Tor: a quick overview (How Twitter can help)

Jacob Appelbaum
The Tor Project
https://www.torproject.org/

About me:

- Free software hacker (libmsr, blockfinder, etc)
- General human and other animal rights activist
- Founder of Noisebridge
- Cold Boot Attack
- MD5 Considered Harmful Now: Constructing a Rogue CA Certificate
- Cult of the Dead Cow member
- Chaos Computer Club supporter
- EFF supporter
- Tor Project Developer

Tor: Big Picture

- Freely available (Open Source), unencumbered.
- Comes with a spec and full documentation: Dresden, Aachen, Yale groups implemented their own compatible Java Tor clients; researchers use it to study anonymity.
- 2000 active relays, 250,000+ active users, >3Gbit/s.
- Official US 501(c)(3) nonprofit. Seven funded developers, dozens more dedicated volunteers.
- Funding from U.S. Naval Research Lab, Electronic Frontier Foundation, Voice of America, Human Rights Watch, NLnet, Google, ...you?

Who uses Tor?

- Normal people use Tor
- Bloggers use Tor
- Militaries use Tor
- Journalists and their audience use Tor
- Law enforcement officers use Tor
- IT professionals use Tor
- Activists and whistleblowers use Tor
- High and low profile people use Tor
- Business executives use Tor

Anonymity isn't just wishful thinking...

“You can't prove it was me!”

“Promise you won't look!”

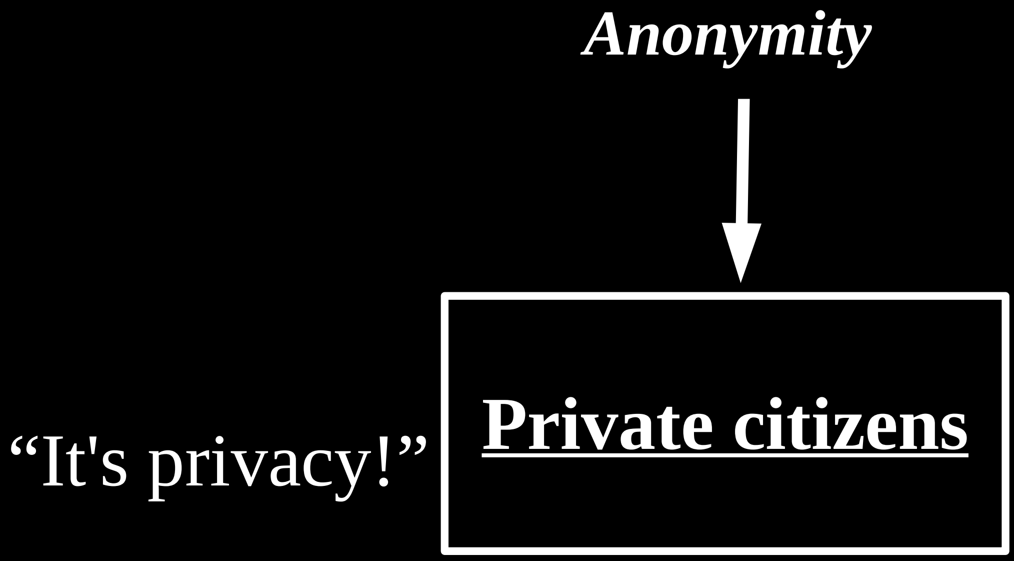
“Promise you won't remember!”

“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.

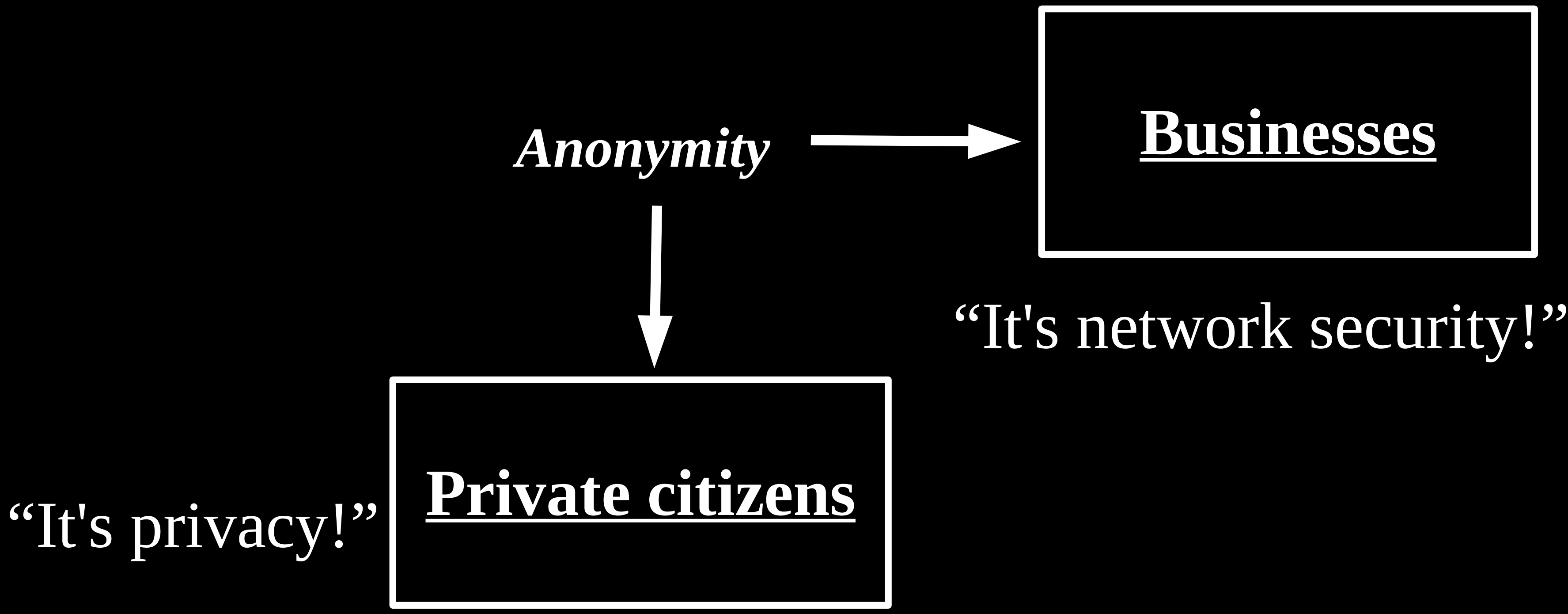


Anonymity

“It's privacy!”

Private citizens

Anonymity serves different interests for different user groups.



Anonymity

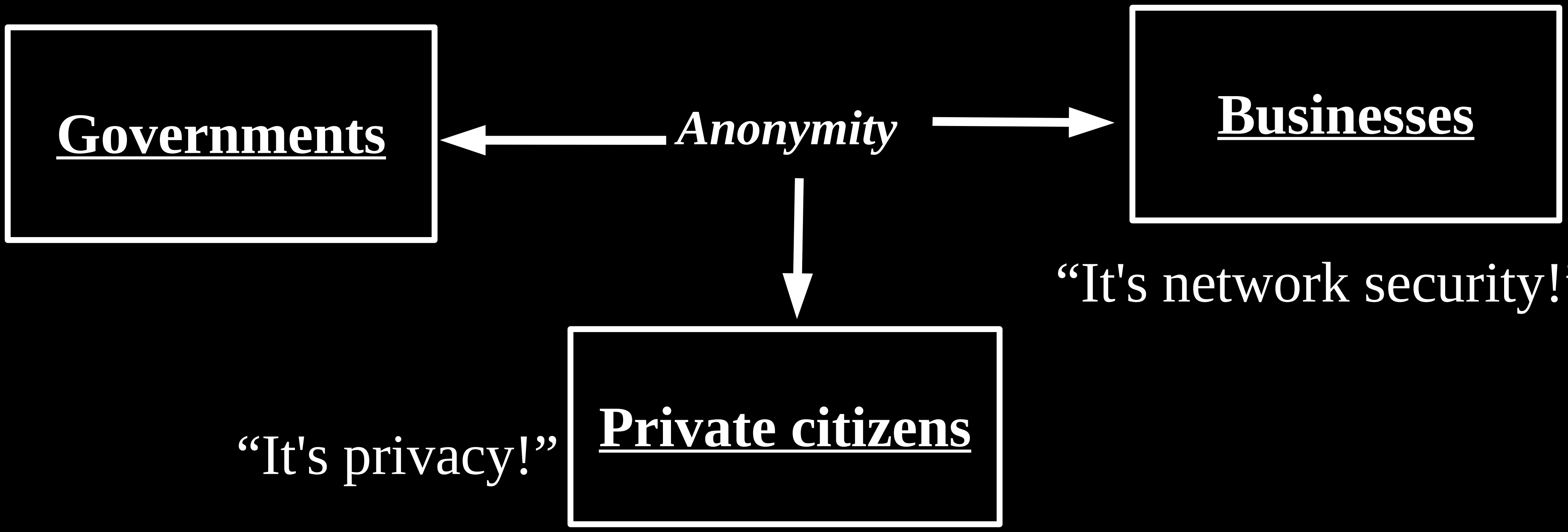
Businesses

“It's network security!”

Private citizens

“It's privacy!”

Anonymity serves different interests for different user groups.



“It's traffic-analysis resistance!”

Governments

Anonymity

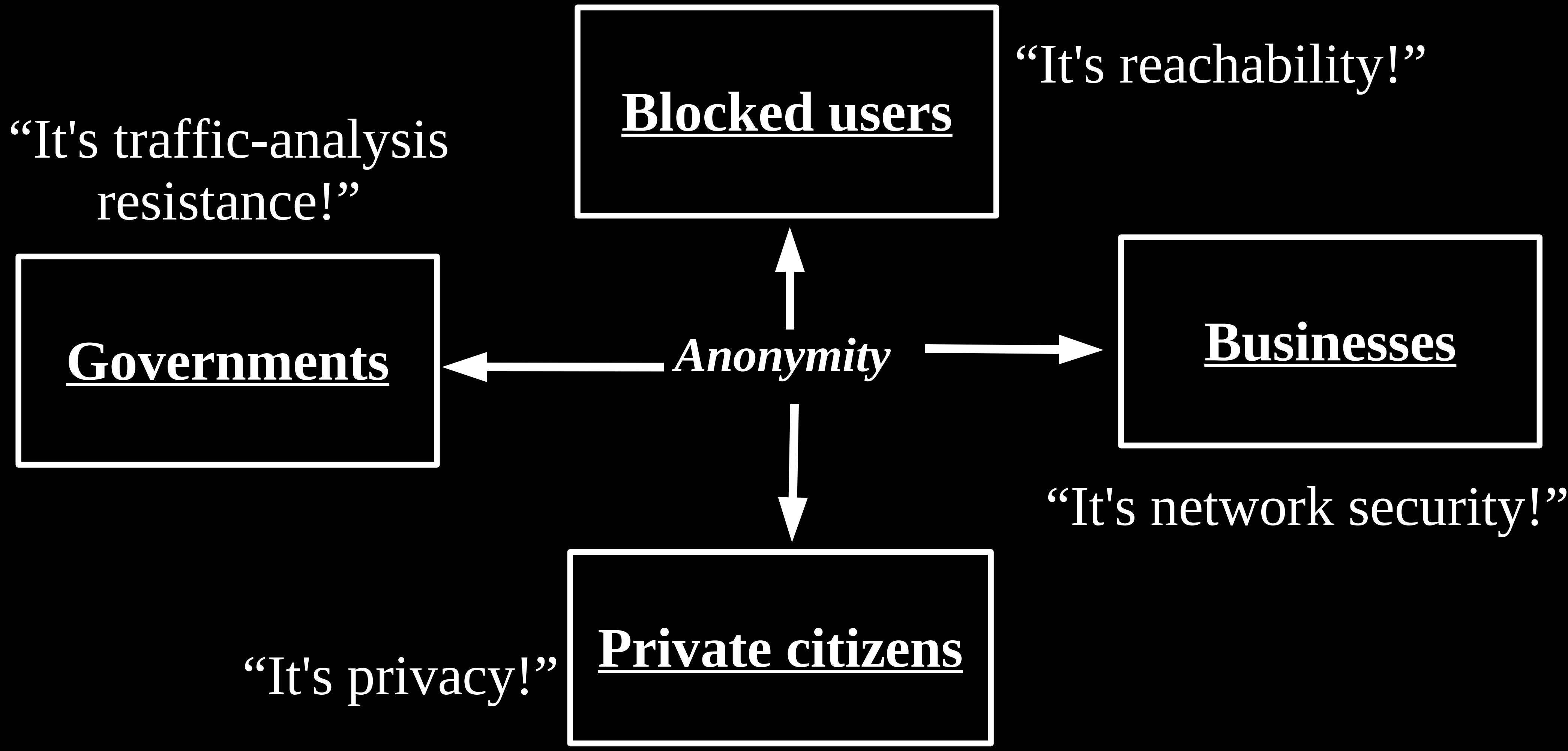
Businesses

“It's network security!”

“It's privacy!”

Private citizens

Anonymity serves different interests for different user groups.



Blocked users

"It's reachability!"

Governments

"It's traffic-analysis resistance!"

