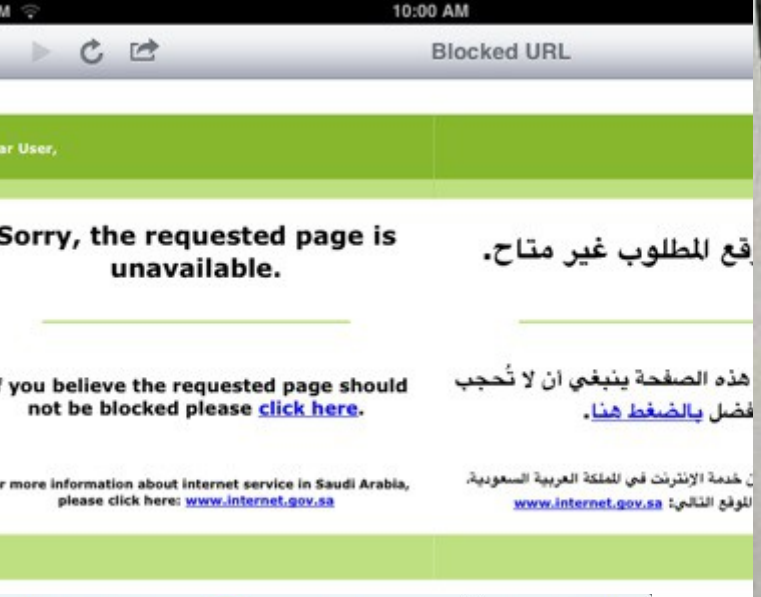
2) By blocking all the relay IP addresses in the directory, or the addresses of other Tor services

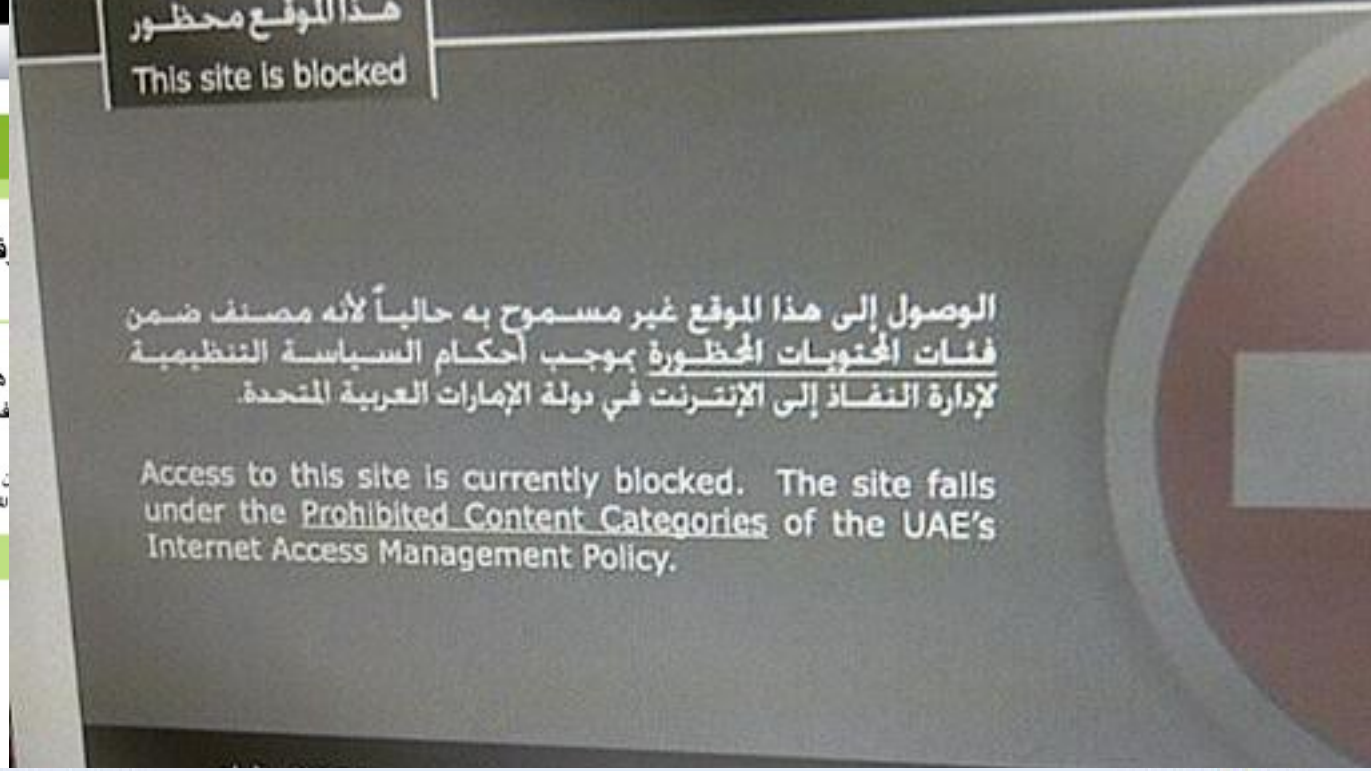
3) By filtering based on Tor's network fingerprint

