Tor

Source Barcelona 2010

Sebastian Hahn
The Tor Project
https://torproject.org/

What is Tor?

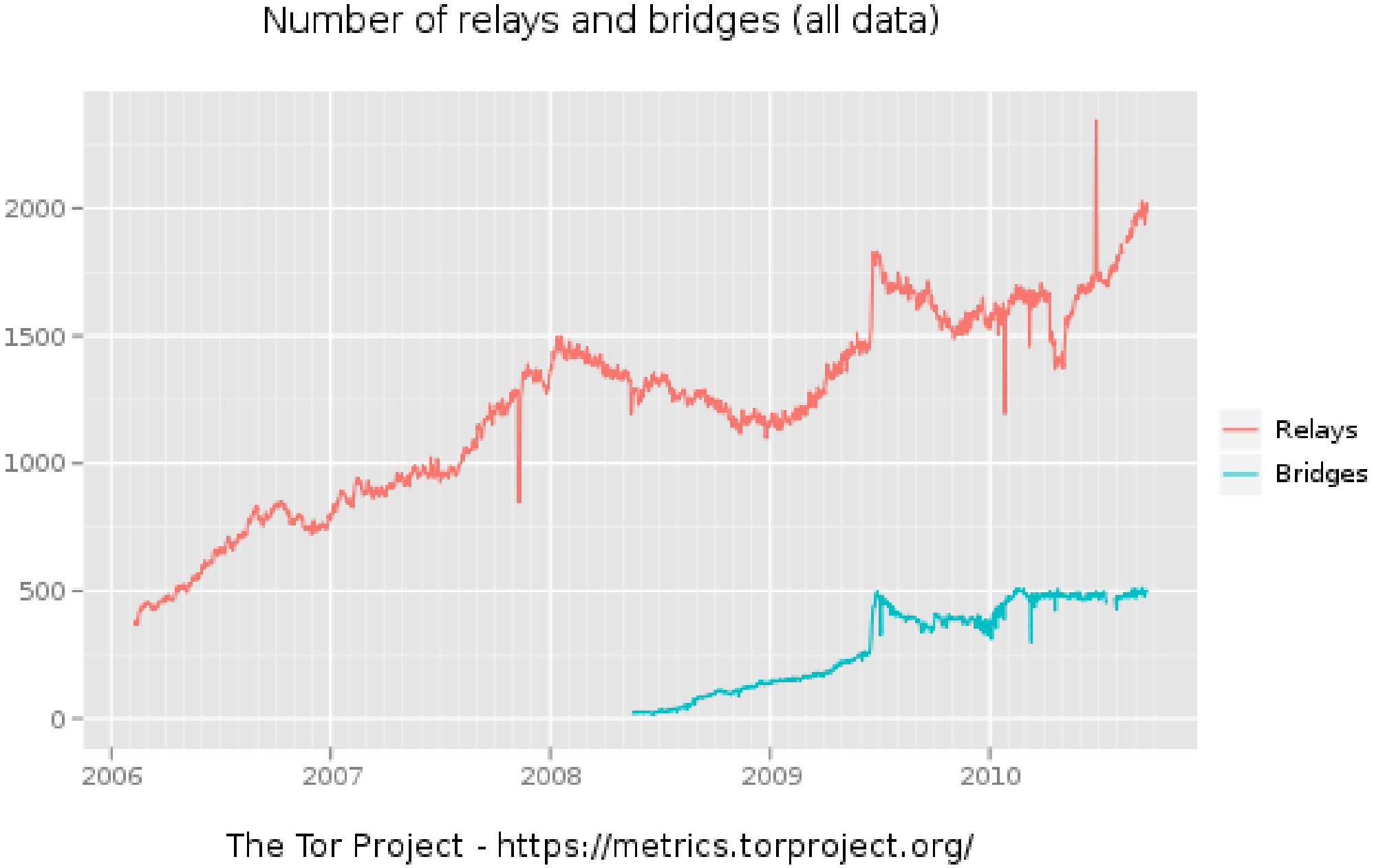
- Online anonymity software and volunteer-run network
- Open source, freely available
- Community of researchers, developers, users, and relay operators
- A popular circumvention tool in various countries and other places with restricted internet access

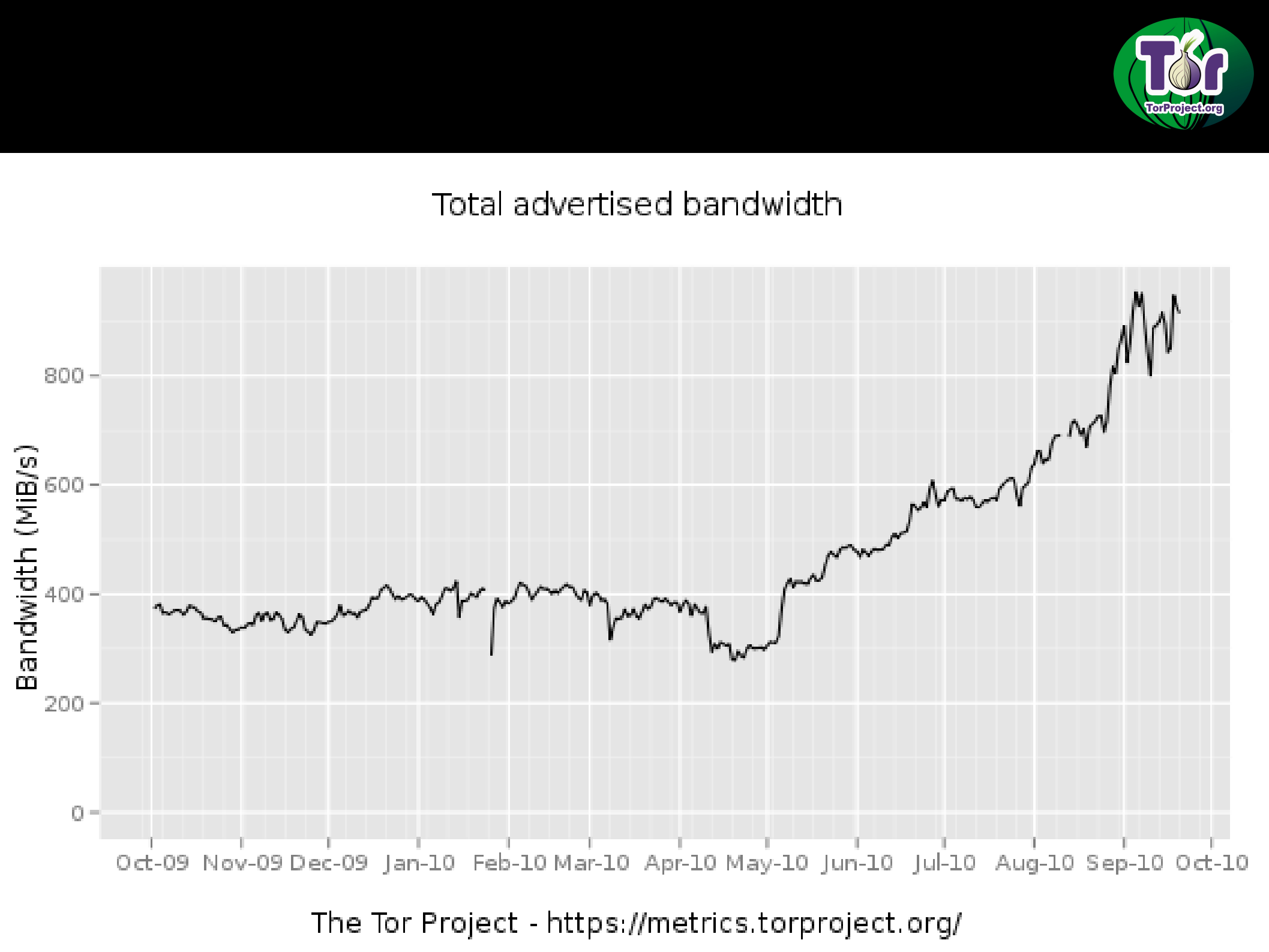
The Tor Project, Inc.

- Non-Profit corporation dedicated to developing tools for online privacy and anonymity
- 15 funded developers, dozens of volunteers and > 1,000 relay operators
- Tor has been funded by a diverse set of parties, such as the US government, the EFF, the NSF, private donations