Anonymity

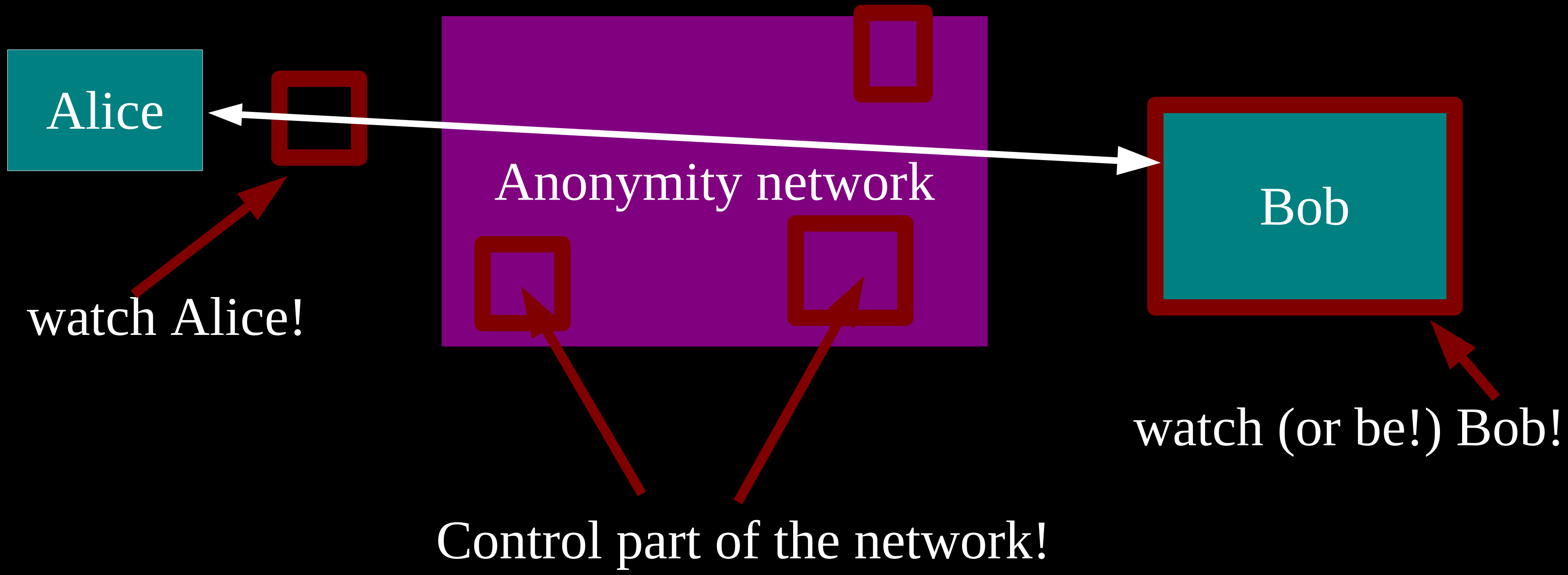
Businesses

"It's network security!"

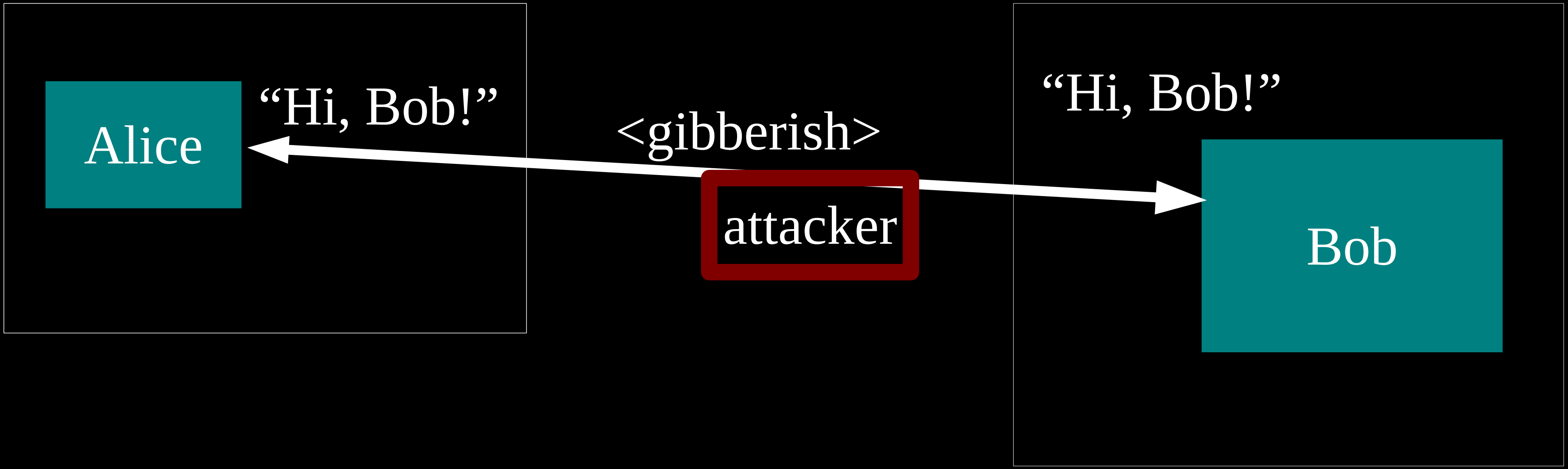
Private citizens

"It's privacy!"

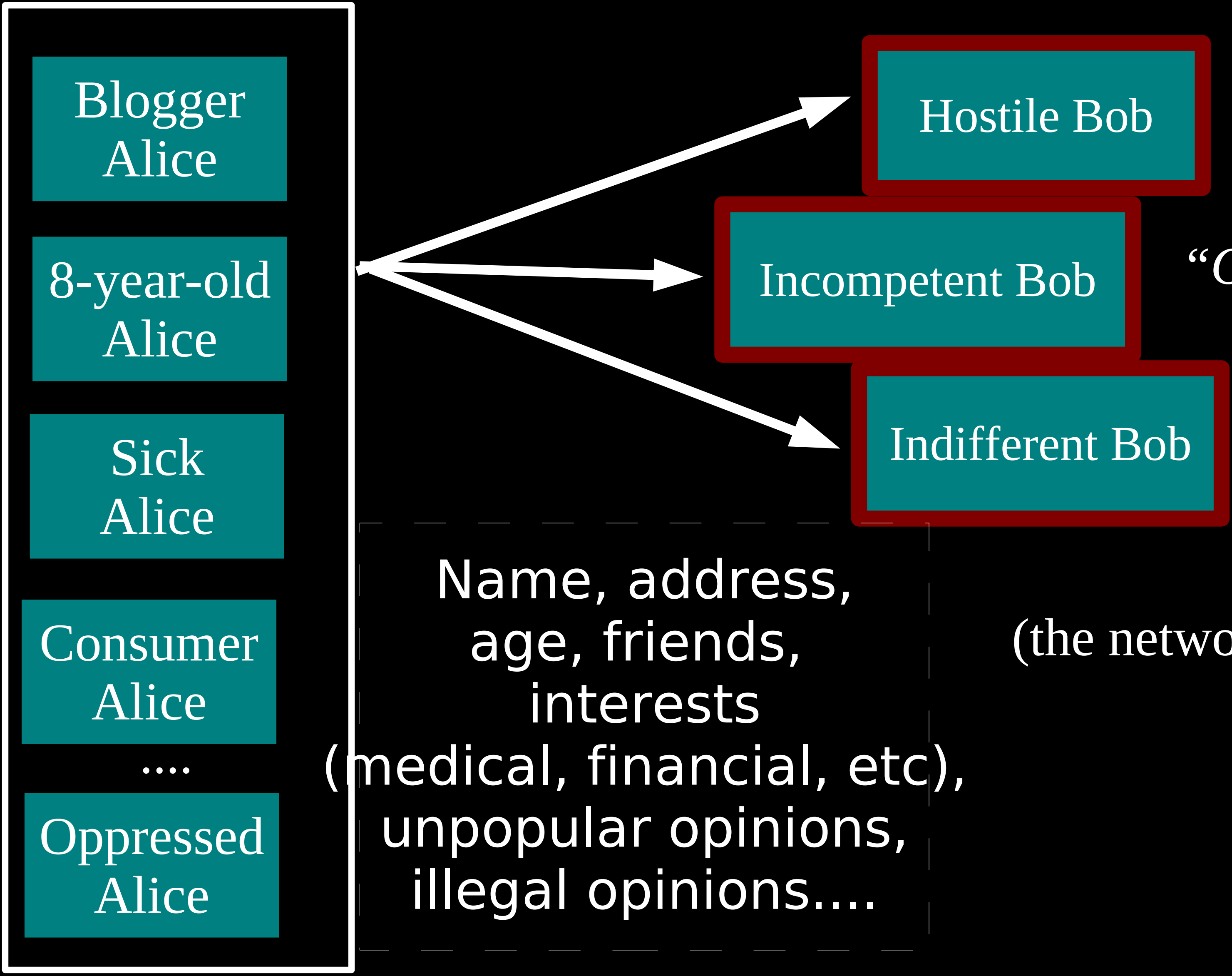
Threat model: what can the attacker do?



Anonymity isn't cryptography: Cryptography just protects contents.



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



Blogger Alice

8-year-old Alice

Sick Alice

Consumer Alice

....

Oppressed Alice

Hostile Bob

Incompetent Bob

Indifferent Bob

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

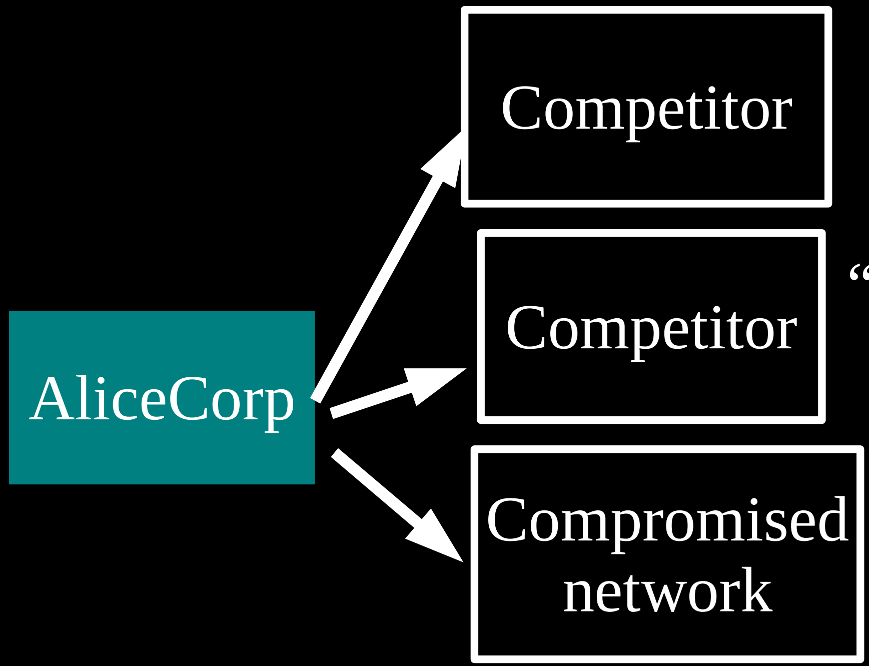
“I sell the logs.”

“Oops, I lost the logs.”

*“Hey, they aren't **my** secrets.”*

(the network can track too)

Businesses need to keep trade secrets.