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

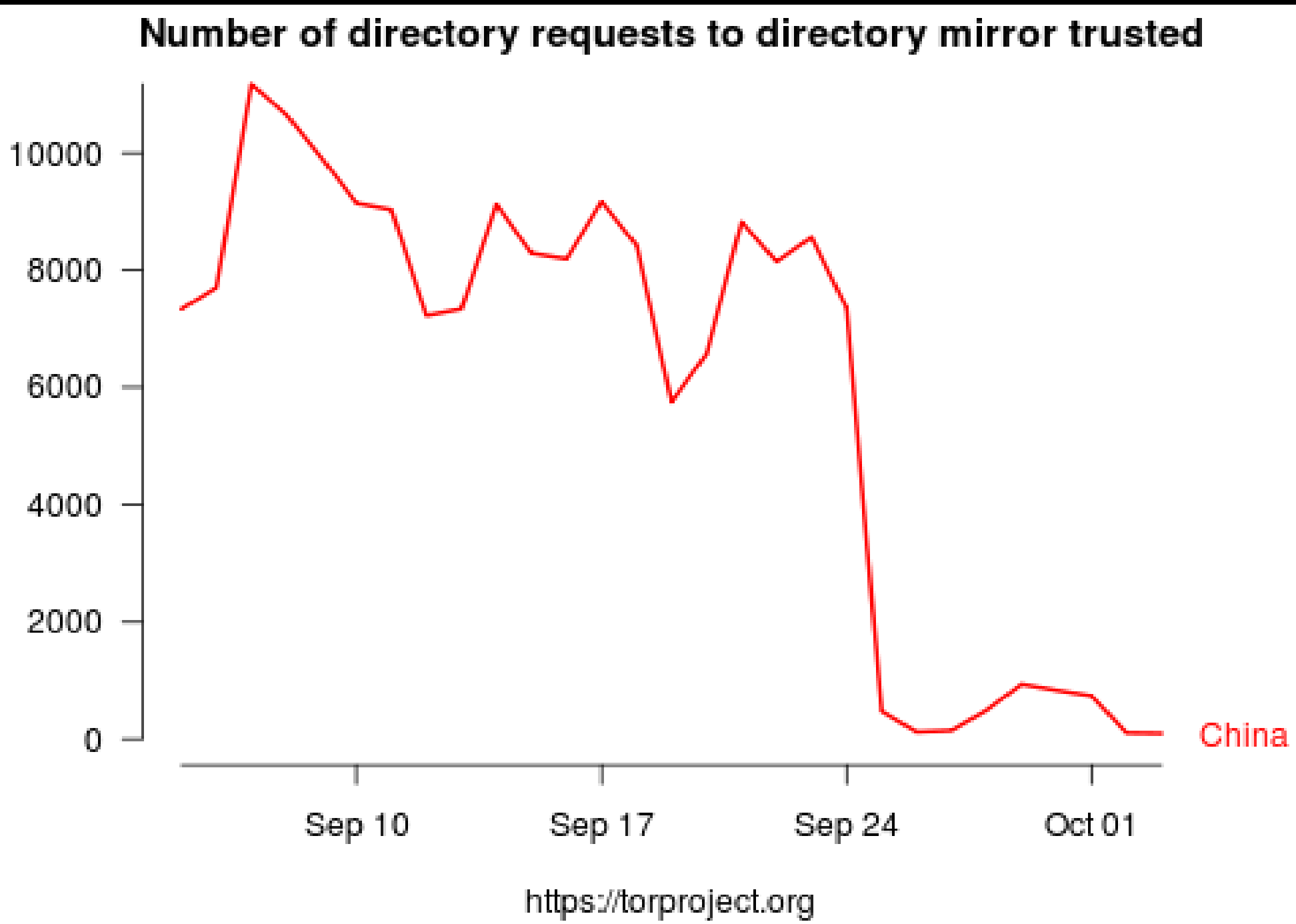

10:00 AM
Blocked URL
ar User,
Sorry, the requested page is unavailable.
قع المطلوب غير متاح.
you believe the requested page should not be blocked please click here.
هذه الصفحة ينبغي أن لا تُحجب
فضل بالضغط هنا.
r more information about internet service in Saudi Arabia, please click here: www.internet.gov.sa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

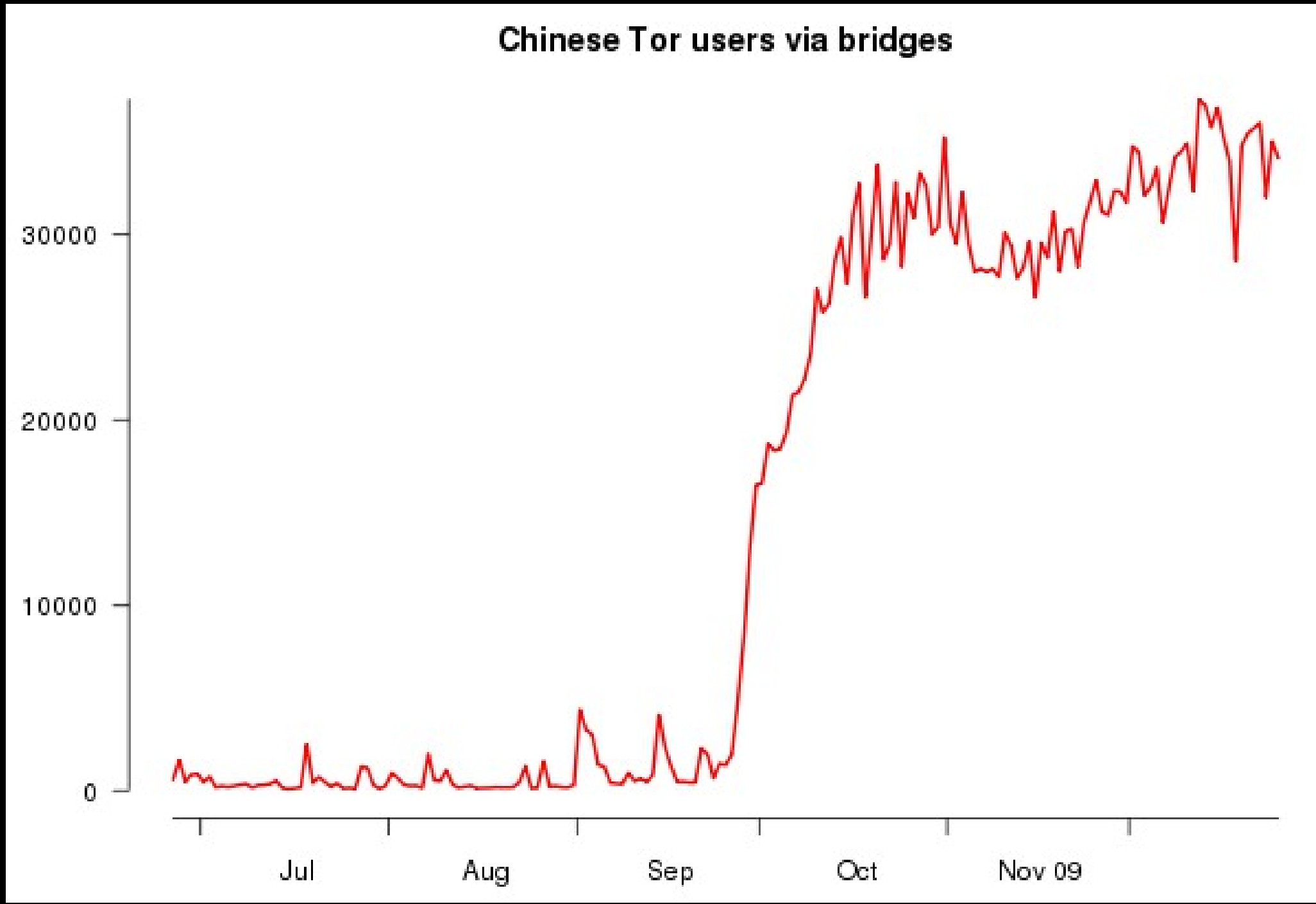

This site is blocked
الوصول إلى هذا الموقع غير مسموح به حالياً لأنه مصنف ضمن فئات المحتويات المحظورة بموجب أحكام السياسة التنظيمية لإدارة النفاذ إلى الإنترنت في دولة الإمارات العربية المتحدة.
Access to this site is currently blocked. The site falls under the Prohibited Content Categories of the UAE's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