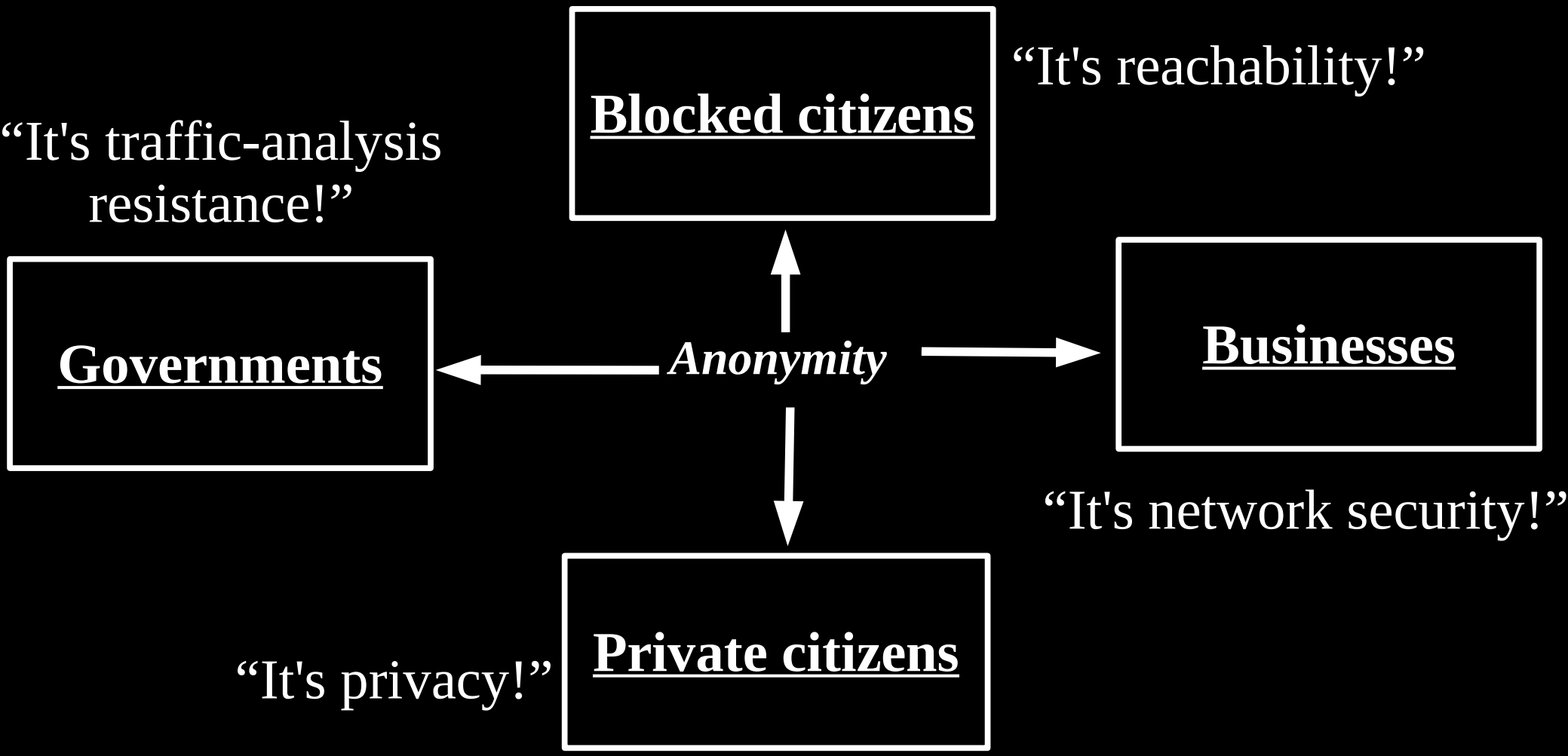
The Tor Network

- Roughly 2000 relays up at any time
- Average of 5Gb/s (last month)
- Approximately 500,000 daily users

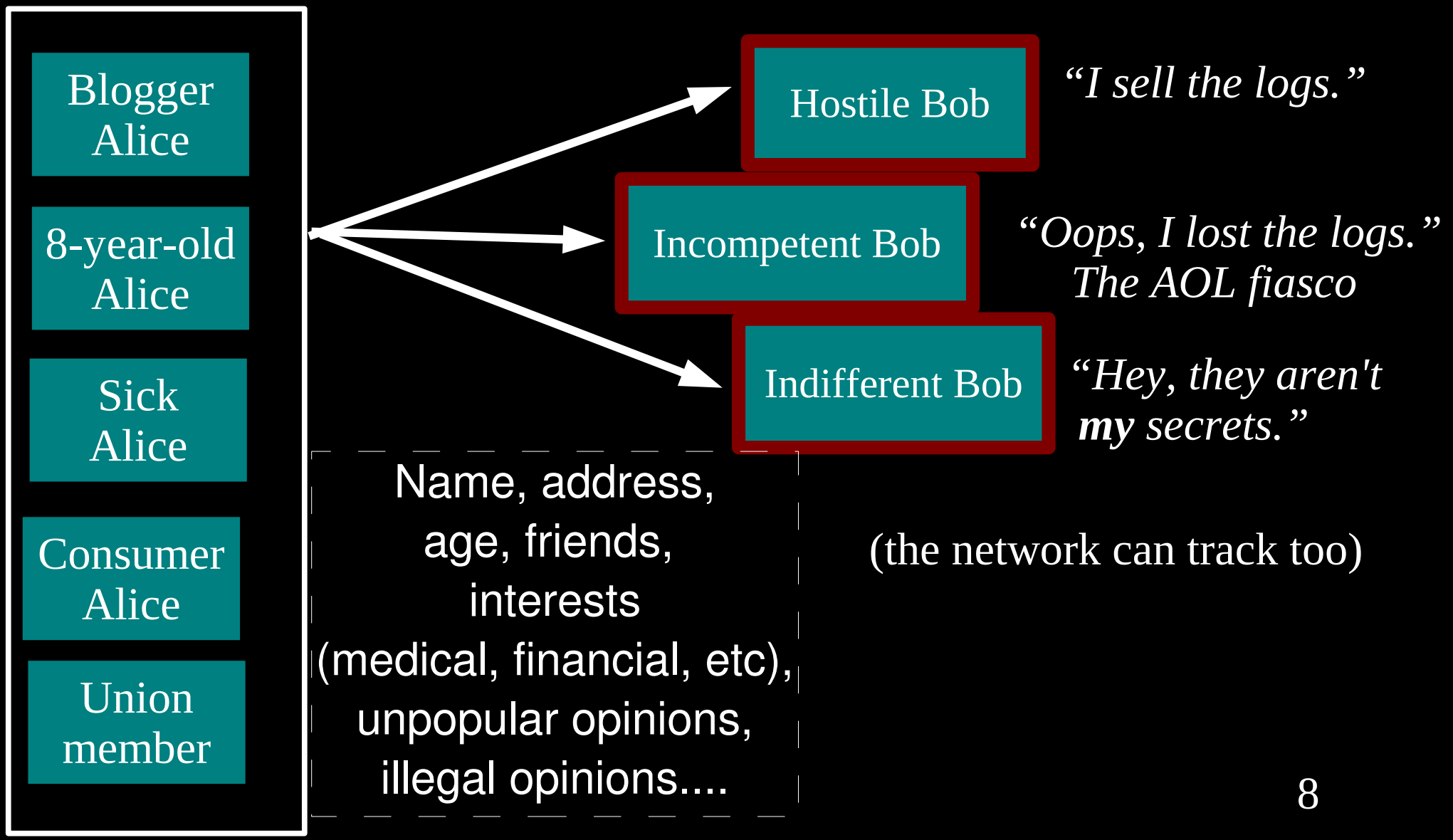

Number of relays and bridges (all data)
2000
1500
1000
500
0
2006
2007
2008
2009
2010
Relays
Bridges
The Tor Project - https://metrics.torproject.org/


Total advertised bandwidth
Bandwidth (MiB/s)
800
600
400
200
0
Oct-09
Nov-09
Dec-09
Jan-10
Feb-10
Mar-10
Apr-10
May-10
Jun-10
Jul-10
Aug-10
Sep-10
Oct-10
The Tor Project - https://metrics.torproject.org/

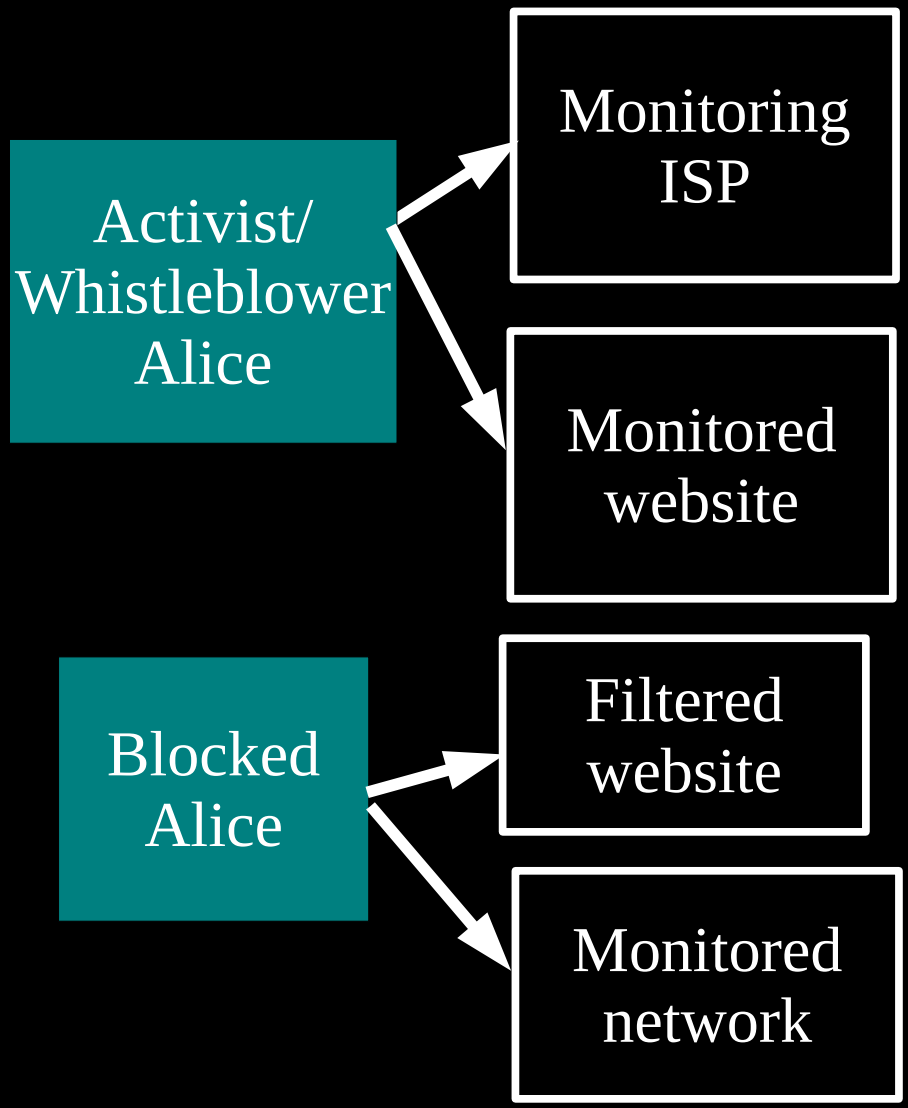
Anonymity serves different interests for different user groups.