AliceCorp

Competitor

Competitor

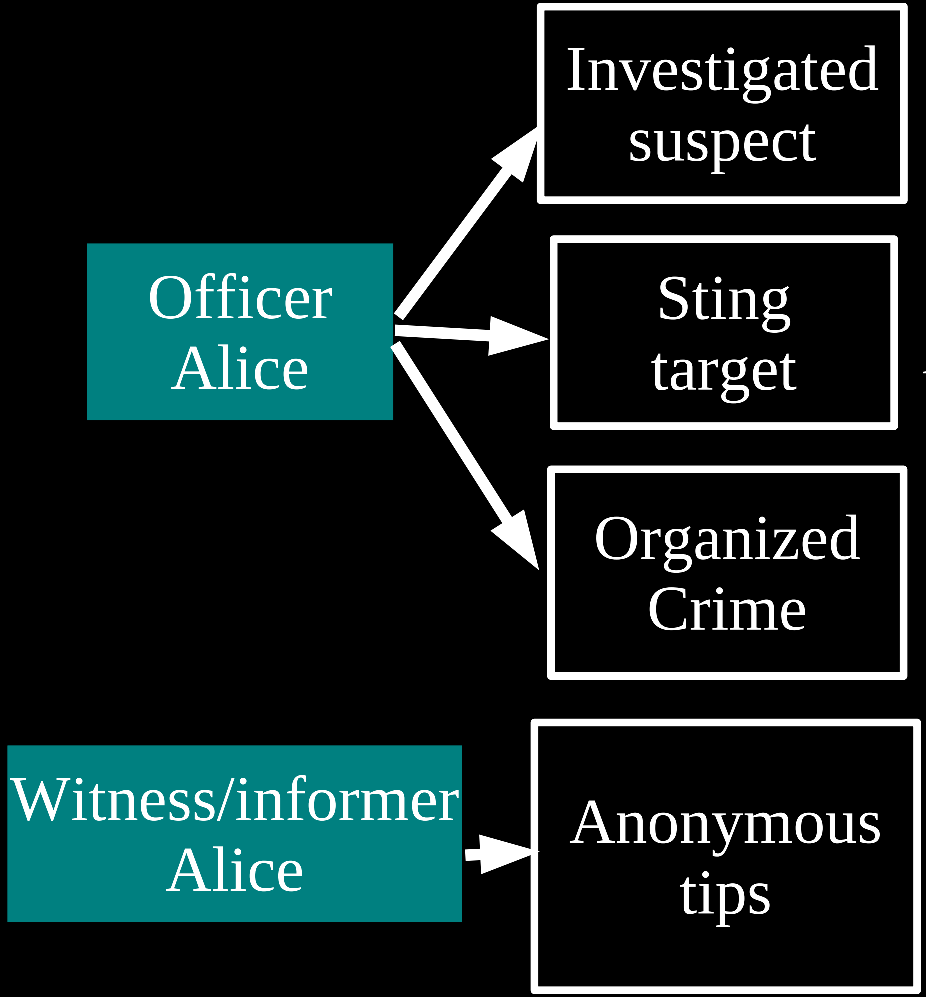
Compromised network

“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

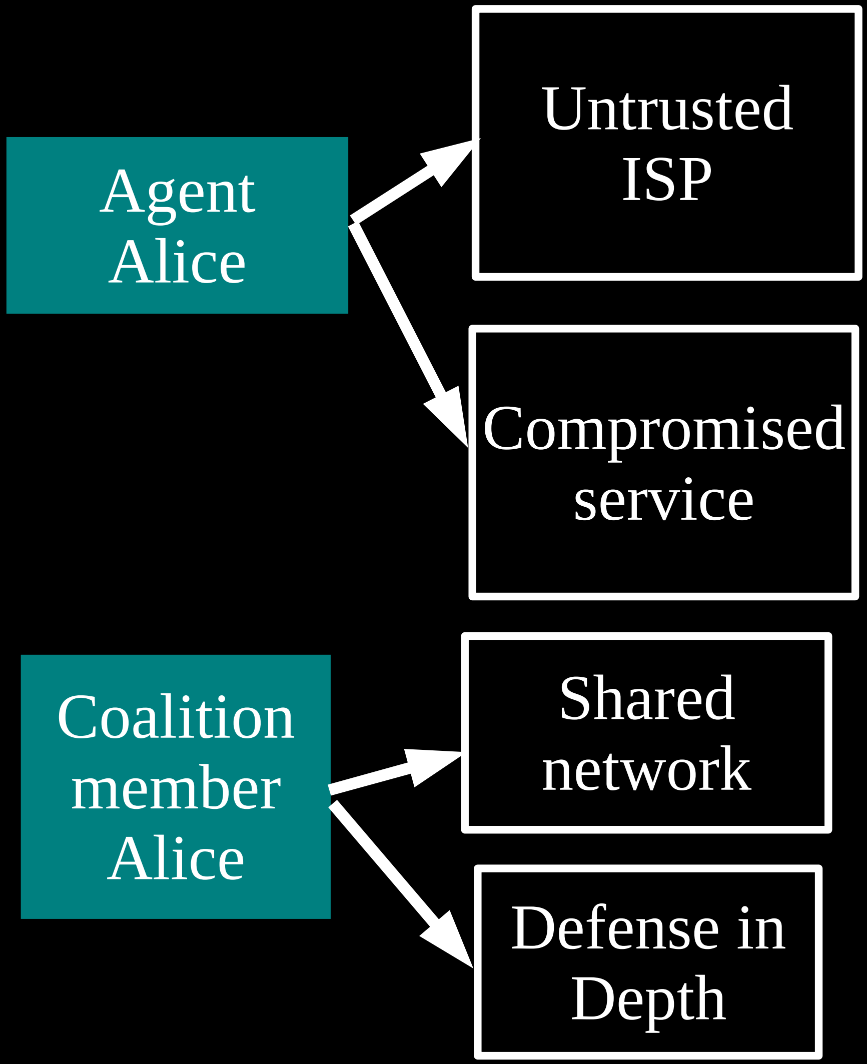
"Is my family safe if I go after these guys?"

Witness/informer Alice

Anonymous tips

"Are they really going to ensure my anonymity?"

Governments need anonymity for their security



Agent Alice

Untrusted ISP

Compromised service

Coalition member Alice

Shared network

Defense in Depth

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

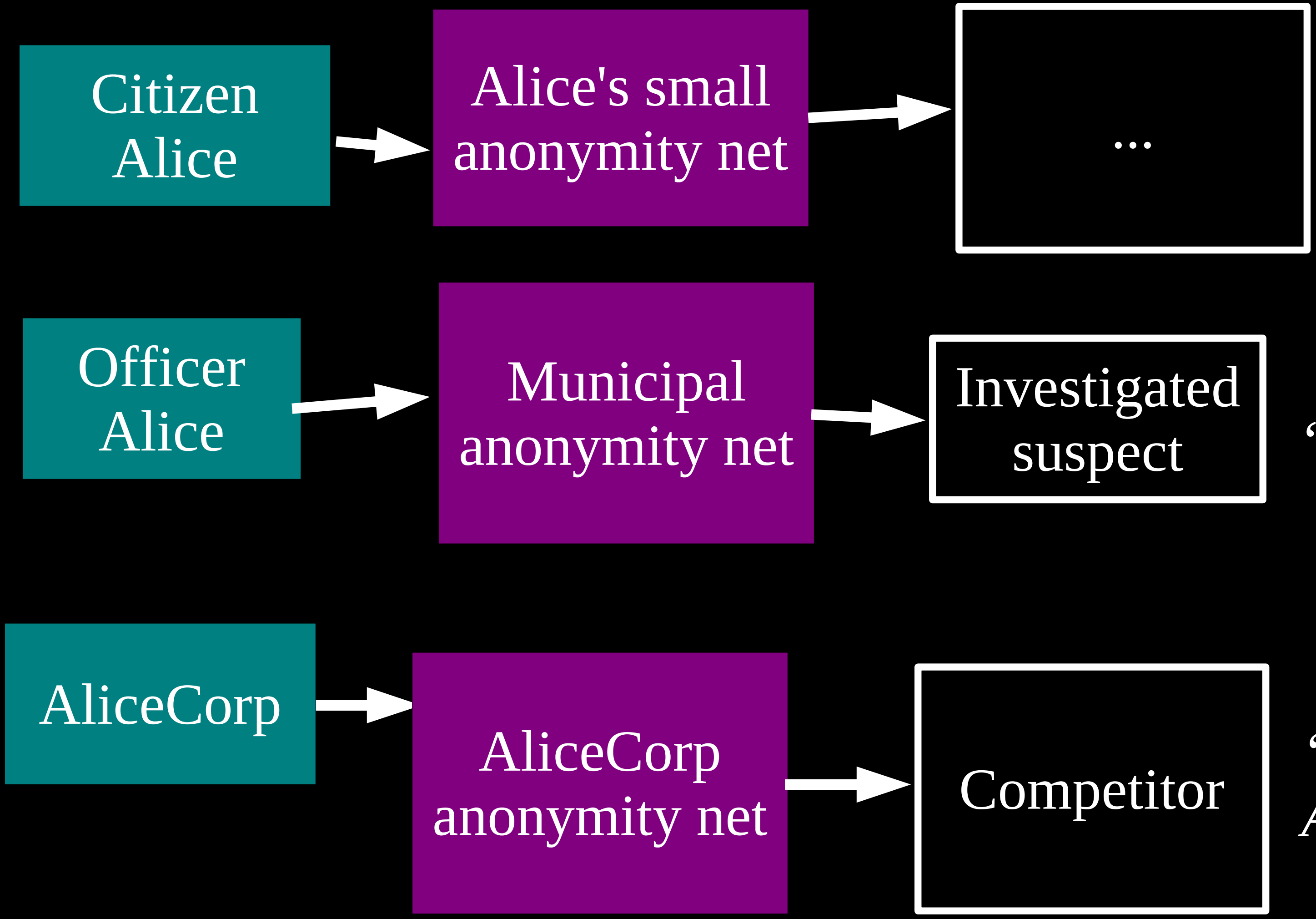
“Somebody in that hotel room just checked his Navy.mil mail!”

“What does *FBI Google for?”*

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

“What about insiders?”

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



Citizen Alice → Alice's small anonymity net → ...

“One of the 25 users on AliceNet.”

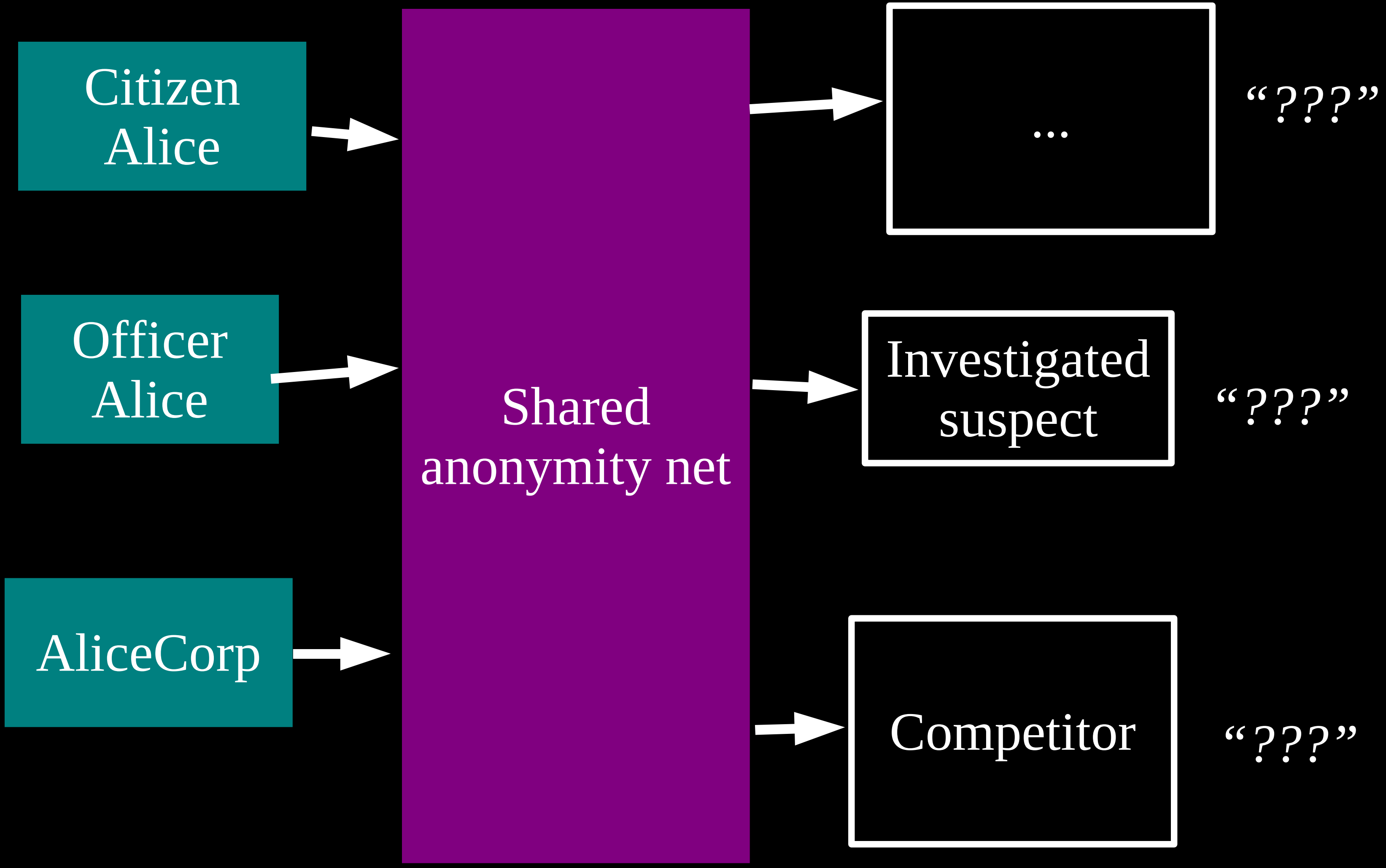
Officer Alice → Municipal anonymity net → Investigated suspect

“Looks like a cop.”

AliceCorp → AliceCorp anonymity net → Competitor

*“It's **somebody** at AliceCorp!”*

… so, anonymity loves company!



Citizen Alice

Officer Alice

AliceCorp

Shared anonymity net

…

"???"