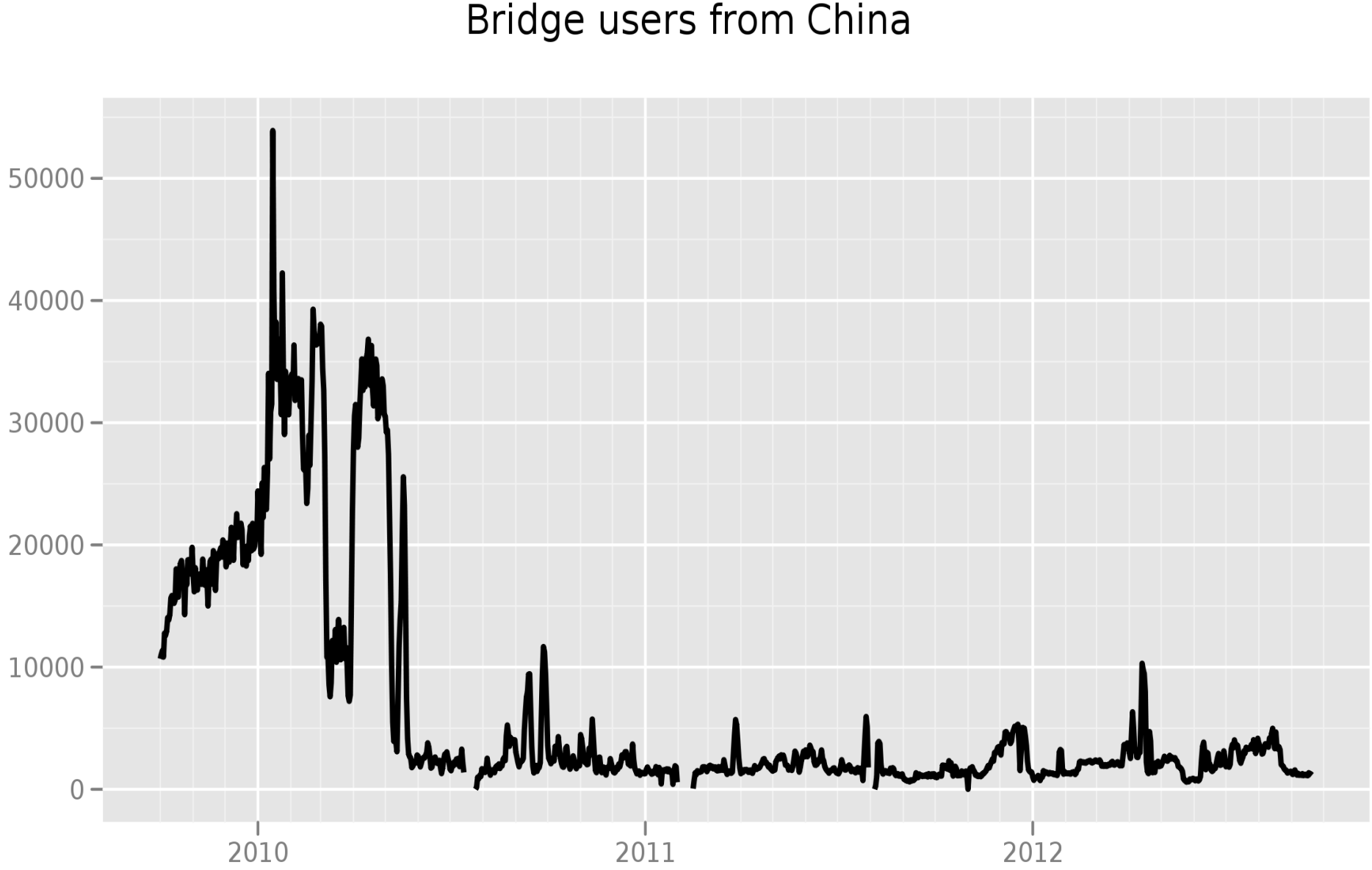

KT WATA...
٩:٢١ ص
87%
Tweet
Blocked by Mada Com...


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



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

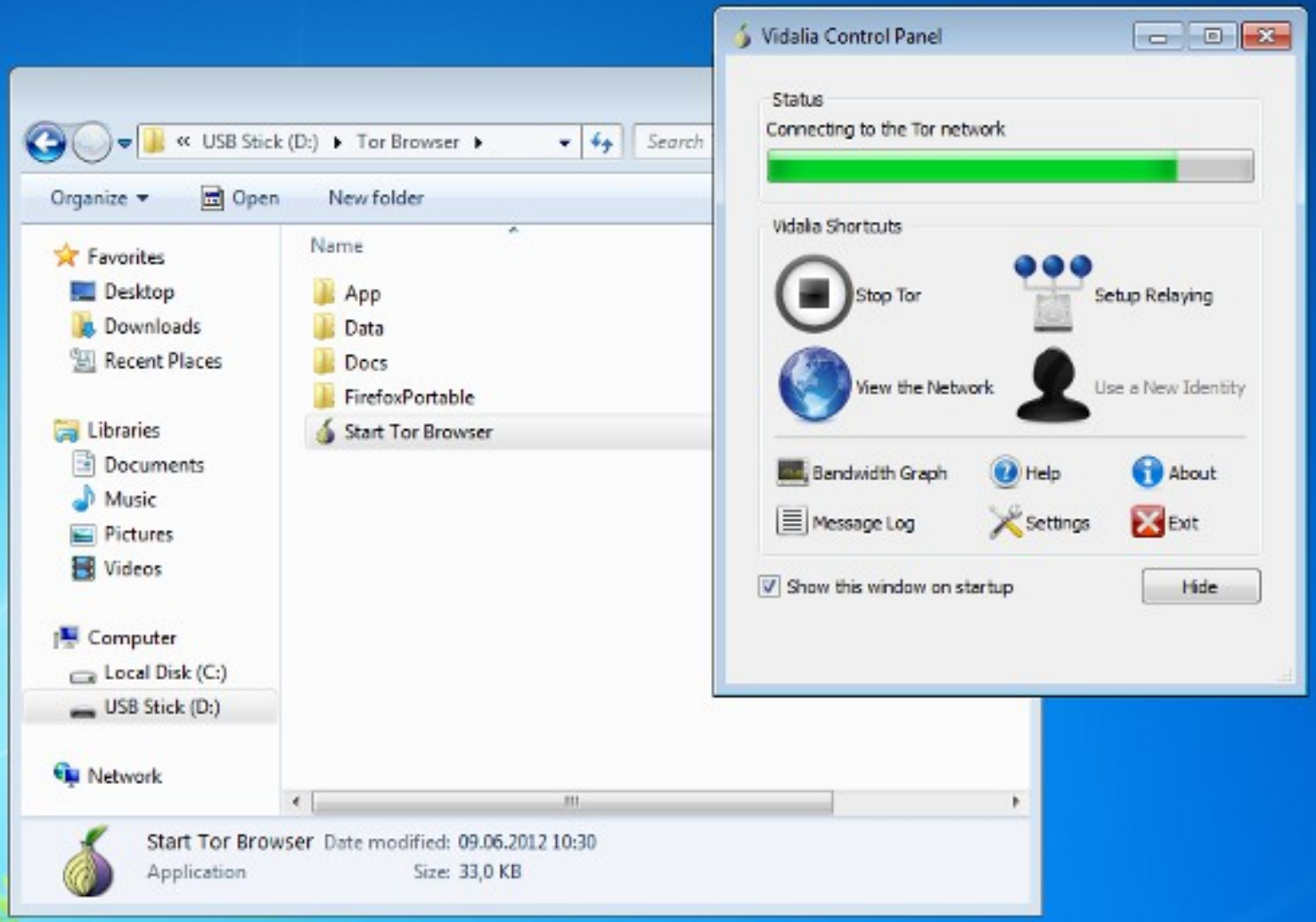
- Javascript refresh attack
- Cookies, History, browser window size, user-agent, language, http auth, ...
- Our Torbutton Firefox extension tackles many of these