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



Journalists and activists need Tor for their personal safety



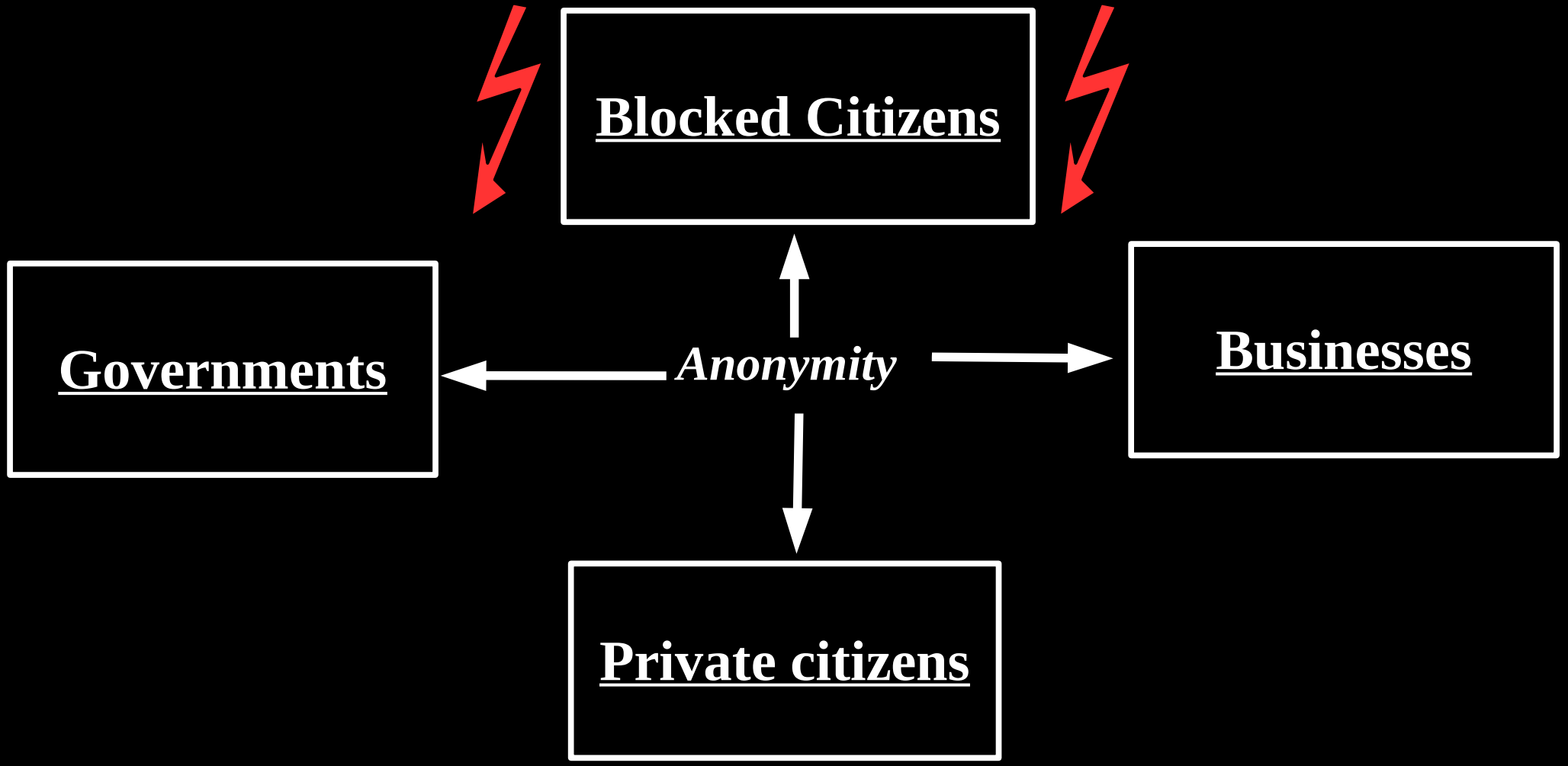
"Did you just post to that website?"

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

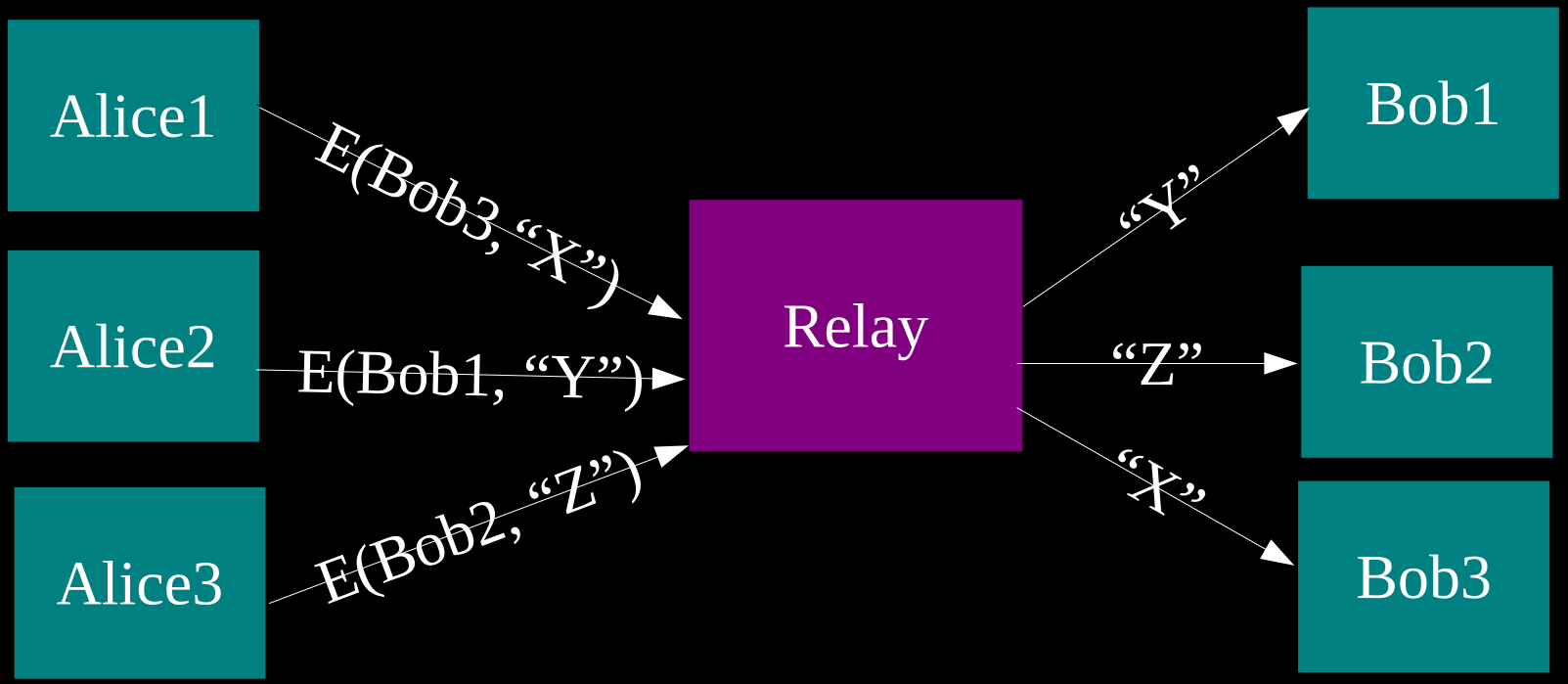
"What does the Global Voices website say today?"
"I want to tell people what's going on in my country"

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

Today: Circumvention

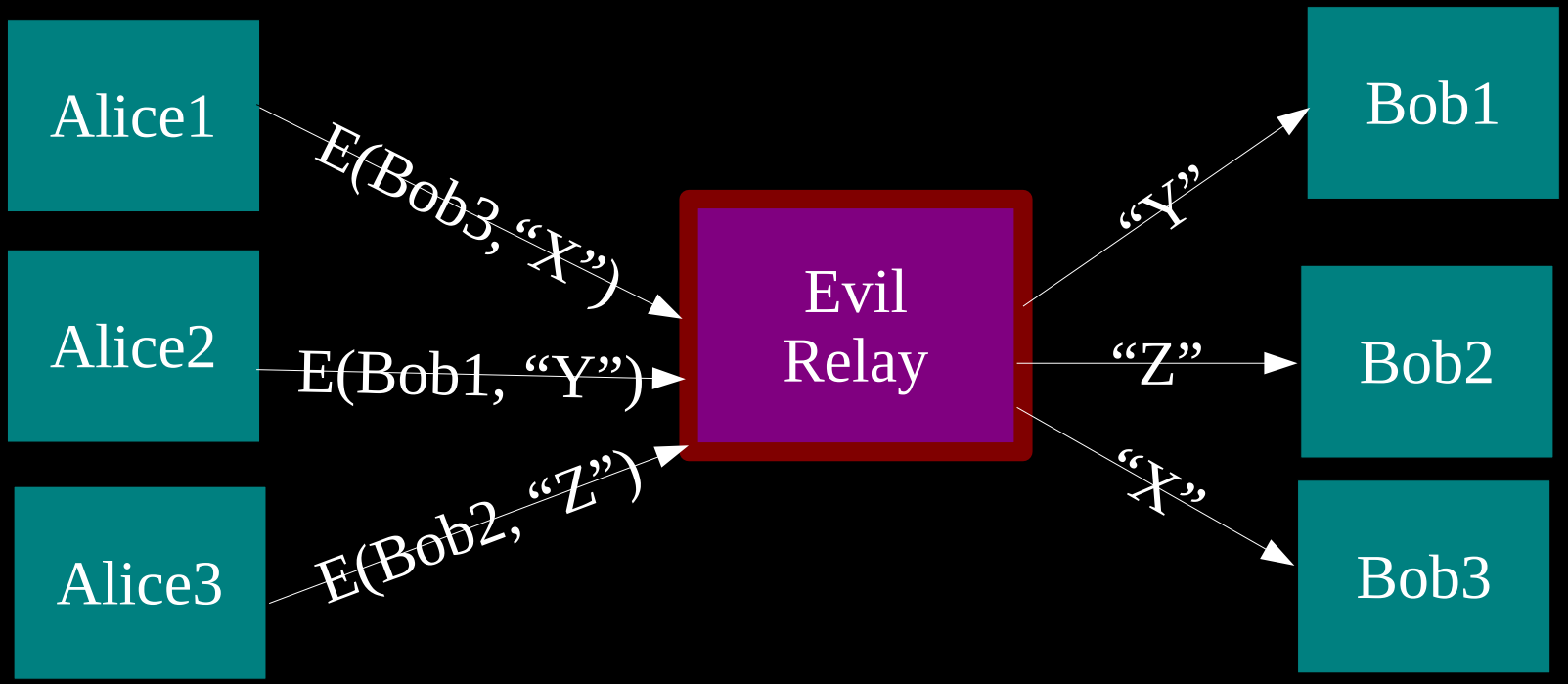


The simplest designs use a single relay to hide connections.