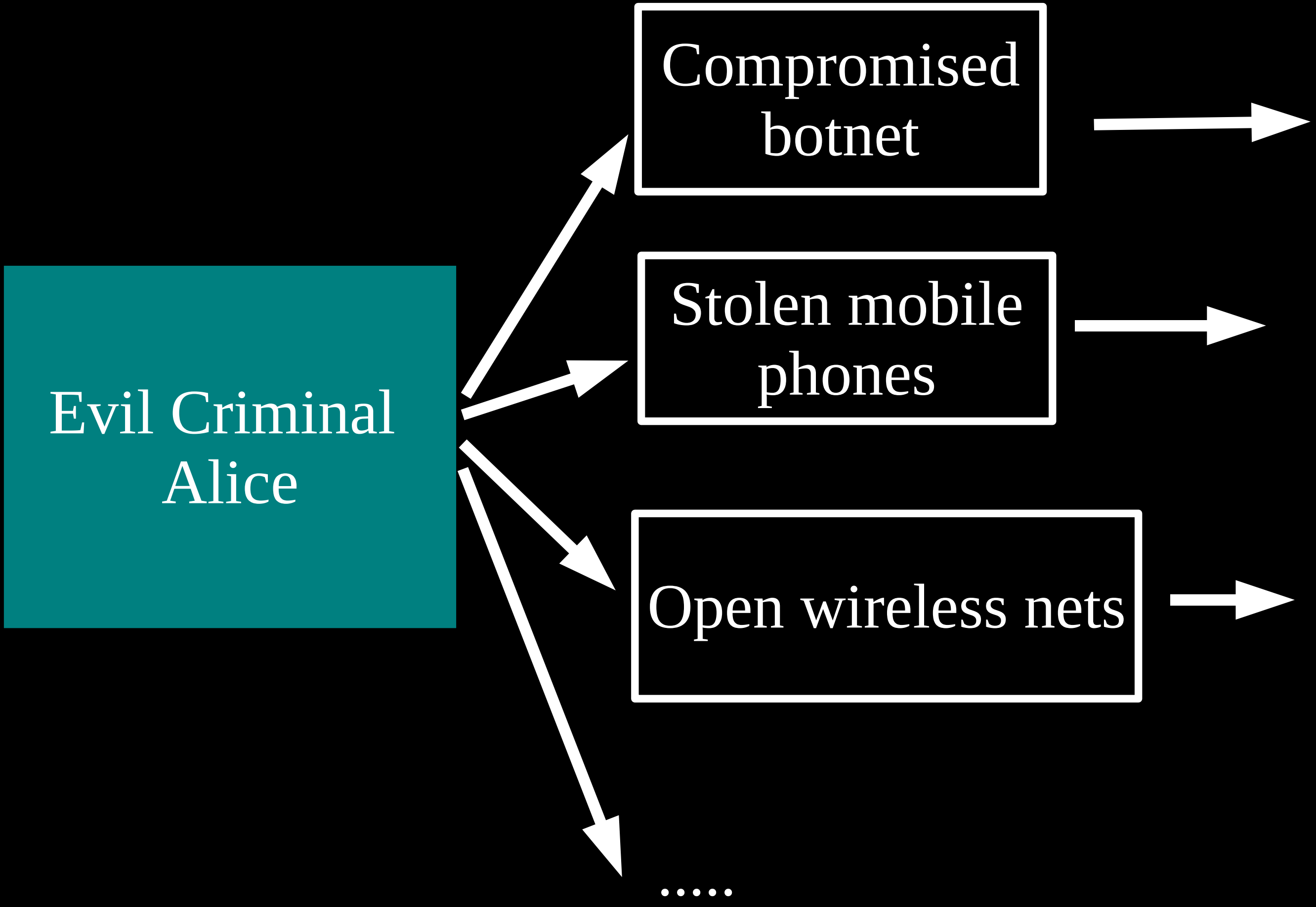
Investigated suspect

"???"

Competitor

"???"

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



Evil Criminal Alice

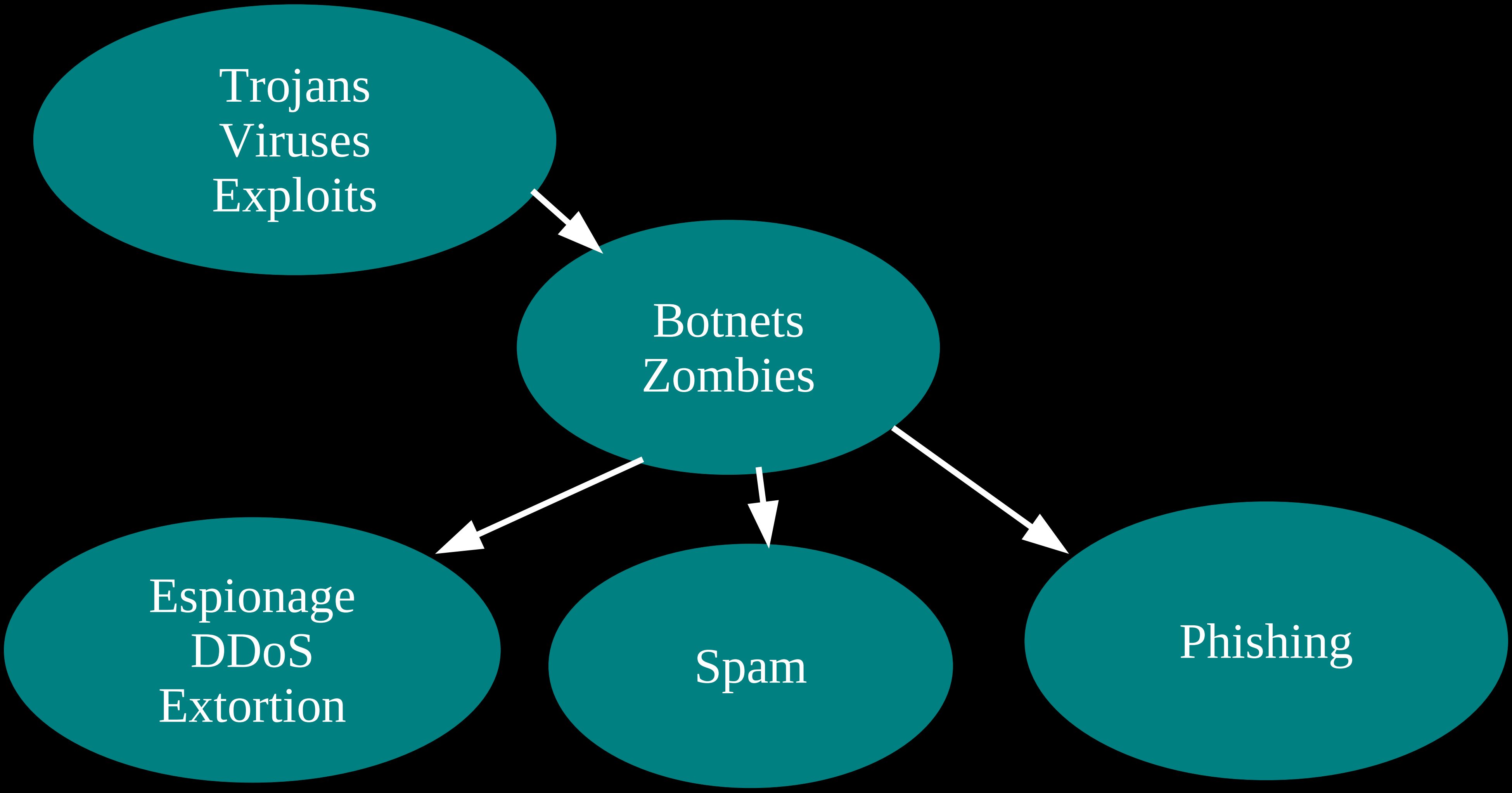
Compromised botnet

Stolen mobile phones

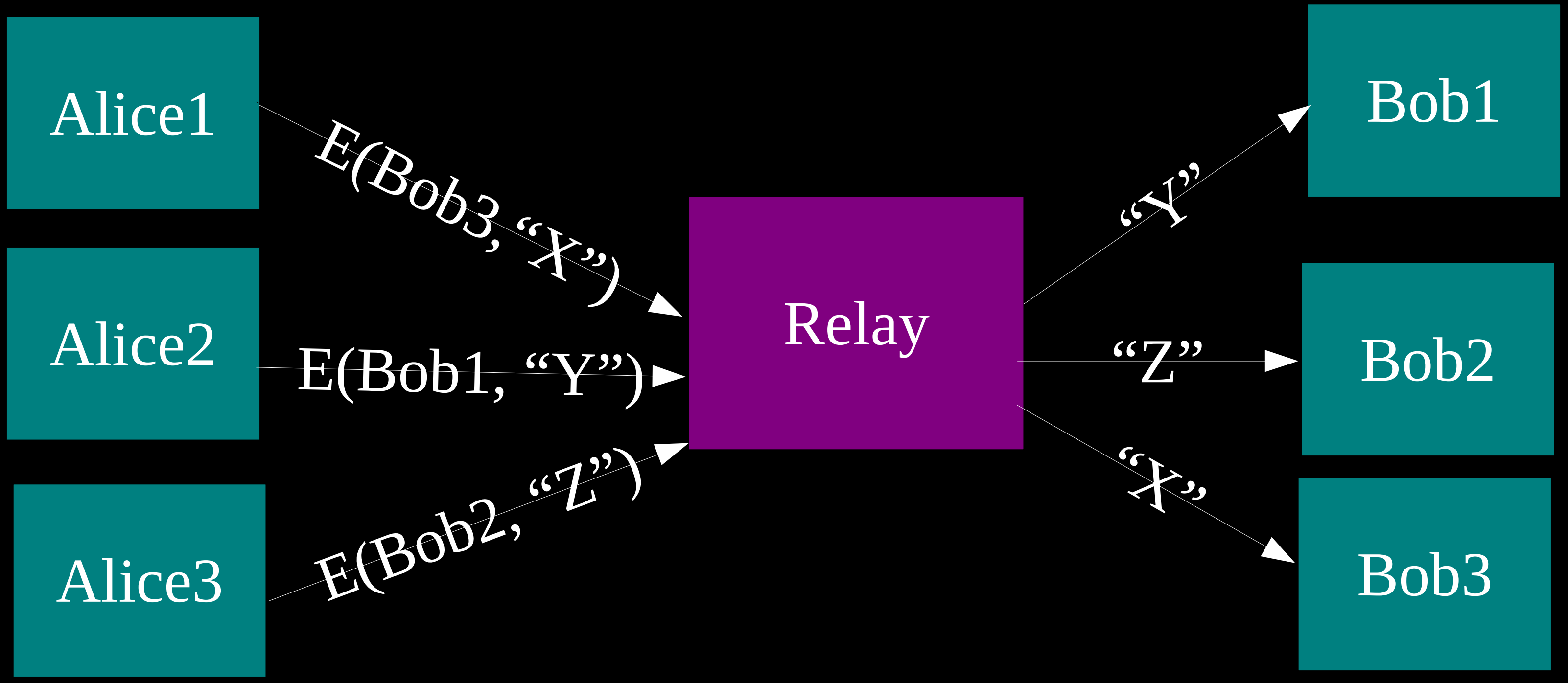
Open wireless nets

.....

Current situation: Bad people on the Internet are doing fine

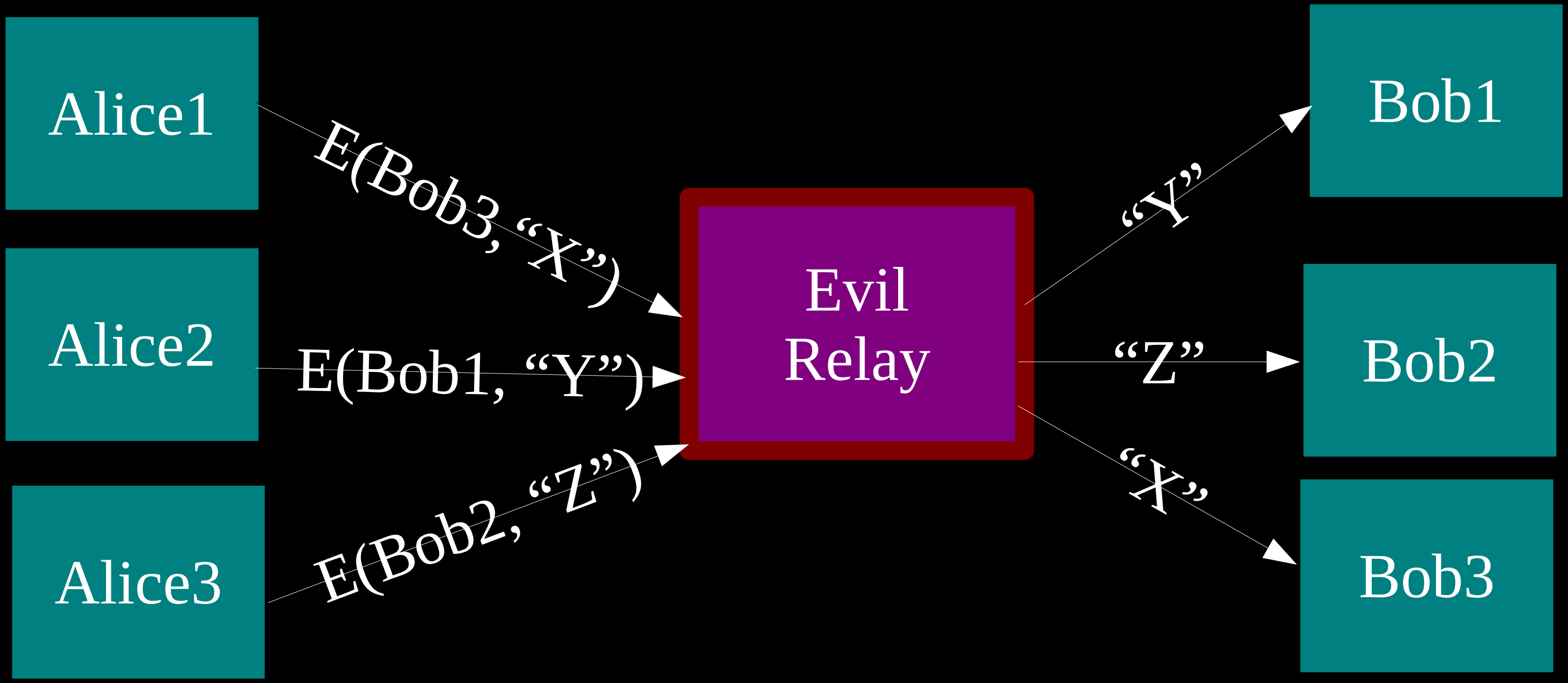


The simplest designs use a single relay to hide connections.