Flash is dangerous too

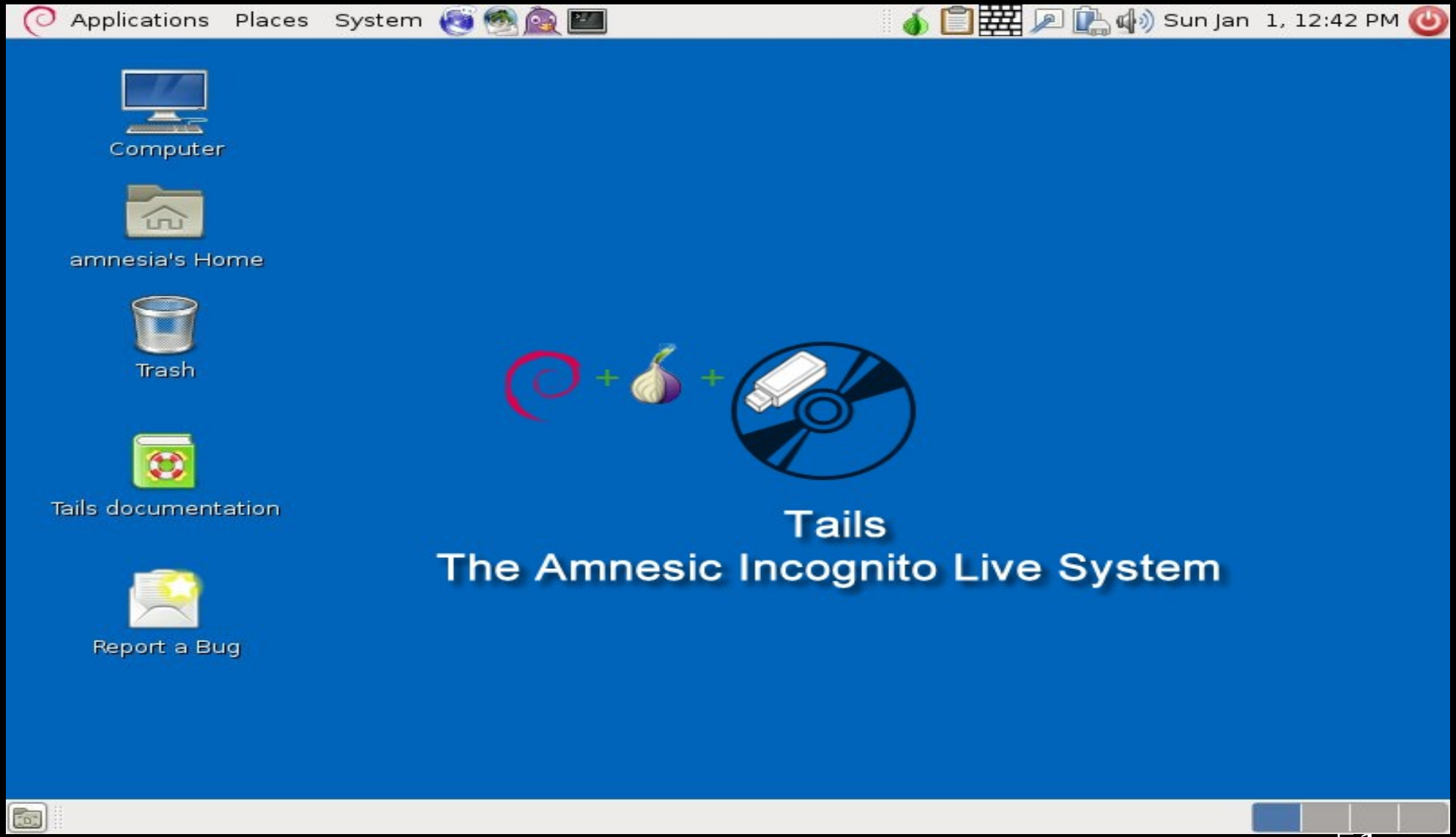
Some apps are bad at obeying their proxy settings.

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

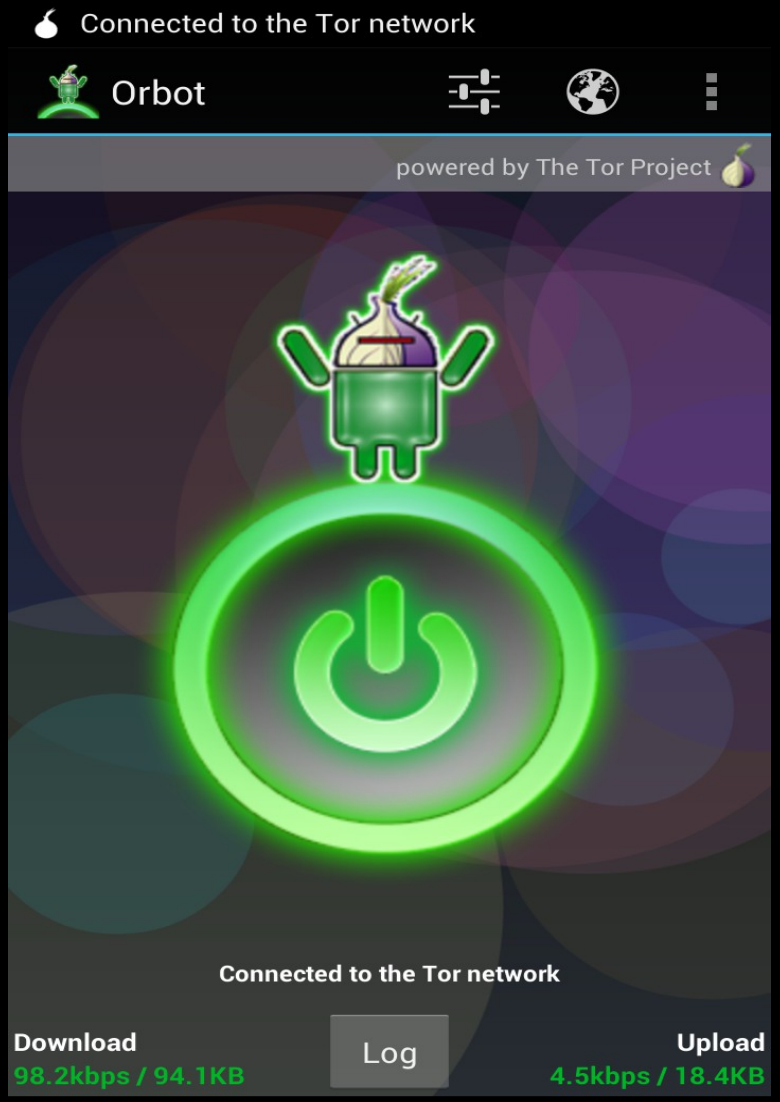
Tor Browser Bundle (TBB)



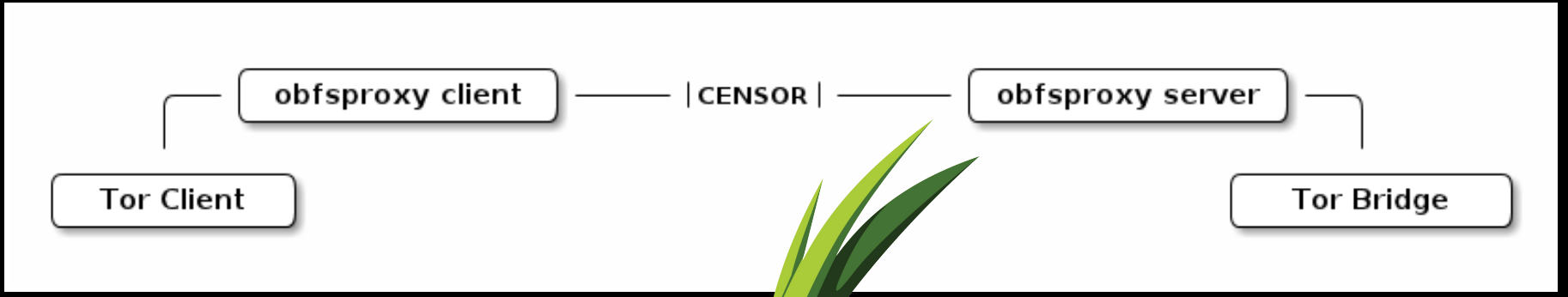
Tails (Tor LiveCD)

