

Tor and circumvention: Lessons learned

Roger Dingledine

The Tor Project

<https://torproject.org/>

What is Tor?

- Online anonymity 1) software, 2) network, 3) protocol
- Open source, freely available
- Community of researchers, developers, users, and relay operators
- Funding from US DoD, Electronic Frontier Foundation, Voice of America, Google, NLnet, Human Rights Watch, ...

The Tor Project, Inc.

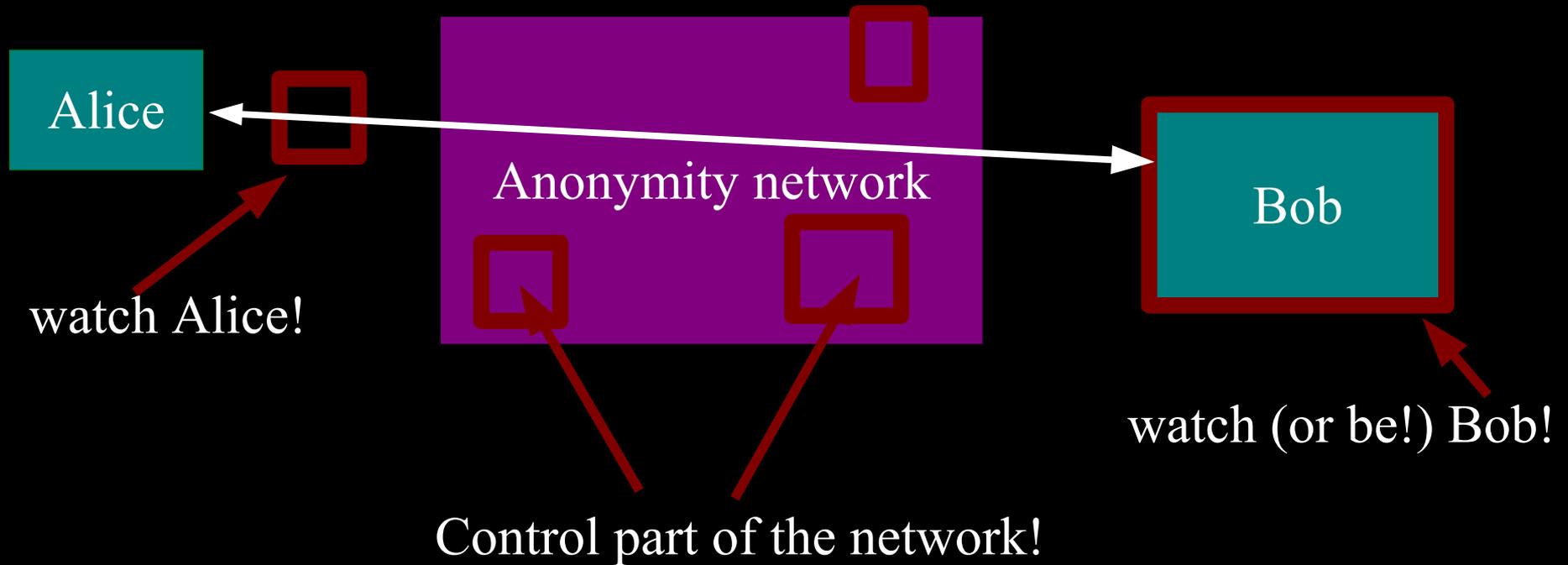


- 501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy