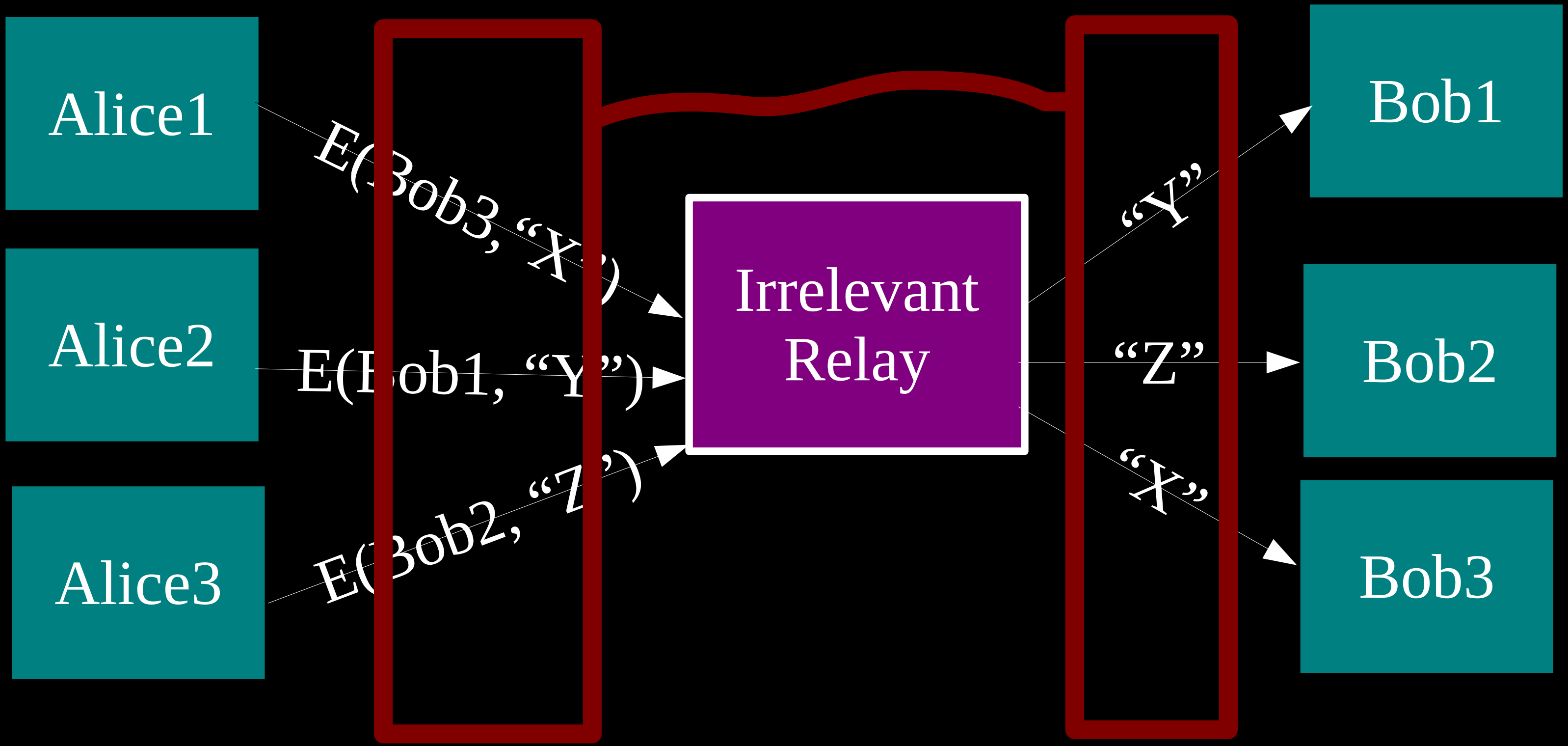


(example: some commercial proxy providers)

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

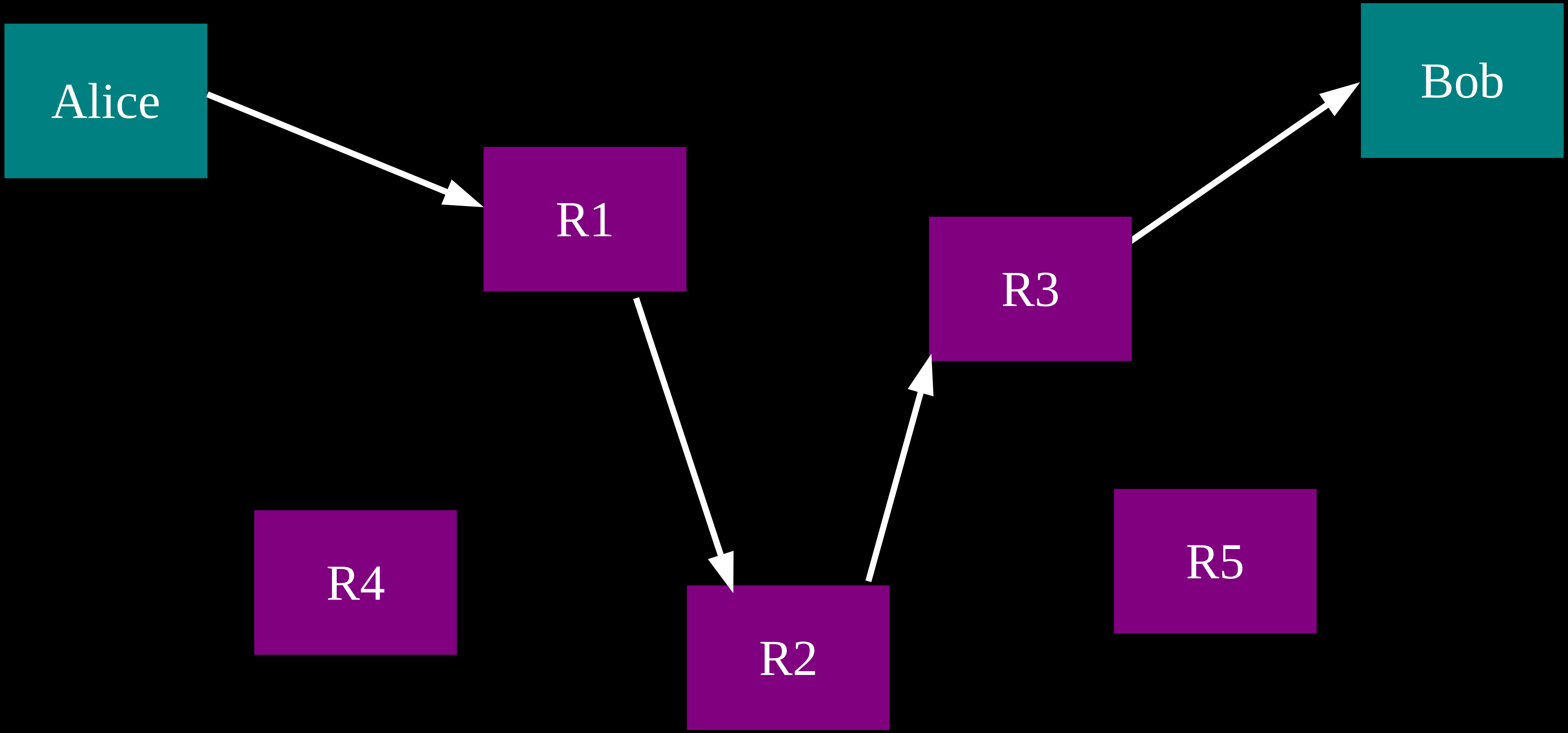


... or a single point of bypass.