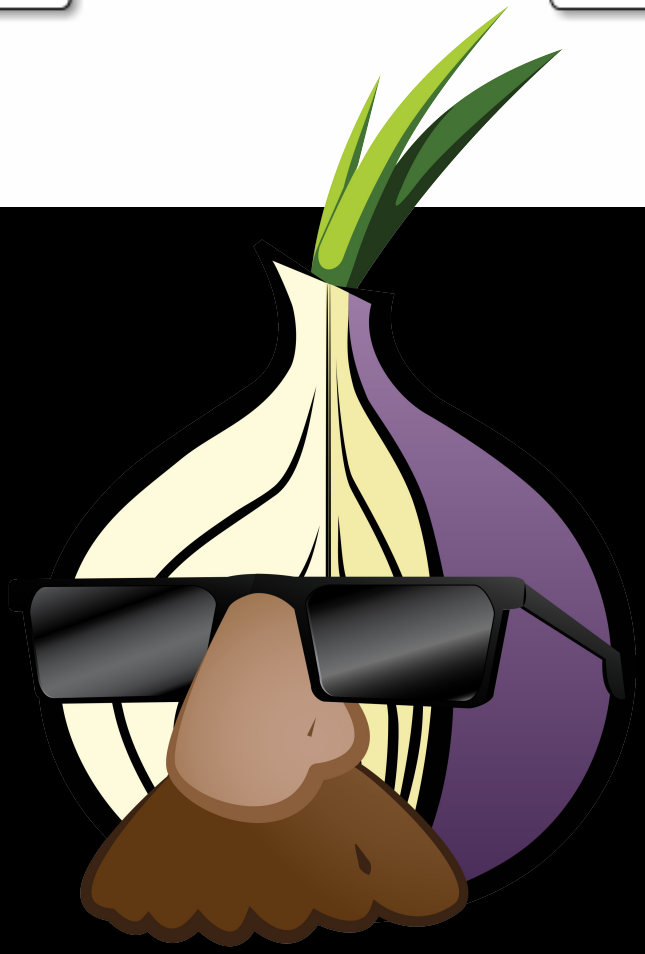


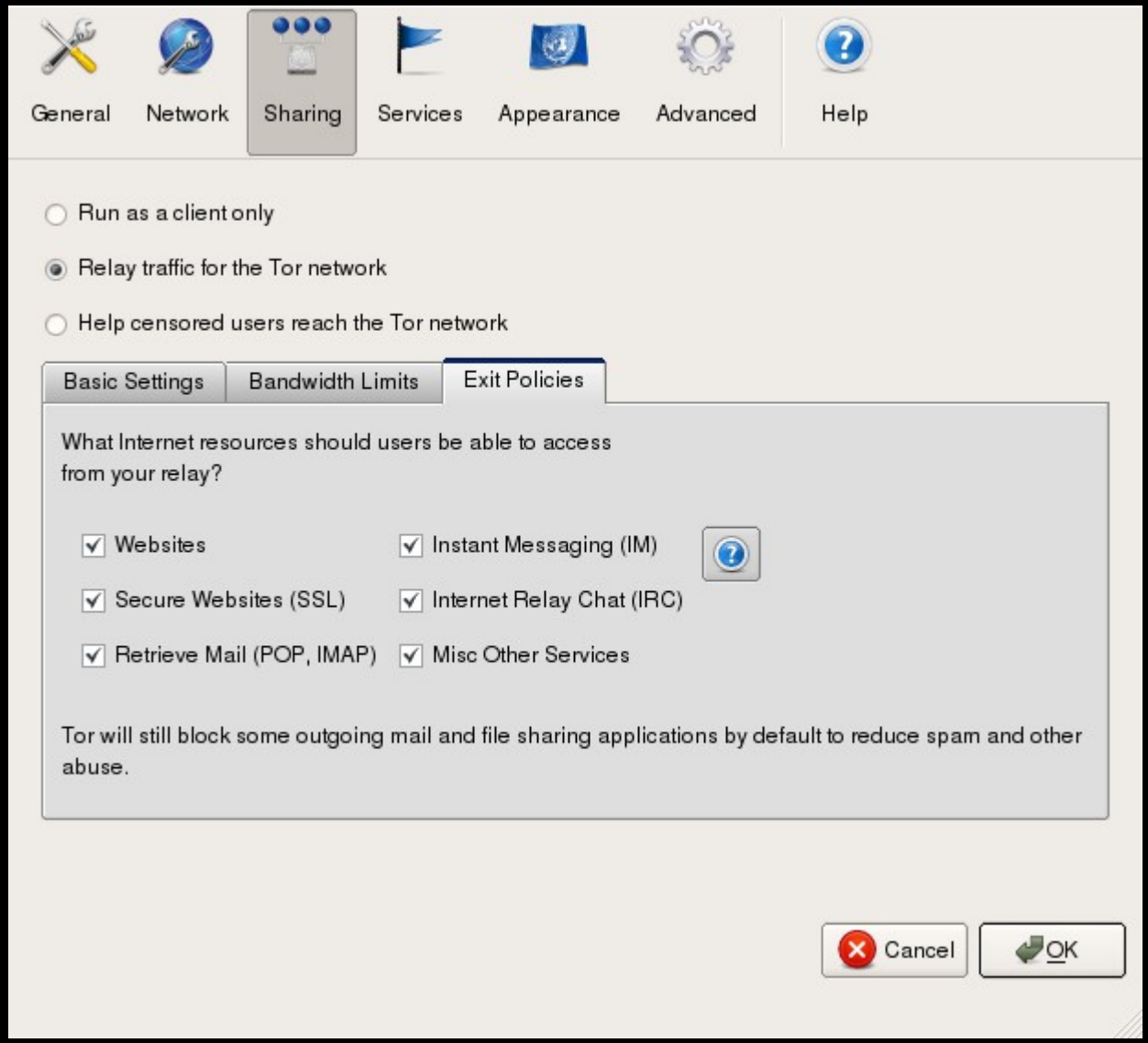
Orbot (Tor for Android)