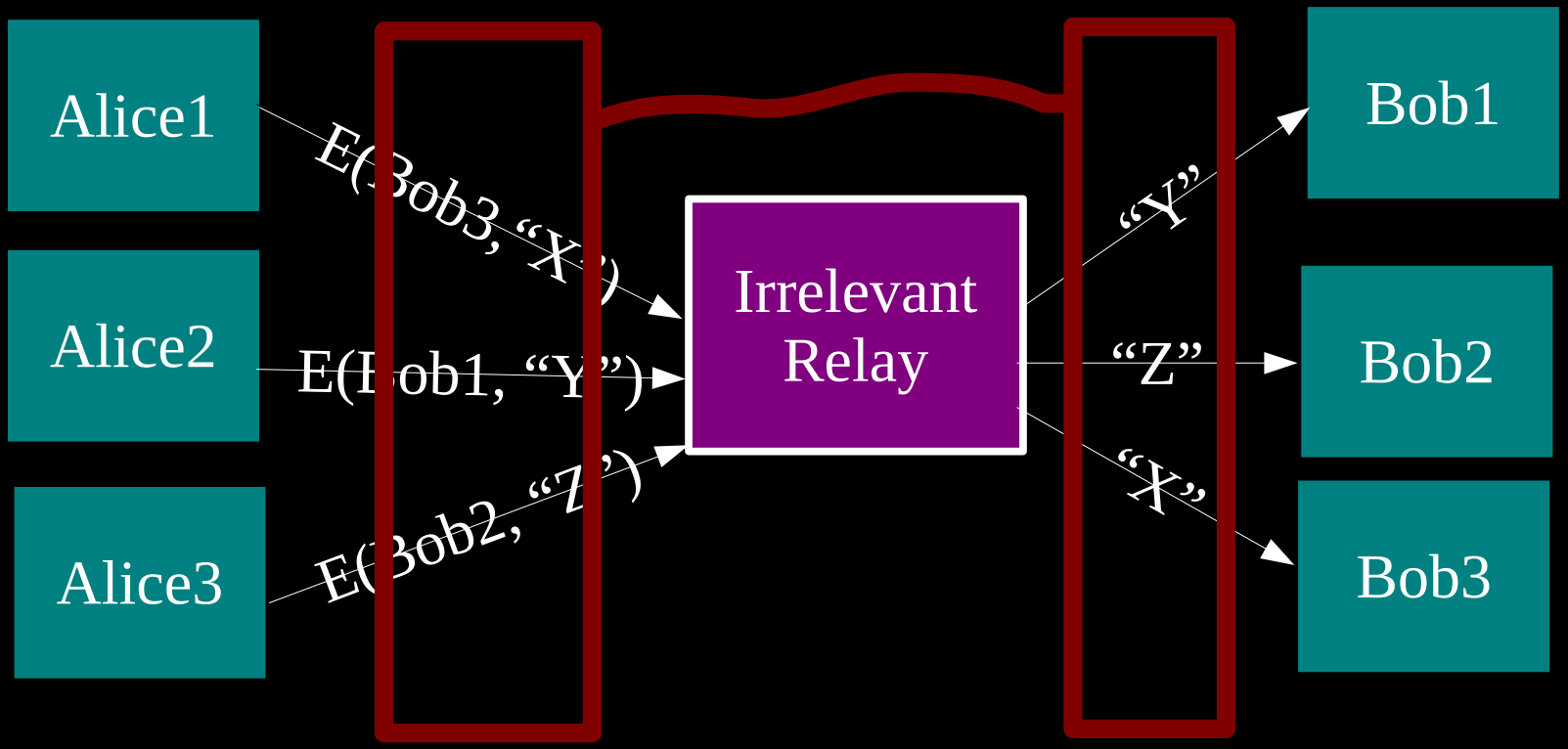


(example: some commercial proxy providers)

One relay is a single point of failure.

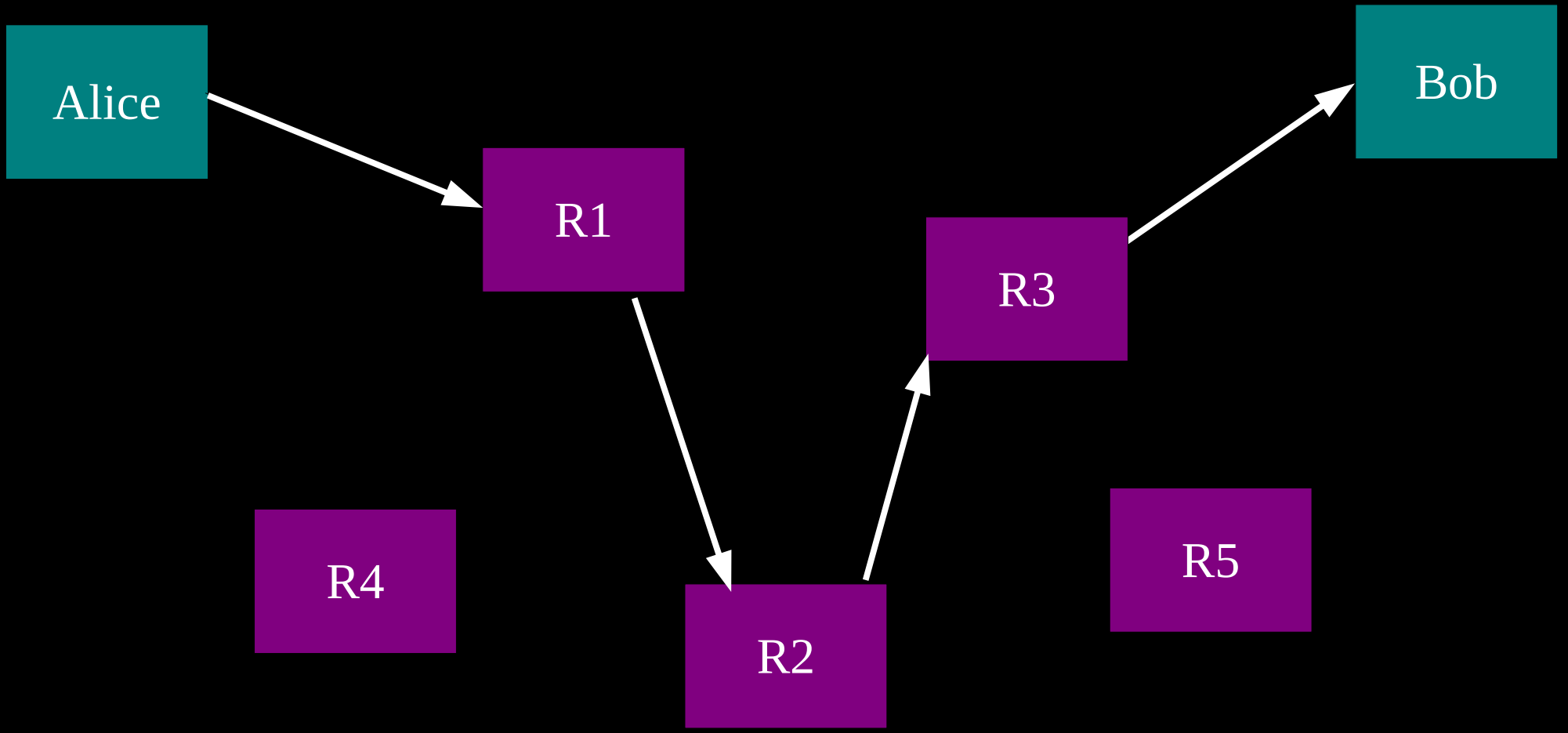


... or a single point of bypass.