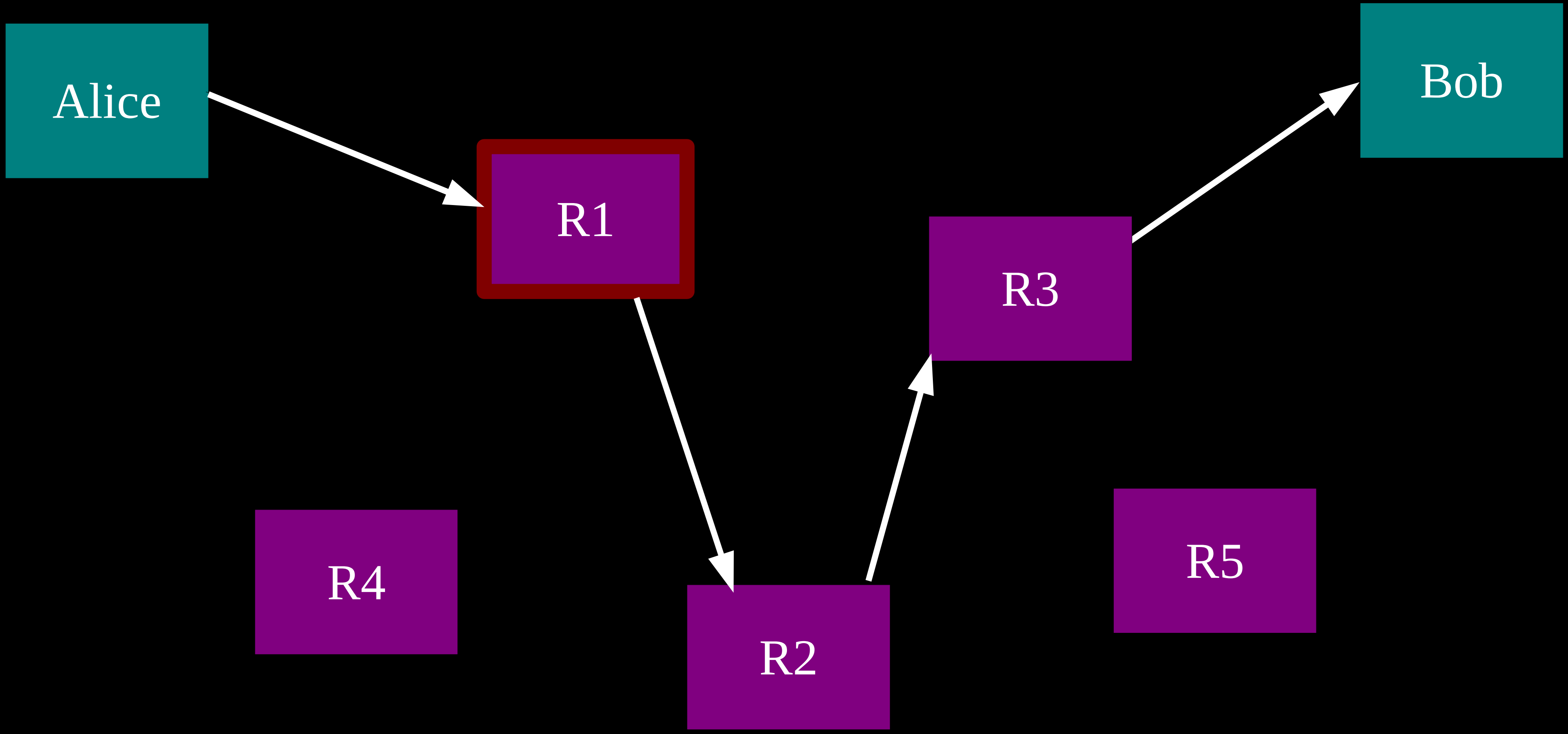


Timing analysis bridges all connections through relay ⇒ An attractive fat target

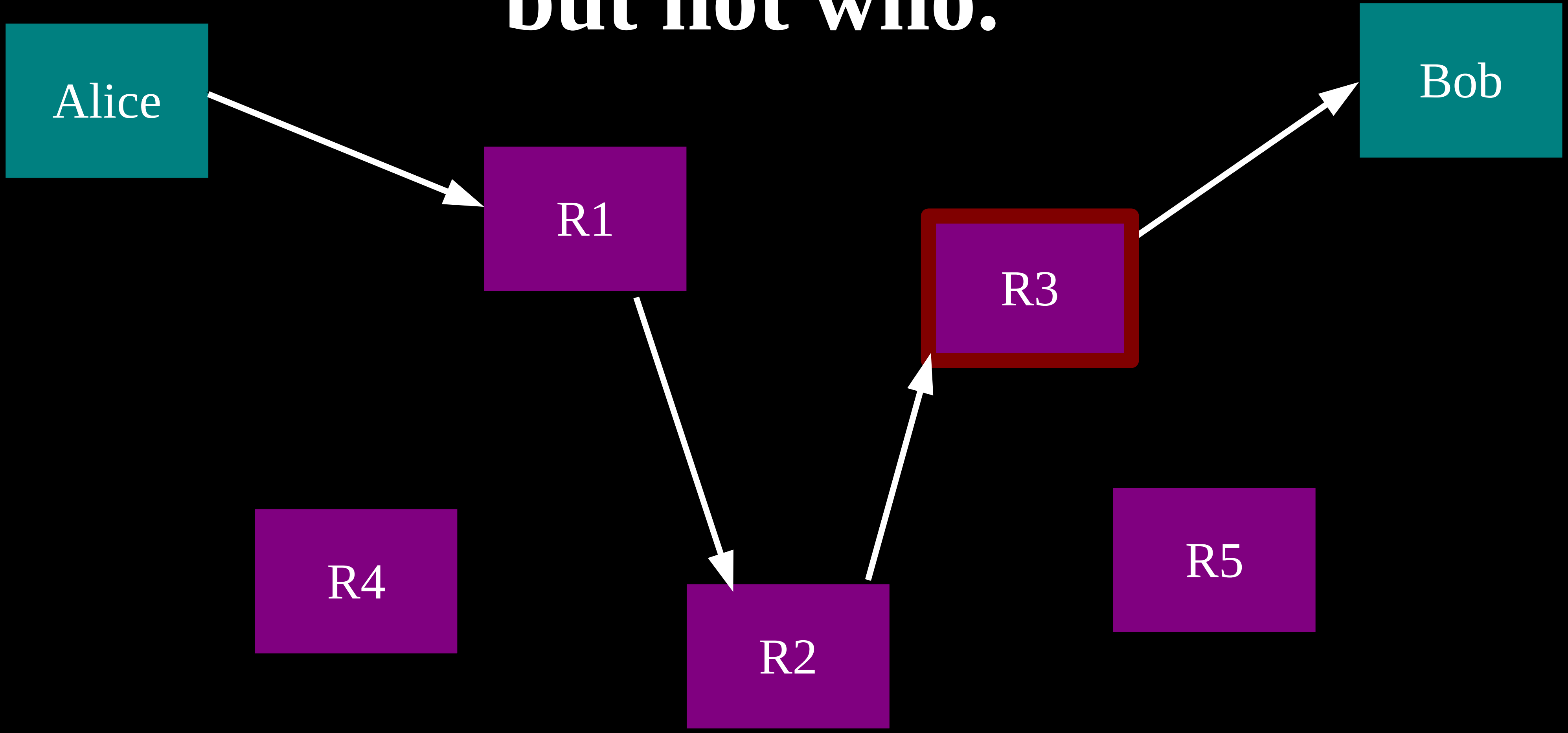
So, add multiple relays so that no single one can betray Alice.



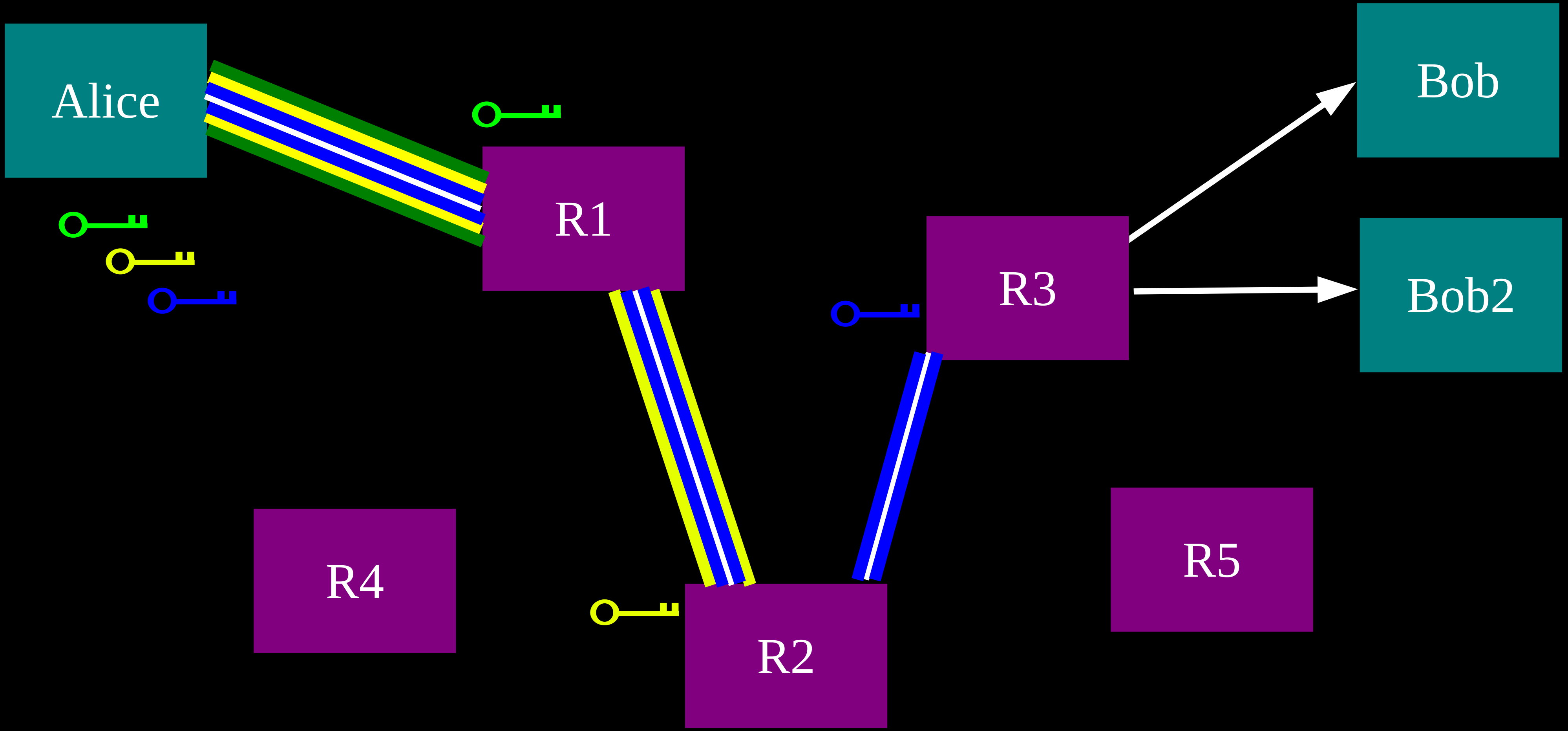
A corrupt first hop can tell that Alice is talking, but not to whom.



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



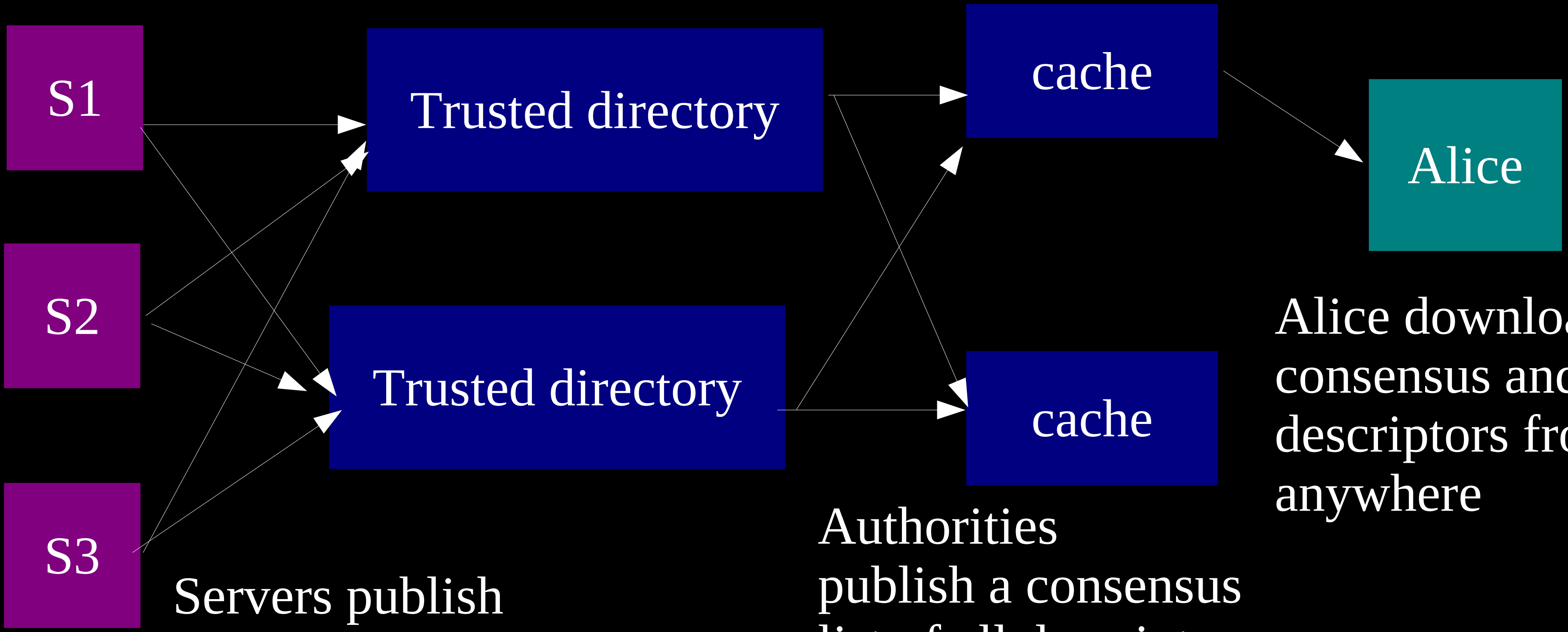
Alice makes a session key with R1
...And then tunnels to R2...and to R3



We're into Privacy by Design!

- Isolate PII information
  - Reduces liability
- Separation of roles
  - Reduces vulnerability
- Discourage logging
- Discourage privacy by *policy*
- Anonymity is an important component of privacy
  - Circumvention generally requires confidentiality
  - Reduce liability and discovery for helpers (bridges, middle relays, etc)

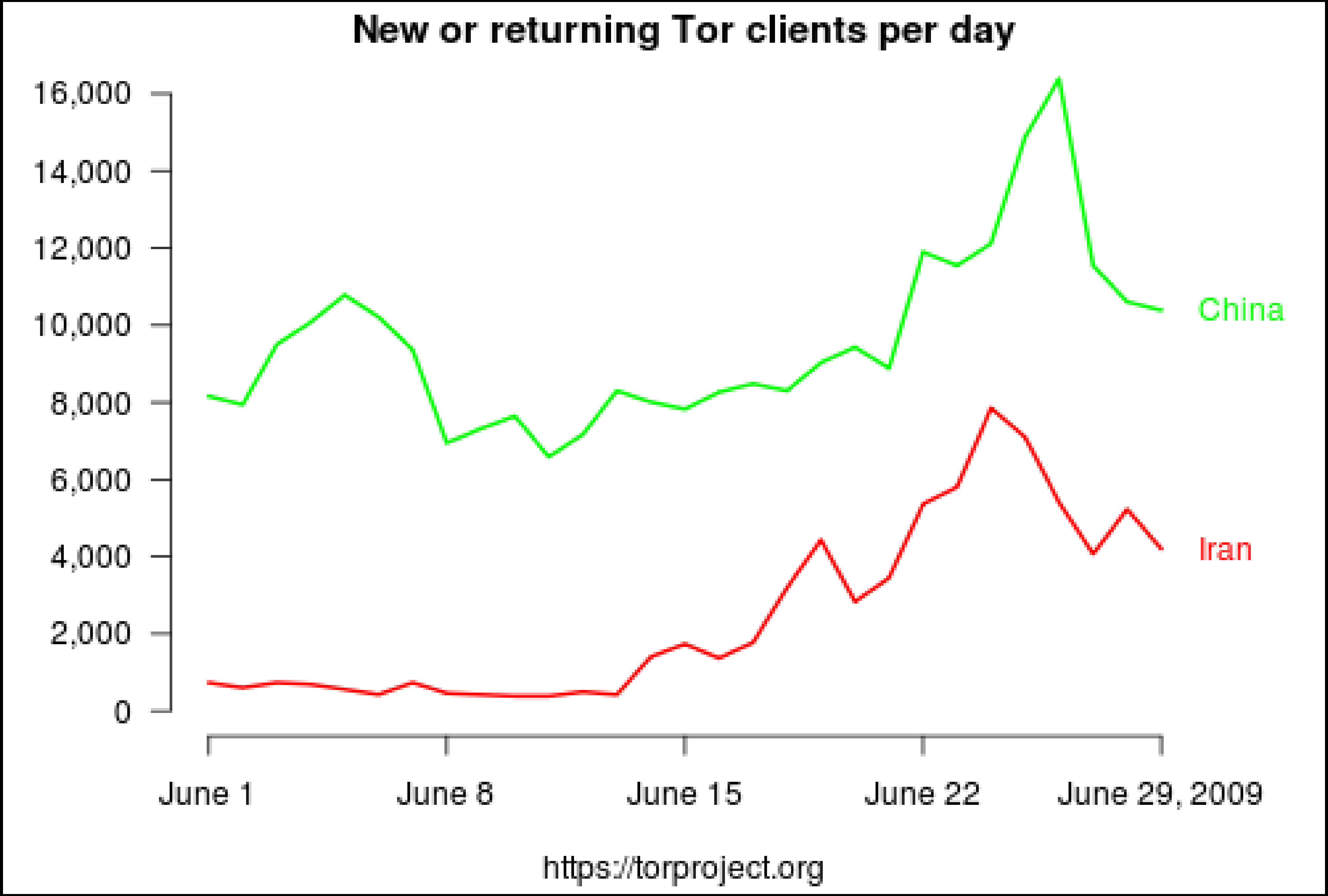
The basic Tor design uses a simple centralized directory protocol.