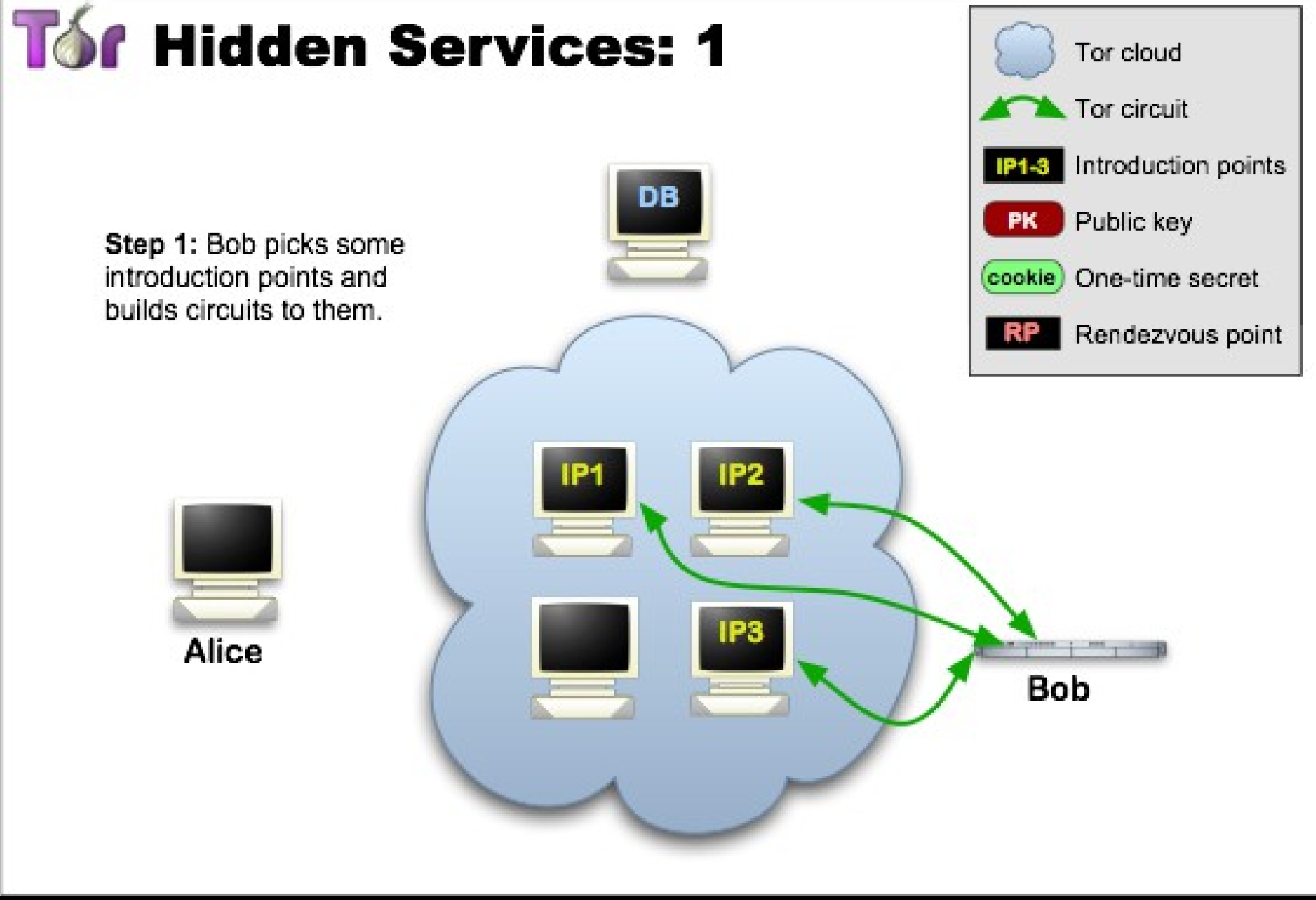
Tor pluggable transports





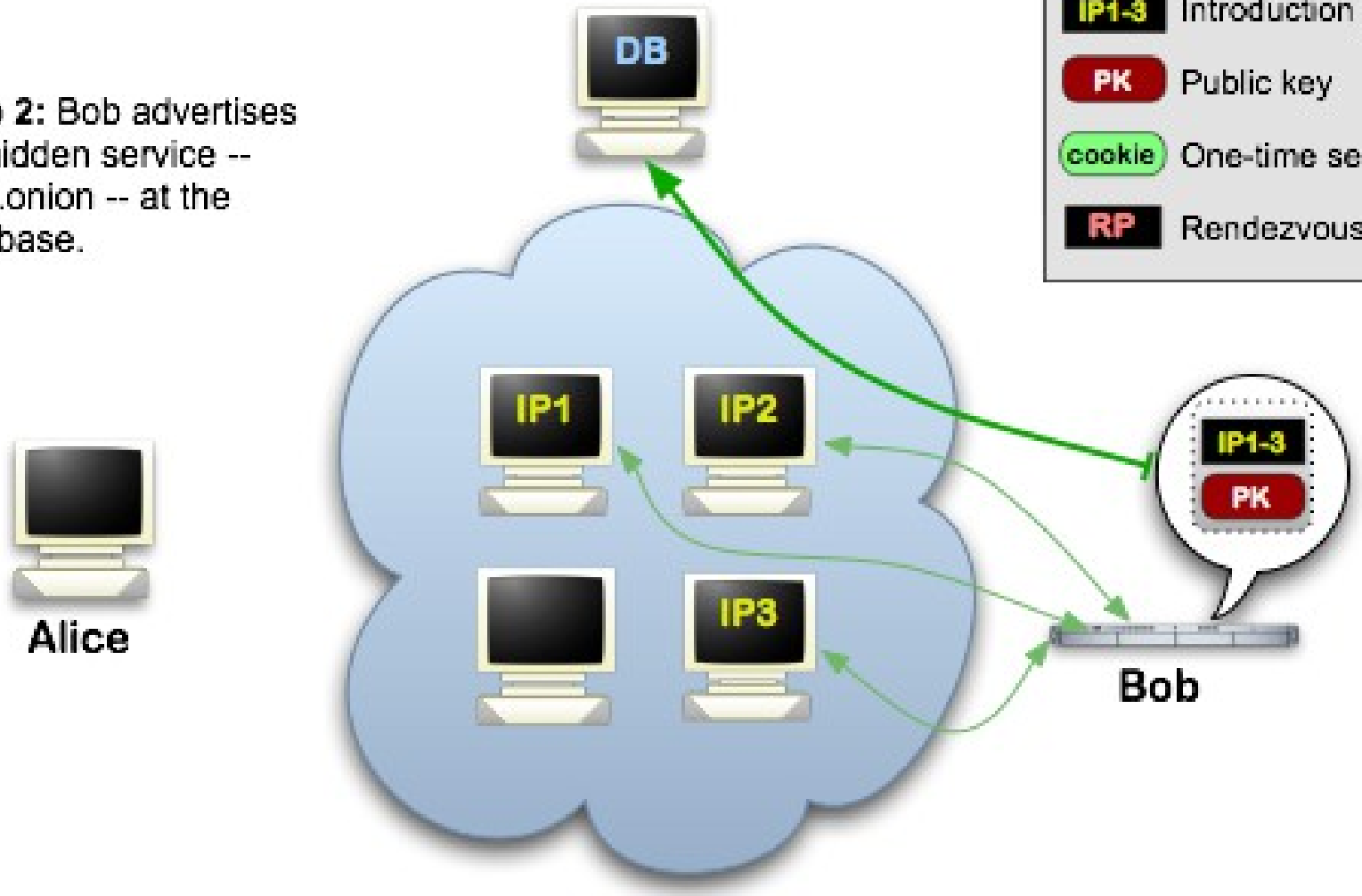

General
Network
Sharing
Services
Appearance
Advanced
Help
Run as a client only
Relay traffic for the Tor network
Help censored users reach the Tor network
Basic Settings
Bandwidth Limits
Exit Policies
What Internet resources should users be able to access from your relay?
Websites
Instant Messaging (IM)
Secure Websites (SSL)
Internet Relay Chat (IRC)
Retrieve Mail (POP, IMAP)
Misc Other Services
Tor will still block some outgoing mail and file sharing applications by default to reduce spam and other abuse.
Cancel
OK