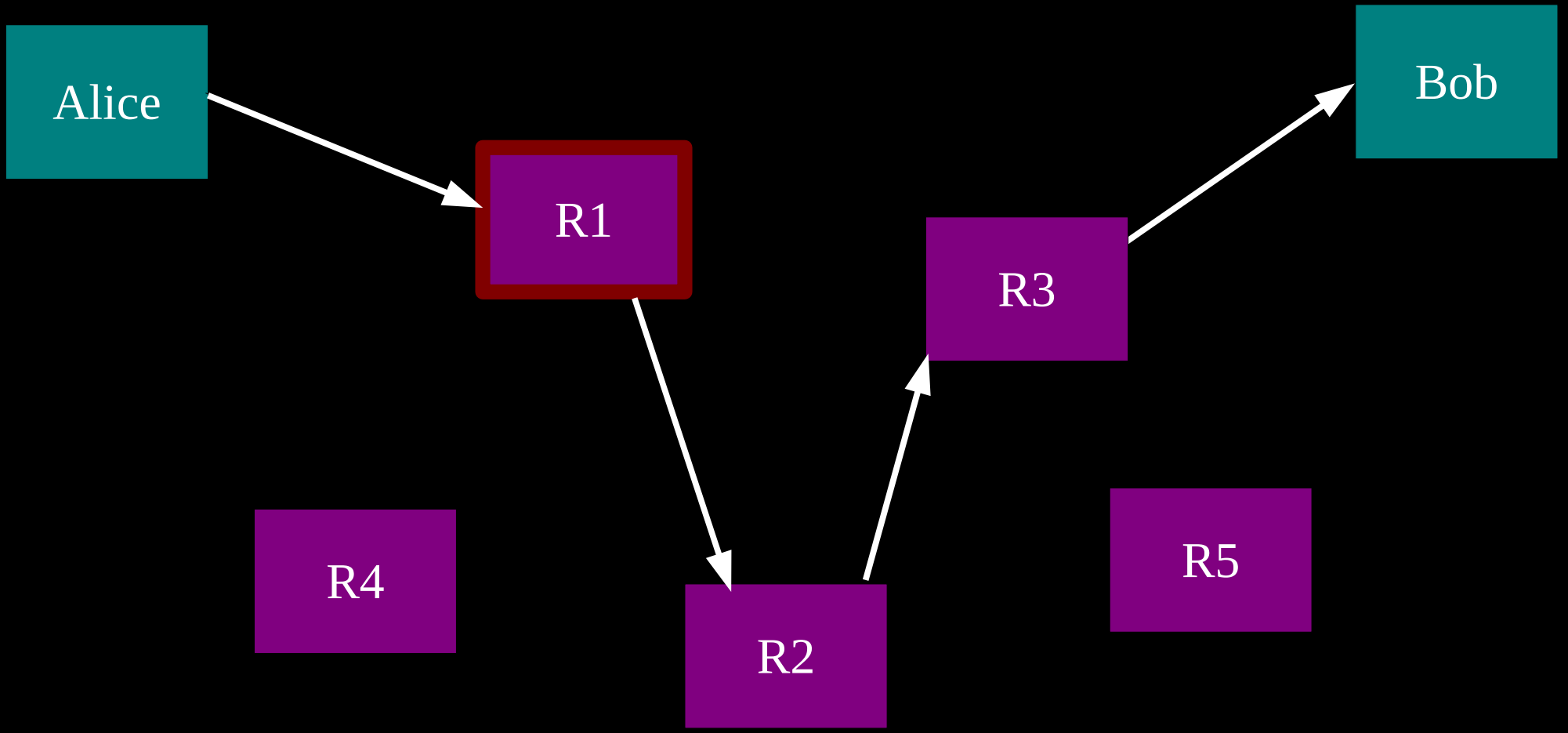


Timing analysis bridges all connections through relay ⇒ An attractive fat target

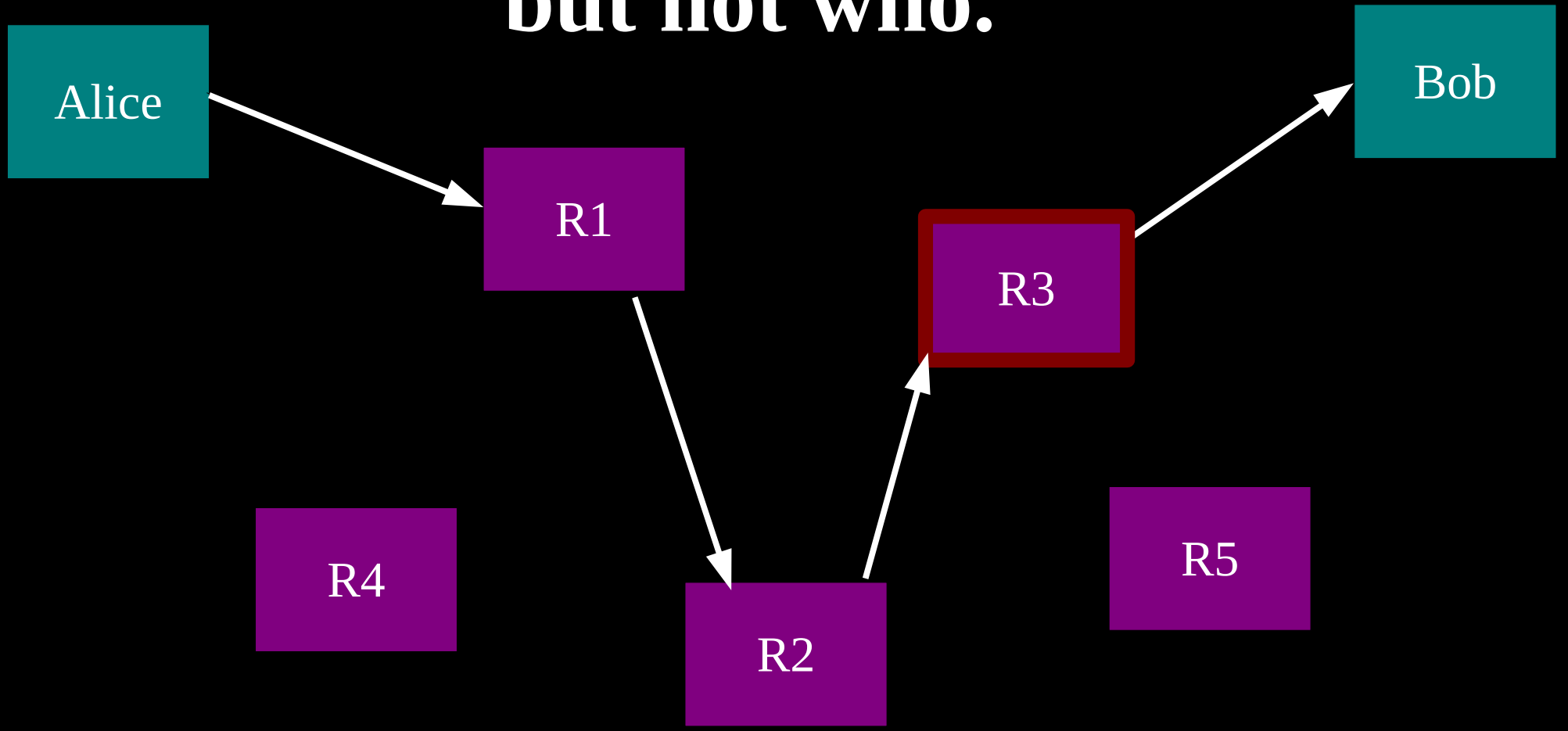
So, add multiple relays so that no single one can betray Alice.



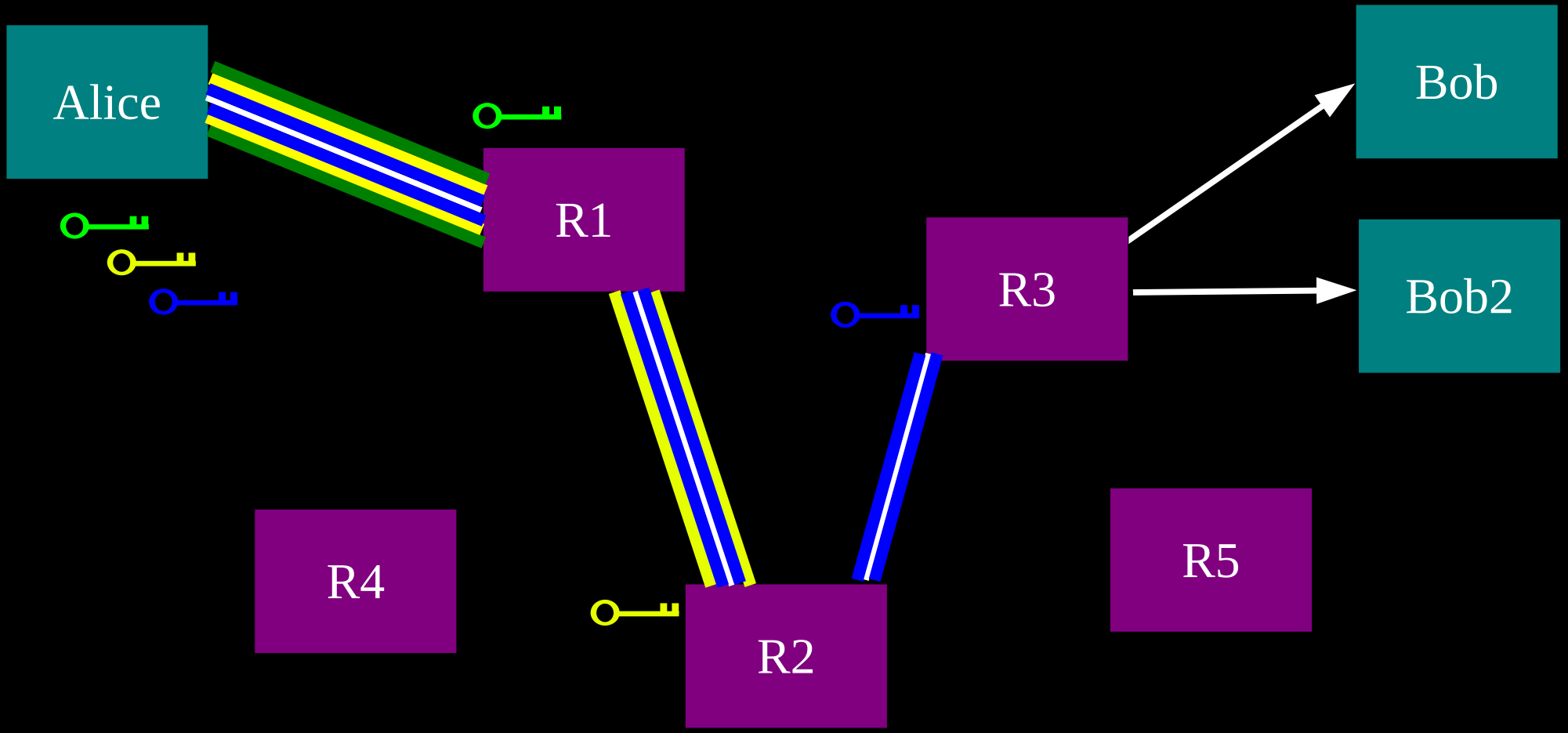
A corrupt first hop can tell that Alice is talking, but not to whom.