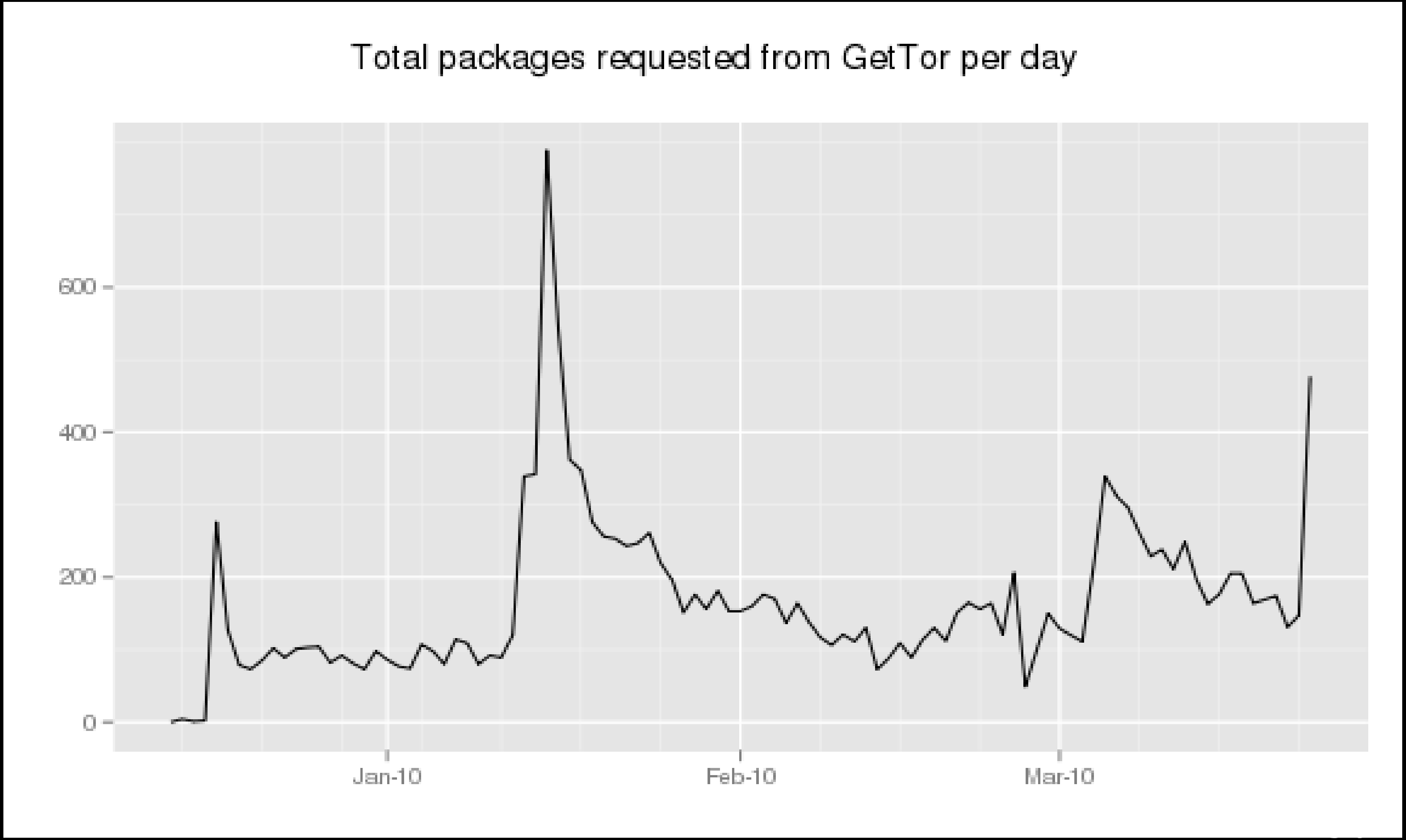
Servers publish self-signed descriptors.

Authorities publish a consensus list of all descriptors

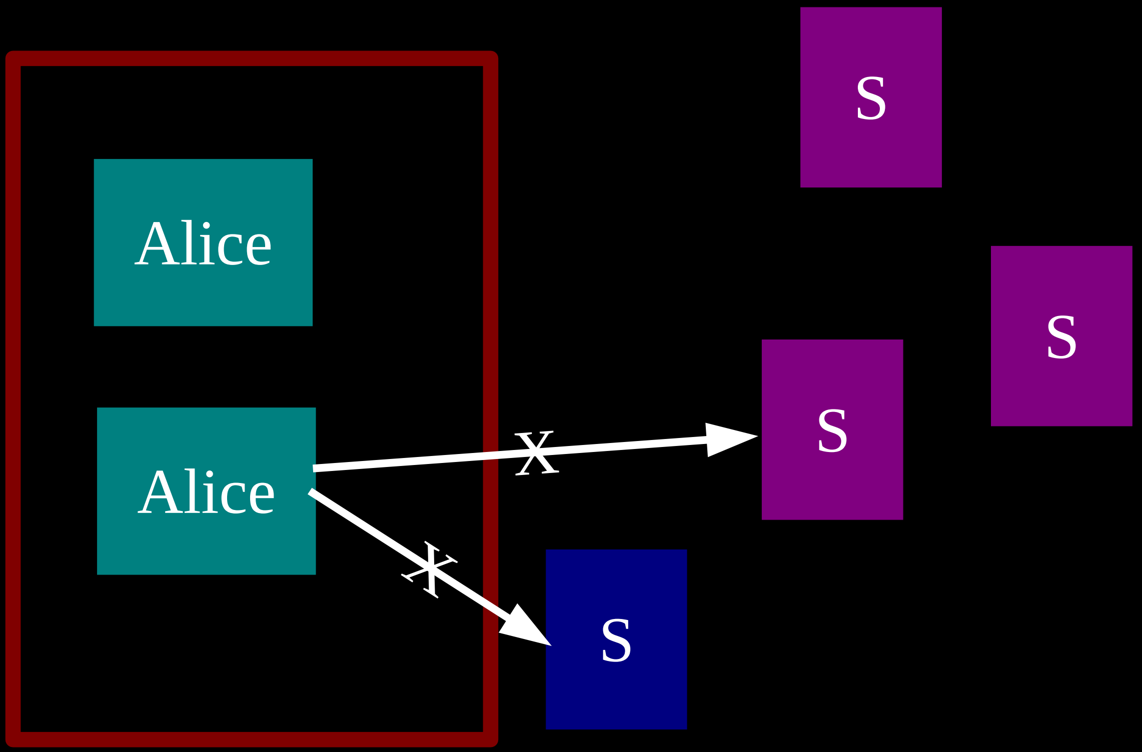
Alice downloads consensus and descriptors from anywhere


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

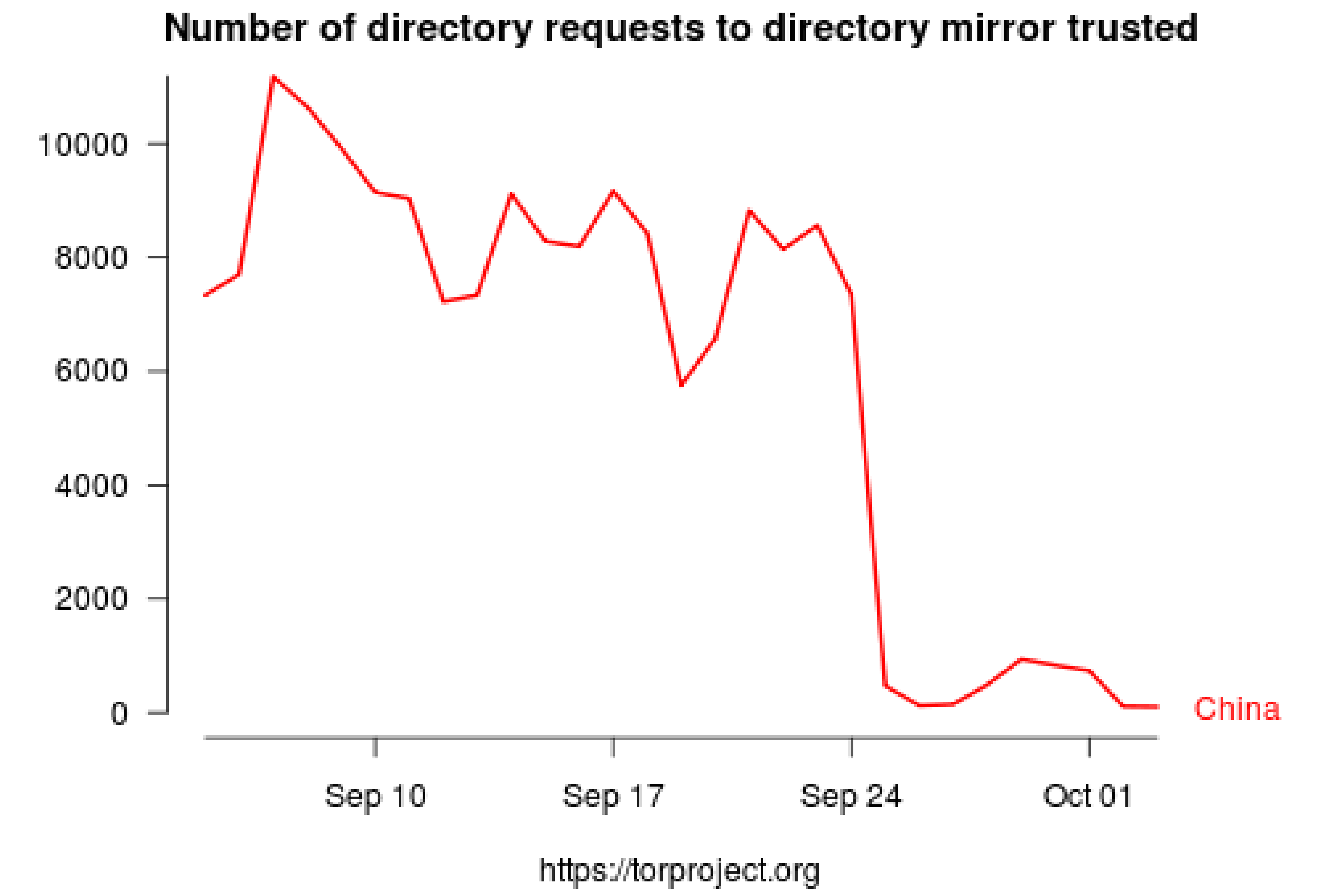
Many firewalls block the Tor website (email resistance)

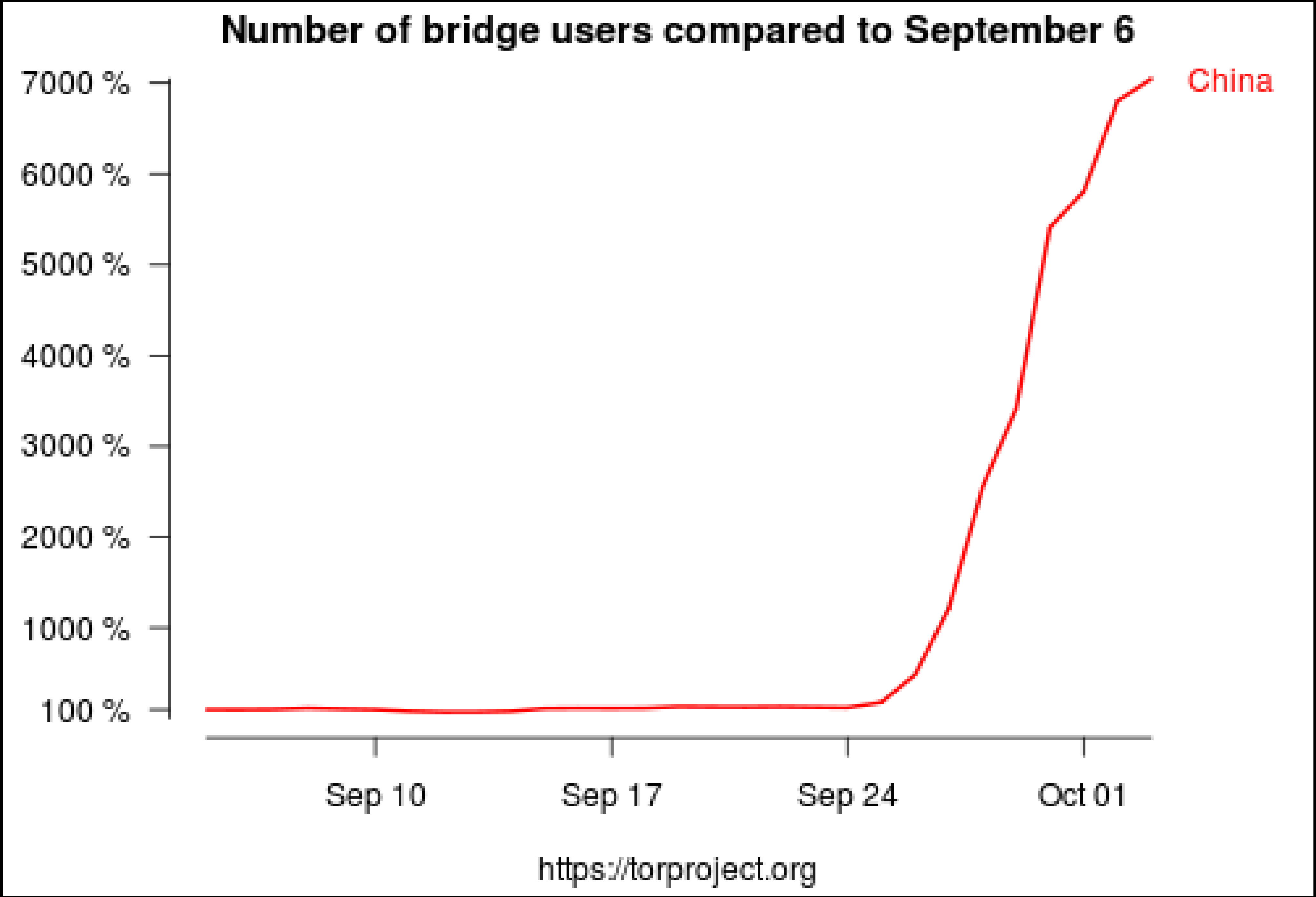


Governments and other firewalls can just block the whole Tor network.