Hidden Services: 1

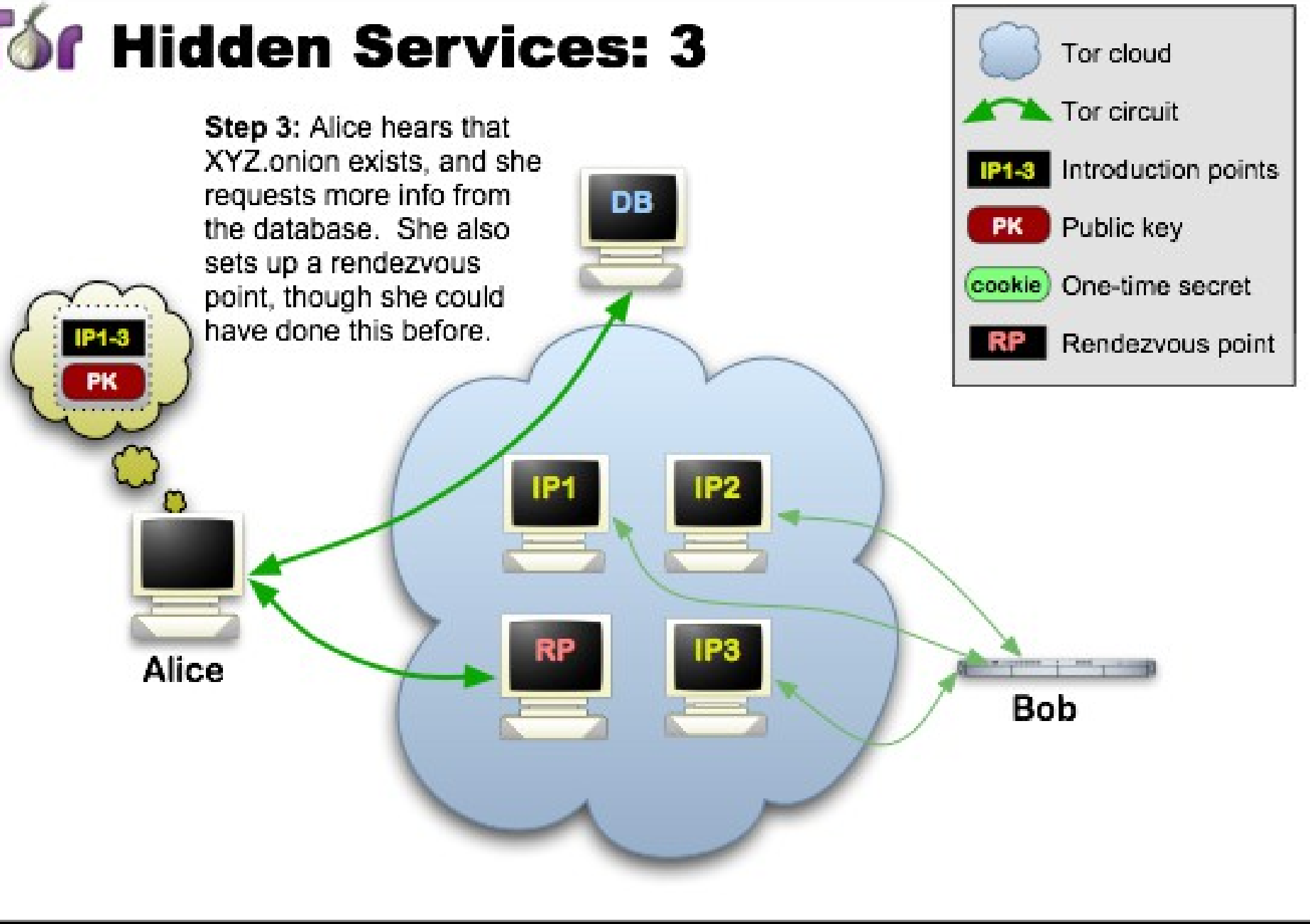


Hidden Services: 2

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

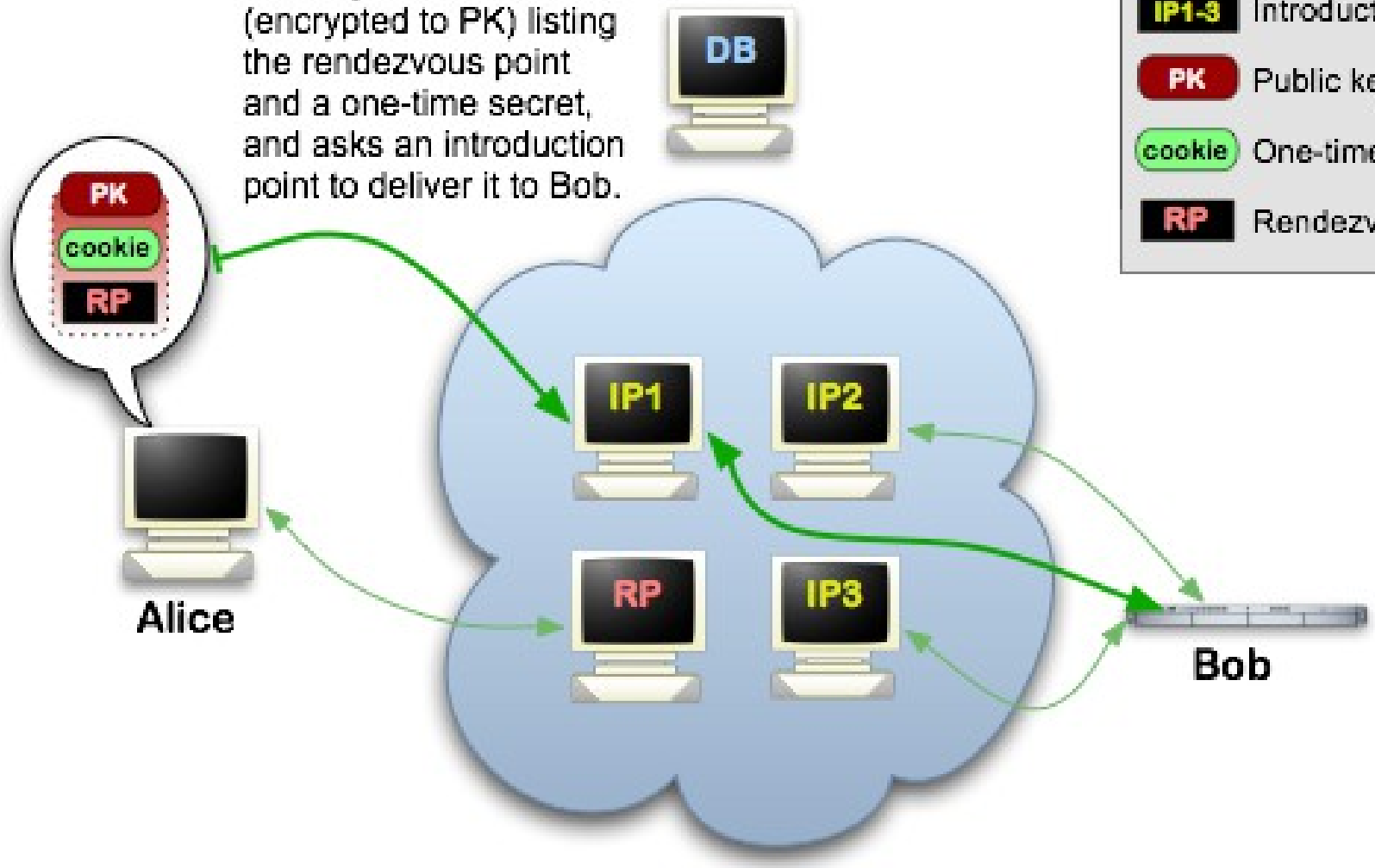


Hidden Services: 3



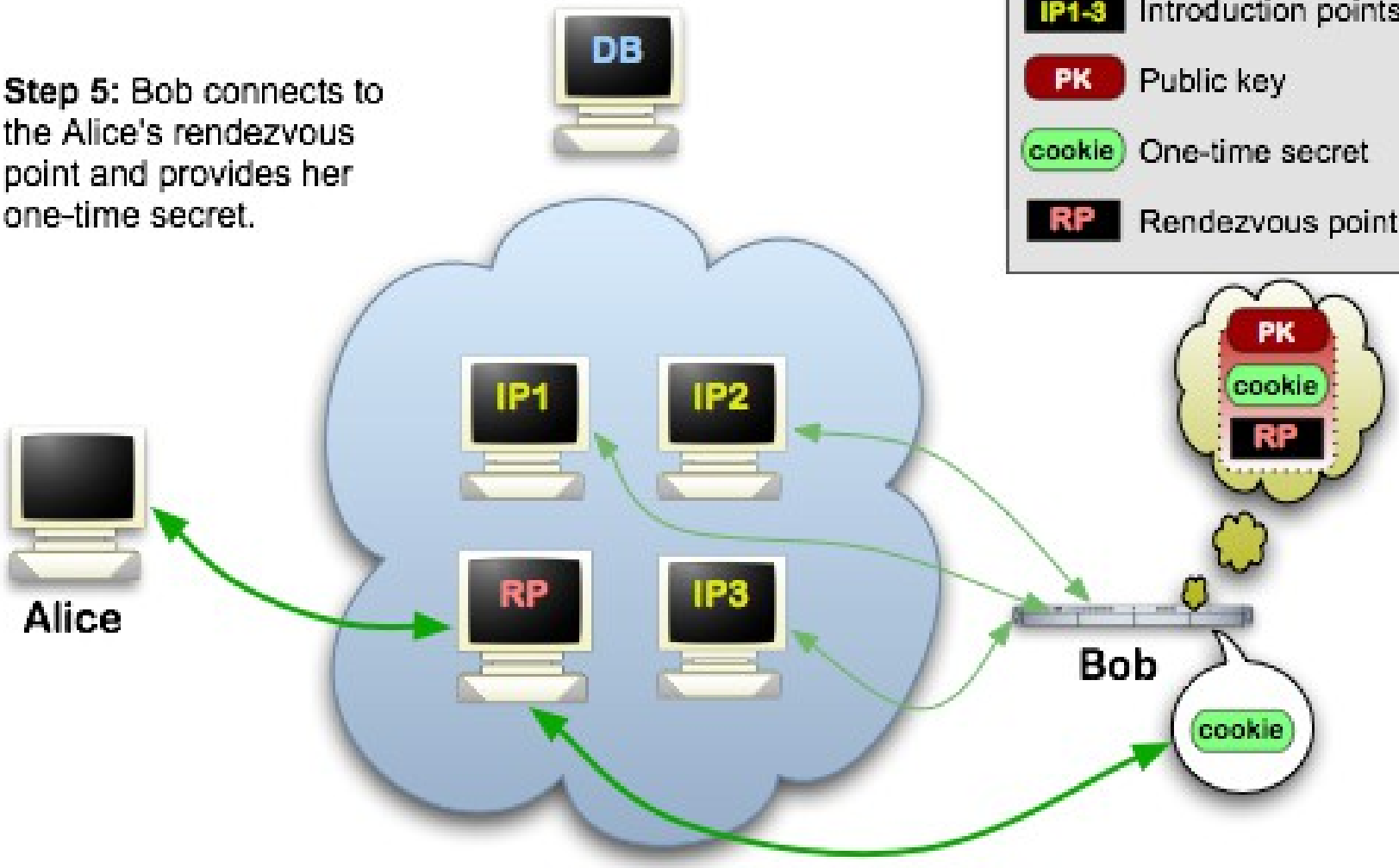
Hidden Services: 4

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.