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



“Just use Tor” isn't enough

- Don't share information you want to keep private
- There are application-level attacks
  - Use Torbutton for web browsing
  - Zero-Install pre-configured bundles
  - Flash is dangerous – even without 0day

Tor does not magically encrypt the Internet!

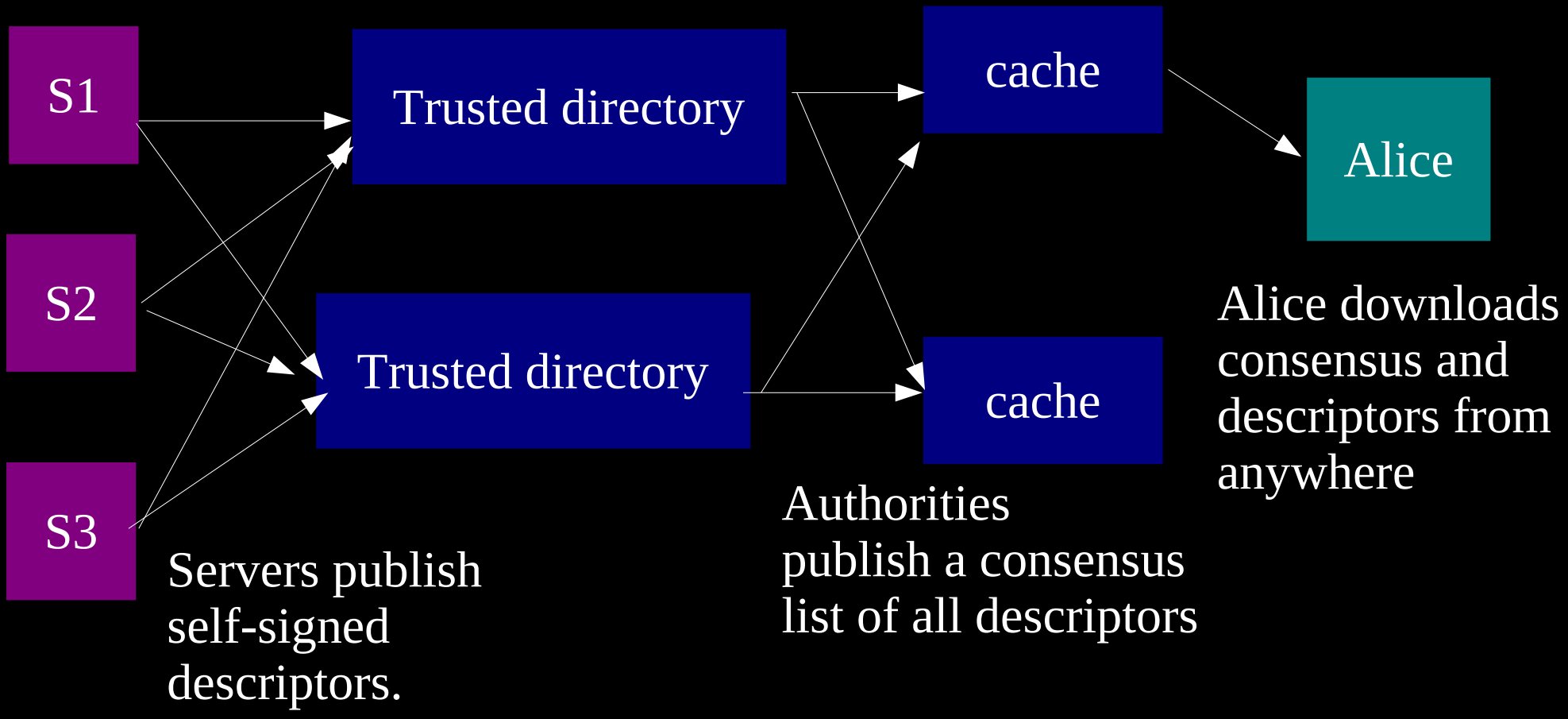
Some external constraints remain

- 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.

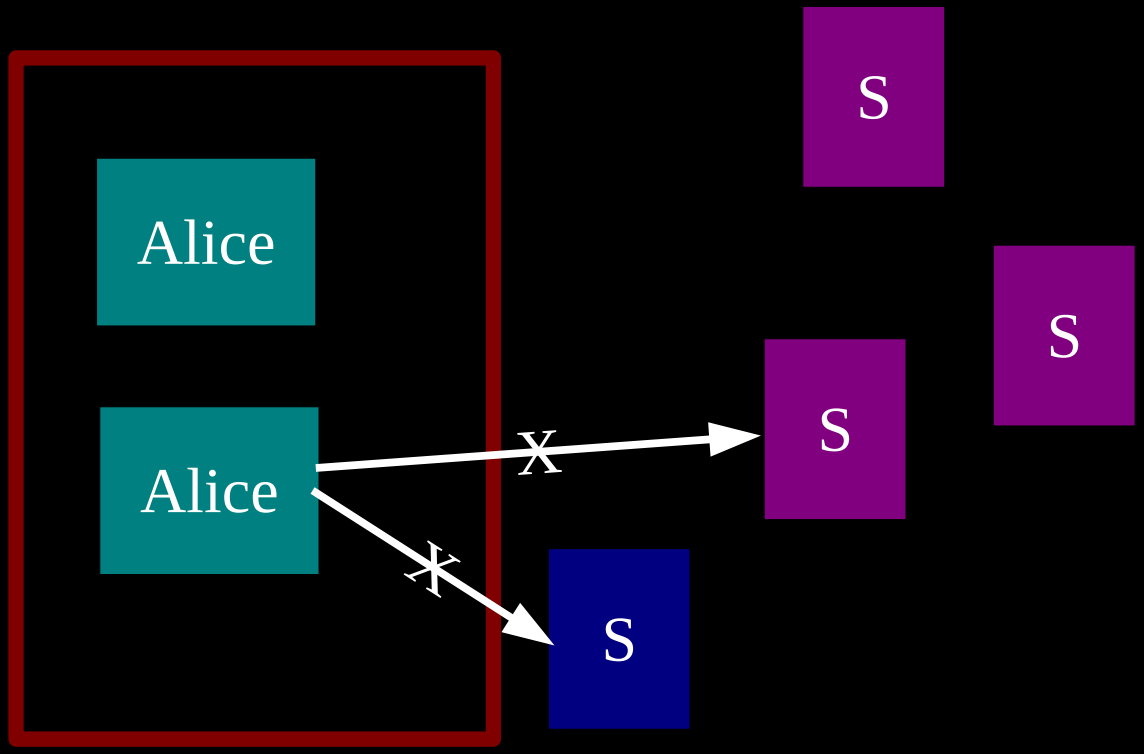
Distributing Tor

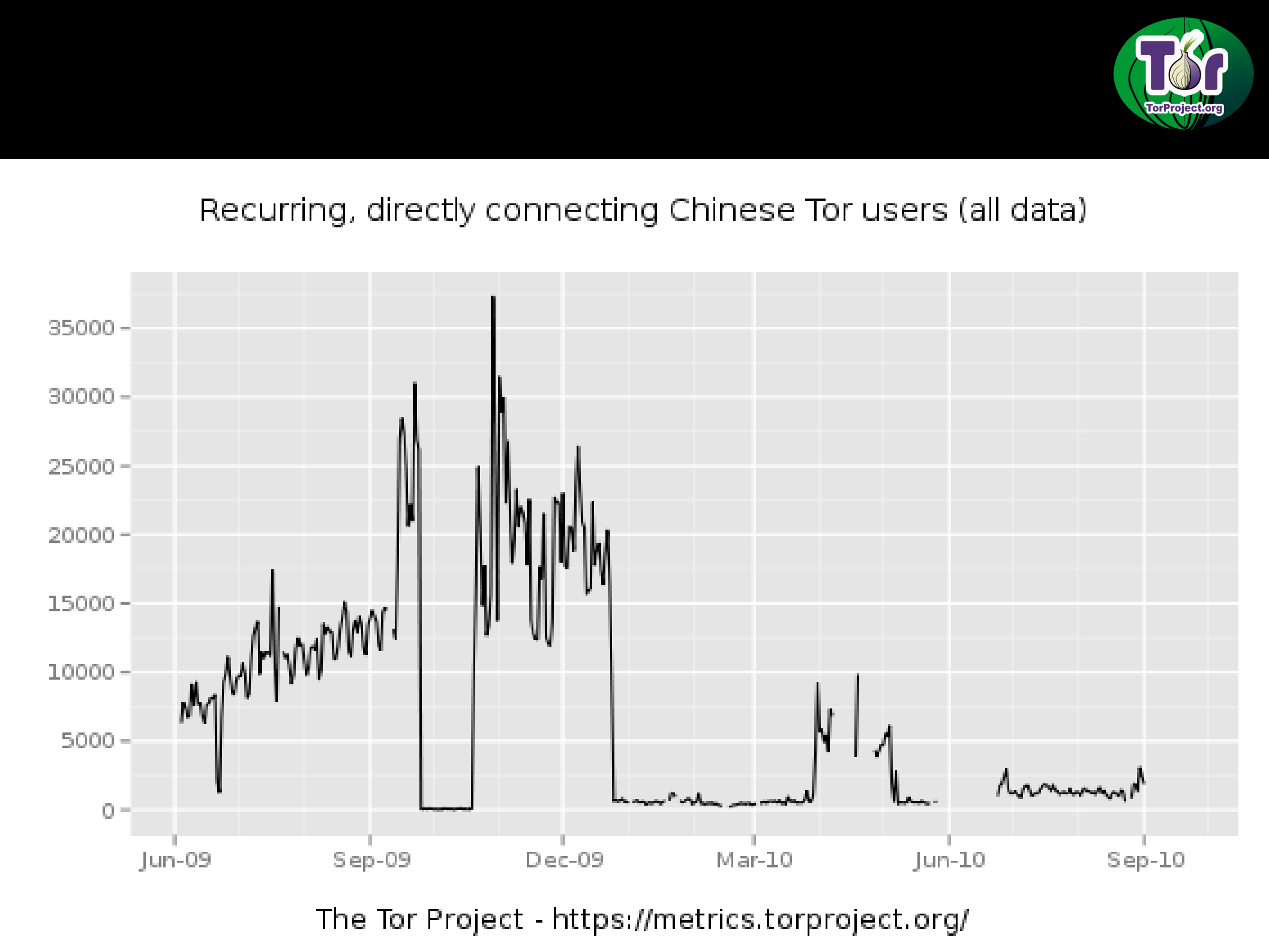
- Gettor
  - Fetch Tor via email, irc, IM
- Thandy (not yet deployed)
  - Tor's secure updater
  - Netinstall capabilities
  - Update over Tor

The basic Tor design uses a simple, centralized directory protocol...