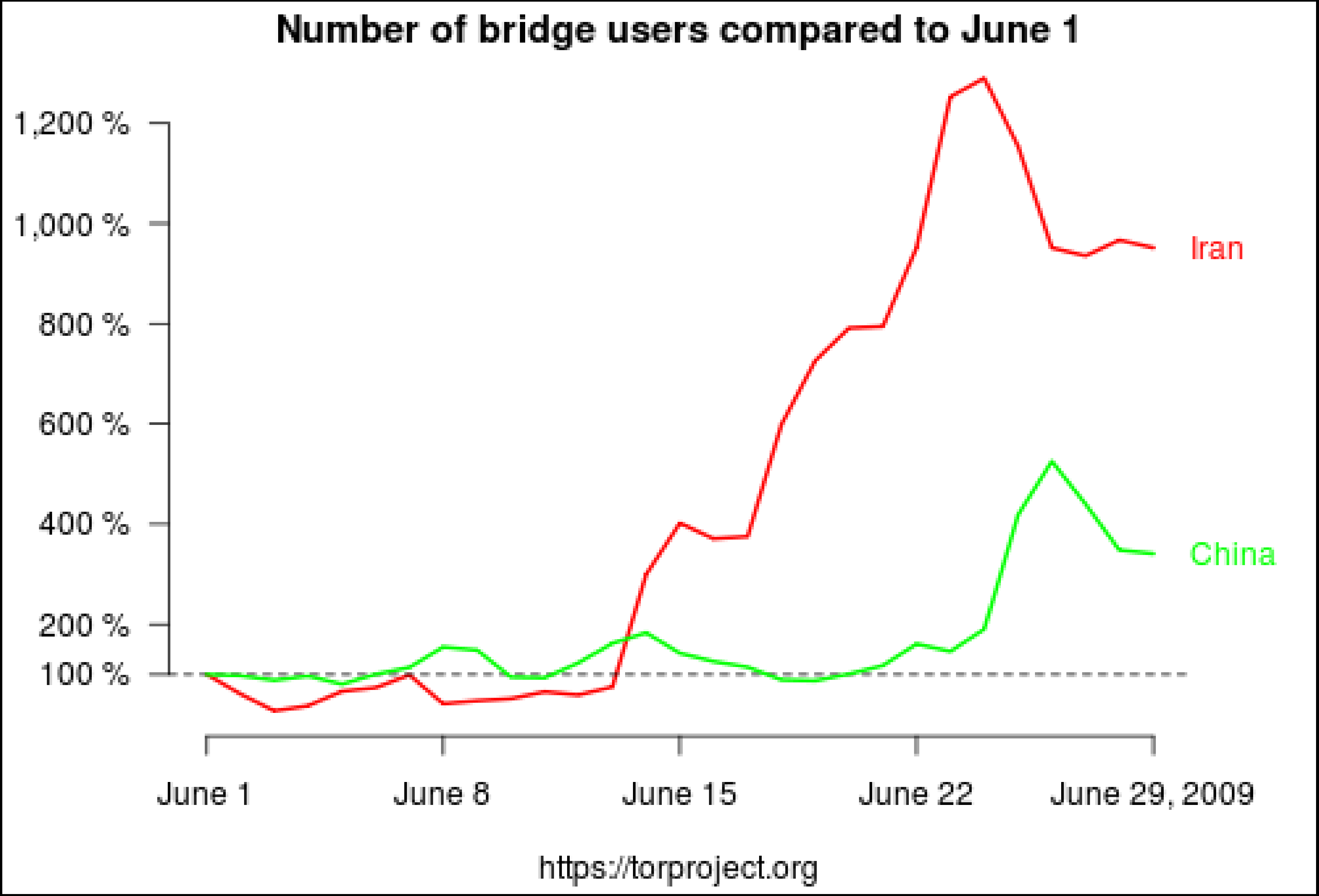
(China and Iran do this today)

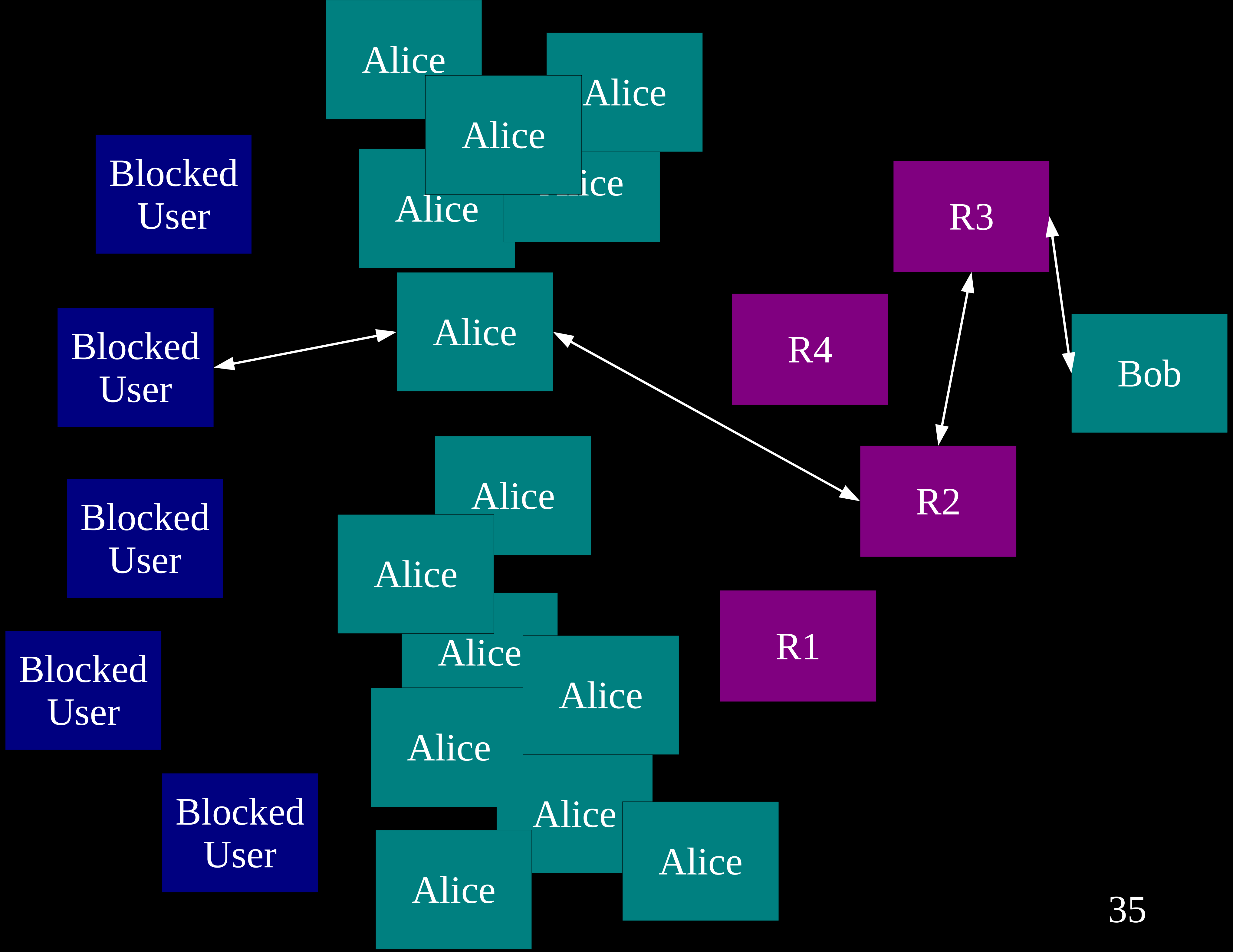

Number of directory requests to directory mirror trusted
10000
8000
6000
4000
2000
0
Sep 10
Sep 17
Sep 24
Oct 01
China
https://torproject.org



Number of bridge users compared to September 6

https://torproject.org


Number of bridge users compared to June 1
1,200 %
1,000 %
800 %
600 %
400 %
200 %
100 %
Iran
China
June 1
June 8
June 15
June 22
June 29, 2009
https://torproject.org



Alice

Alice

Alice

ice

Alice

Blocked User

R3

Blocked User

Alice

R4

Bob

Alice

R2

Blocked User

Alice

Alice

Blocked User

Alice

R1

Alice

Alice

Blocked User

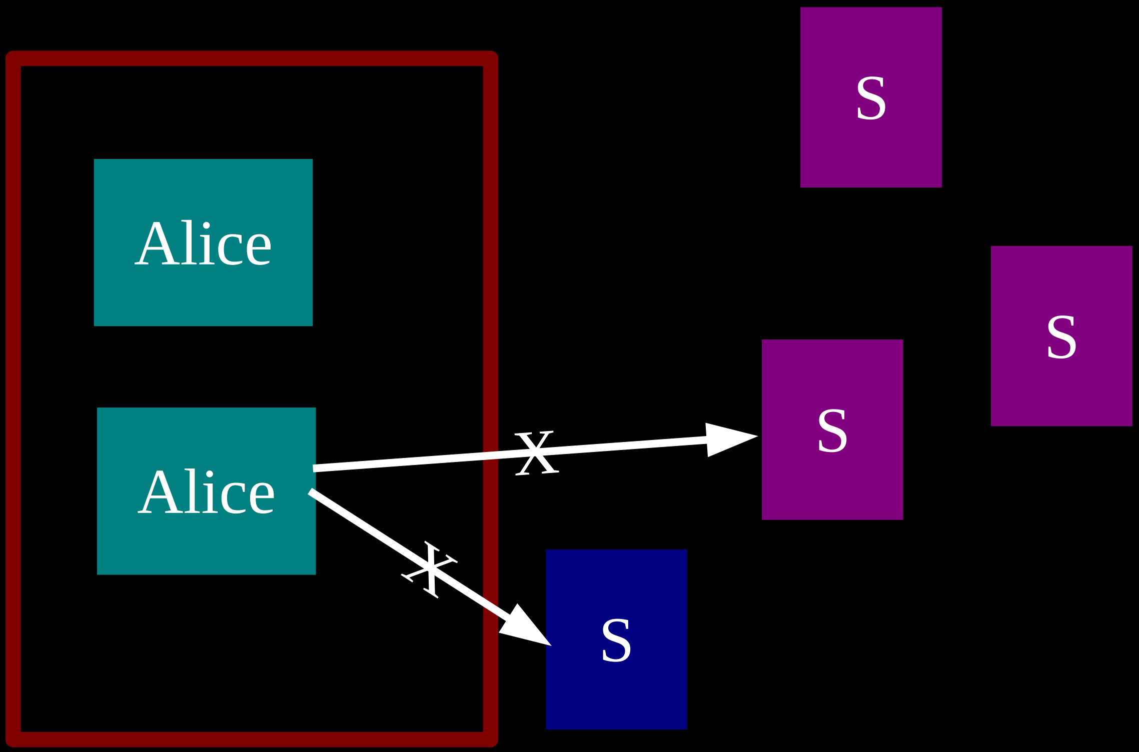
Alice

Alice

How do you find a bridge?

- If you can, go to **https://bridges.torproject.org/** and it will tell you a few based on time and your IP address
- Mail bridges@torproject.org from a gmail/yahoo address, and we'll send you a few
- From your friends, neighbors, and Twitter like before
  - Other private bridges

Others simply discriminate by protocol matching (or mismatching)



Is there a solution for a “whitelisted” Internet?

Twitter and Tor

- Lack of proper SSL support (for mobile too)
  - redirects to plain-text site
  - no SSL (secure link only bit) cookies
  - Unauthenticated (JS) content is loaded too
  - Incorrect host names in certificates
- Changing passwords doesn't change OAuth token
  - Why isn't this done via POST?
- Your captcha is broken (See Jonathan Wilkin's research)
- Blocked in many areas because you're useful!

How can you help?

- The Tor network needs bridges
  - Anyone can run one – no real liability
- The Tor network needs relays
  - A middle node sends only encrypted data
  - Exit nodes are tricky but very important
  - Exit Enclaves are needed
    - tor.twitter.com could exit to itself
  - Hidden service login for Twitter users?
- Ideas, research, feedback?

Questions?