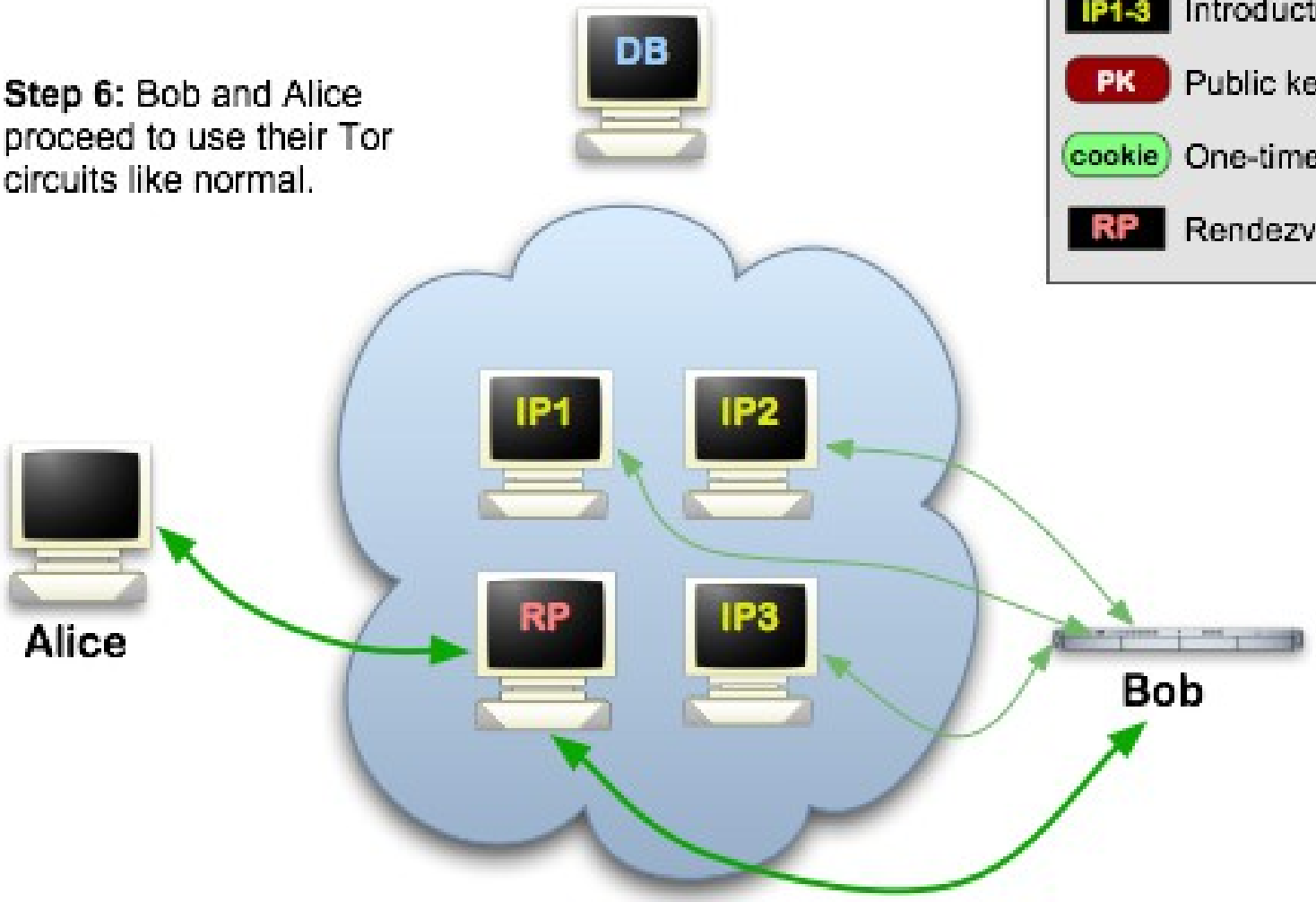
Hidden Services: 5

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



Hidden Services: 6

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



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

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?
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.