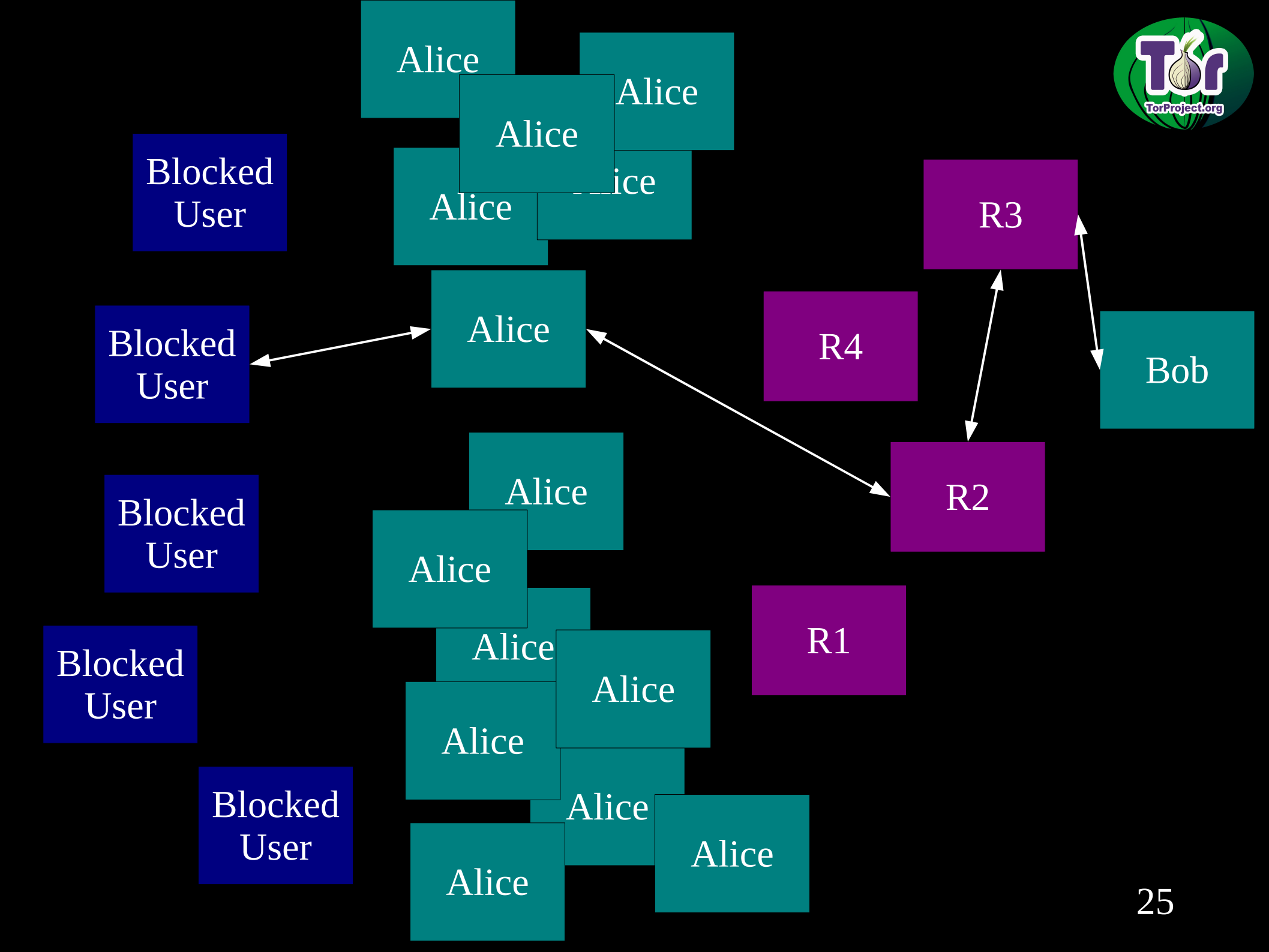
… which is quite easy to block.




Recurring, directly connecting Chinese Tor users (all data)
35000
30000
25000
20000
15000
10000
5000
0
Jun-09
Sep-09
Dec-09
Mar-10
Jun-10
Sep-10
The Tor Project - https://metrics.torproject.org/

Solution: Bridges

- Provide entry points into the Tor network
- Having one working bridge is enough
- Discovery of a few bridges should be easy, enumeration should be hard
- Make sure bridges can be untrusted

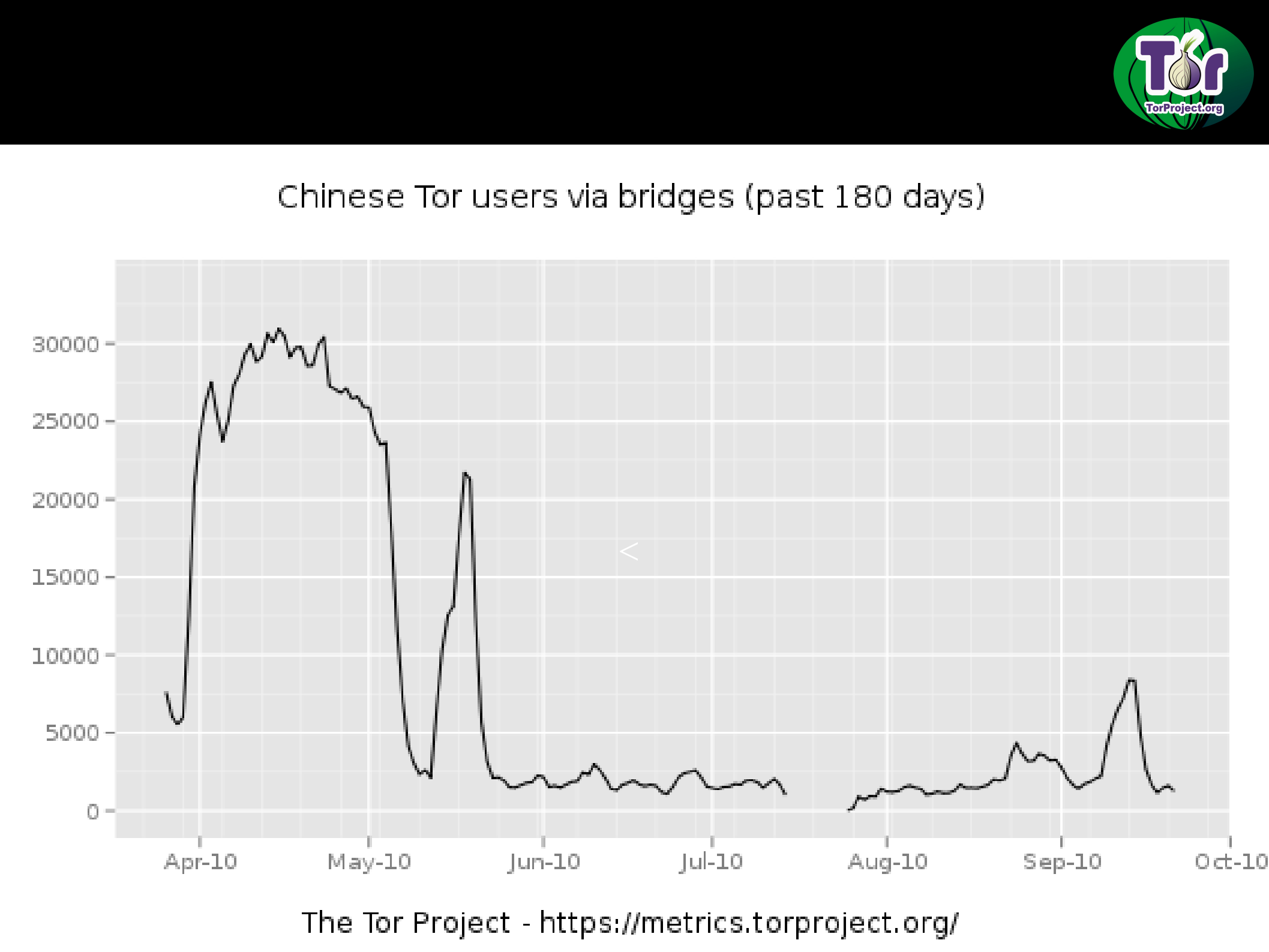

Alice
Alice
Alice
Alice
Alice
Blocked User
Blocked User
Blocked User
Blocked User
Blocked User
Alice
Alice
Alice
Alice
Alice
Alice
Alice
R3
R4
R2
R1
Bob

Important circumvention lessons

- Pick a tool with a diverse set of users
- Make sure your tool provides privacy
- Carefully check what your tool promises
- Use an open, peer-reviewed tool
- The tool should make updating easy
- and it needs to provide good connectivity (bearable latency, low variance in speed)

Circumvention Community

- Many tools make a big splash in the press
  - Censors need to feel in control; publicity removes the appearance of control
- Increase community diversity
  - Make it less suspicious to use a circumvention tool
- Funding needs to be diverse, too


Chinese Tor users via bridges (past 180 days)
30000
25000
20000
15000
10000
5000
0
Apr-10
May-10
Jun-10
Jul-10
Aug-10
Sep-10
Oct-10
The Tor Project - https://metrics.torproject.org/

China

- Very precise blocking
- Thousands of “real humans” work for the censors, so relying on Turing tests alone is pointless
- Bridge churn needs to increase

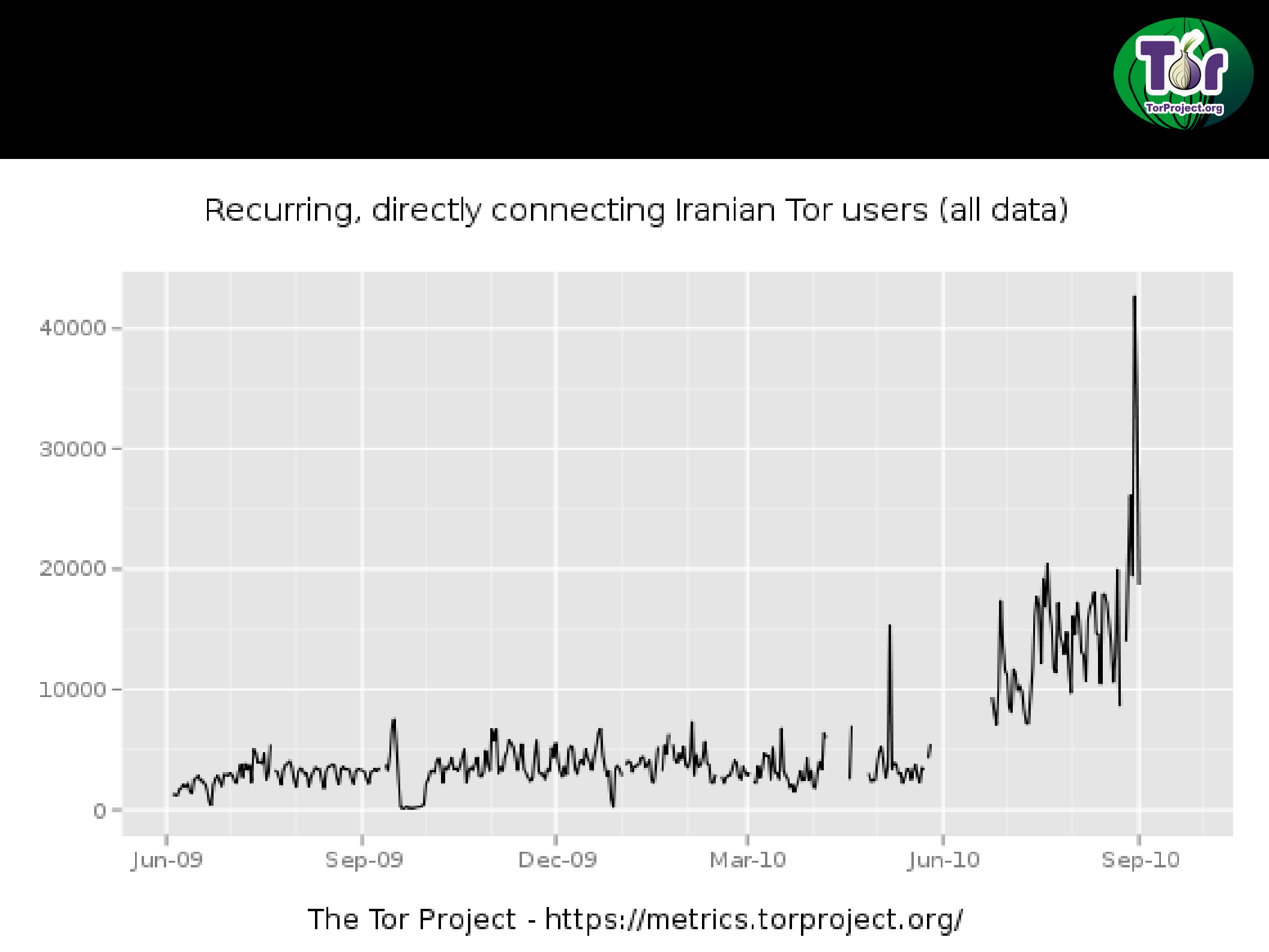
China

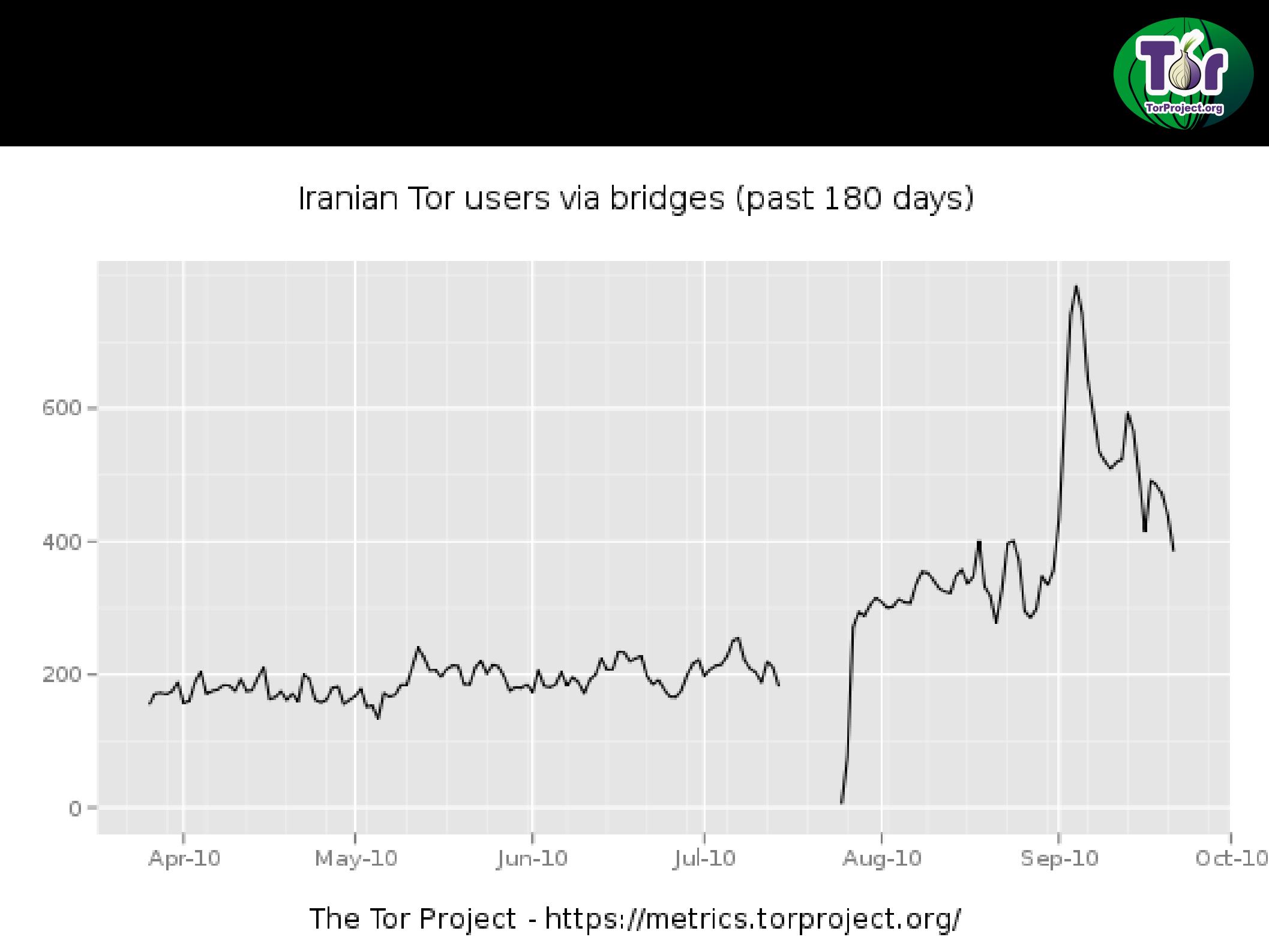
- Currently we see mostly IP:Port based blocks
- Blocks are revoked after some time
- If you use many ports, your packets get nullrouted – you lose connectivity to China, too

- We haven't seen active mitm attacks
- China probably can't afford to just disable all SSL

Iran

- Tor still works without a bridge, but more people should probably use bridges
- Distributing Tor from friend to friend (USB stick) is the most common distribution strategy
- Iran has the ability to throttle all encrypted connections country-wide


Recurring, directly connecting Iranian Tor users (all data)
40000
30000
20000
10000
0
Jun-09
Sep-09
Dec-09
Mar-10
Jun-10
Sep-10
The Tor Project - https://metrics.torproject.org/


Iranian Tor users via bridges (past 180 days)
600
400
200
0
Apr-10
May-10
Jun-10
Jul-10
Aug-10
Sep-10
Oct-10
The Tor Project - https://metrics.torproject.org/

Other countries

- Many countries block our website
- Usually not very sophisticated and easily detected
  - DNS based blocks
  - Filter based on string matching in headers
  - Proxy cascades

- **Most use tools manufactured by western companies to oppress their citizens!**

What can you do to help?

Please run a bridge!

Maybe two? Or even three.

- Low bandwidth or dynamic IP addresses are OK
- Distribute the bridge address yourself or allow us to help

How do we distribute Bridges?

- Bridges advertise their IP address and port
- Available bridges are placed into different pools
  - Web: https://bridges.torproject.org
  - Email: bridges@torproject.org
  - Given to semi-trusted activists
- Future improvements:
  - Measure performance of different pools
  - Don't give out blocked bridges

What we learned

- Private bridges work (basically) everywhere (exception: places that block/mitm all ssl)
- China is (currently) the only place good at blocking bridges
- Most countries don't use very sophisticated blocking schemes – don't cause a big fuzz and you're OK

What's next

- We need to get better about realizing that a bridge has been blocked; and need to adjust our distribution strategies
- Make it easier to become a bridge
- Improve our metrics so we can react to knew developments more quickly

Questions

???