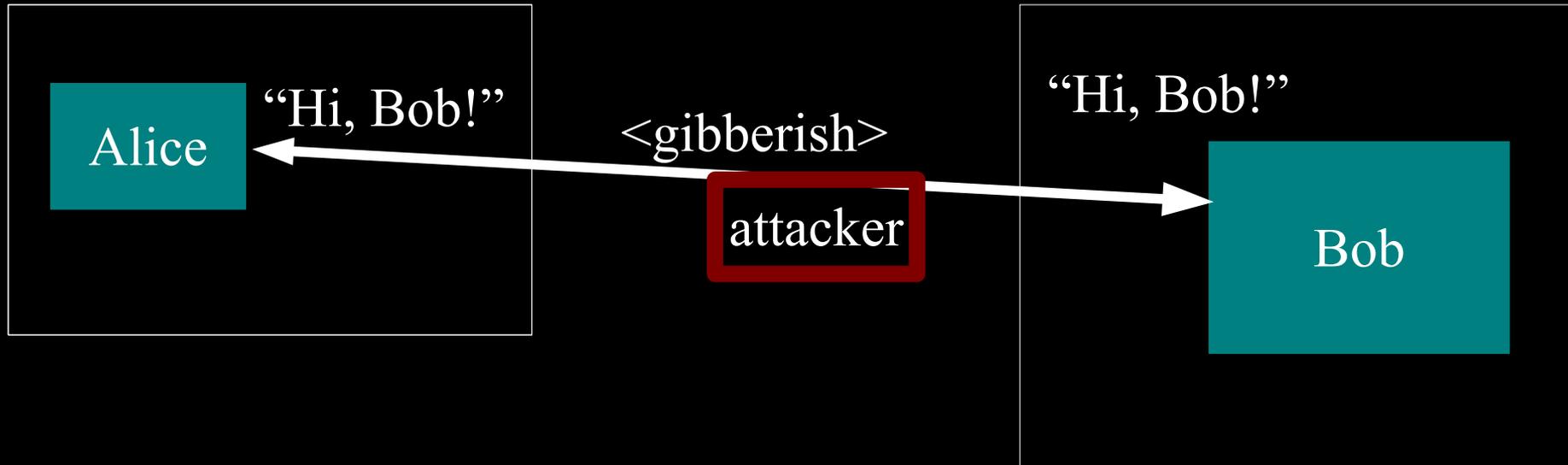


Estimated 300,000
daily Tor users

Threat model: what can the attacker do?



Anonymity isn't cryptography: Cryptography 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.

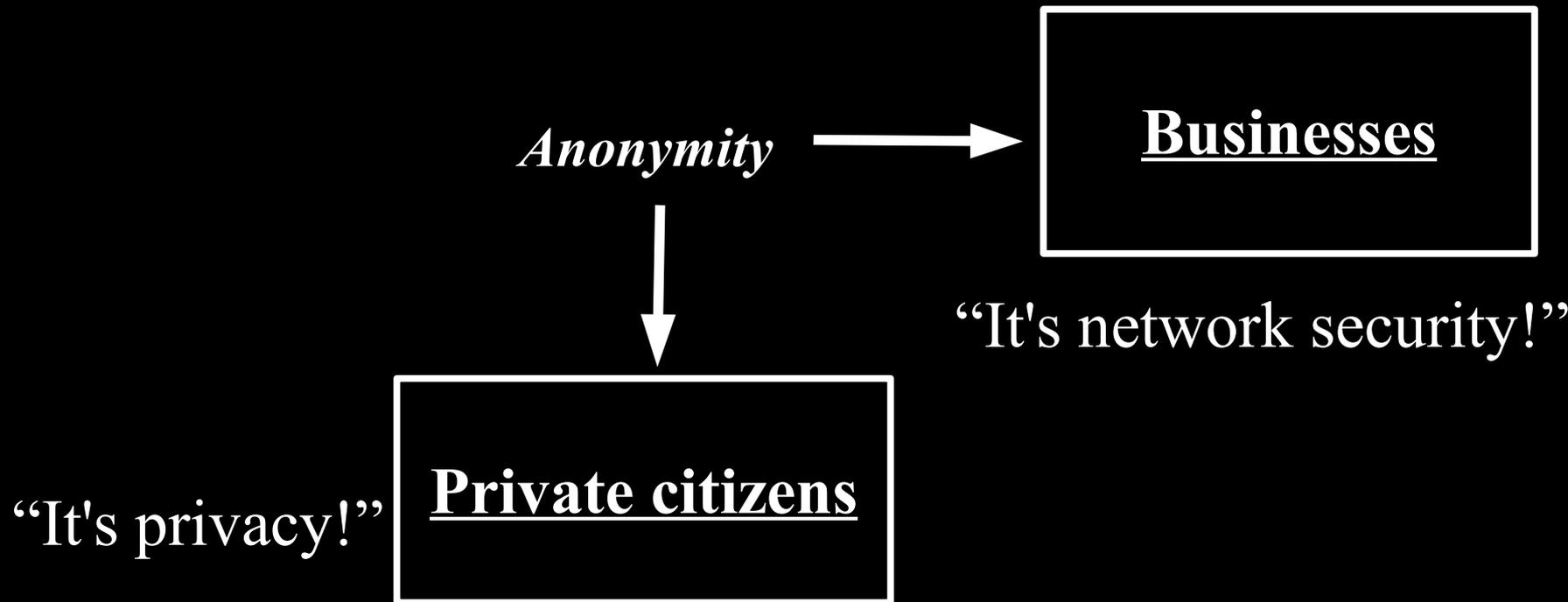
Anonymity



“It's privacy!”

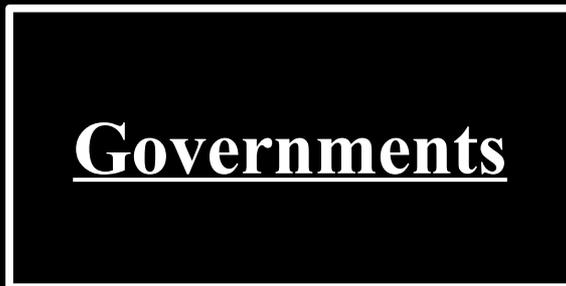
Private citizens

Anonymity serves different interests for different user groups.



Anonymity serves different interests for different user groups.

“It's traffic-analysis resistance!”



Anonymity

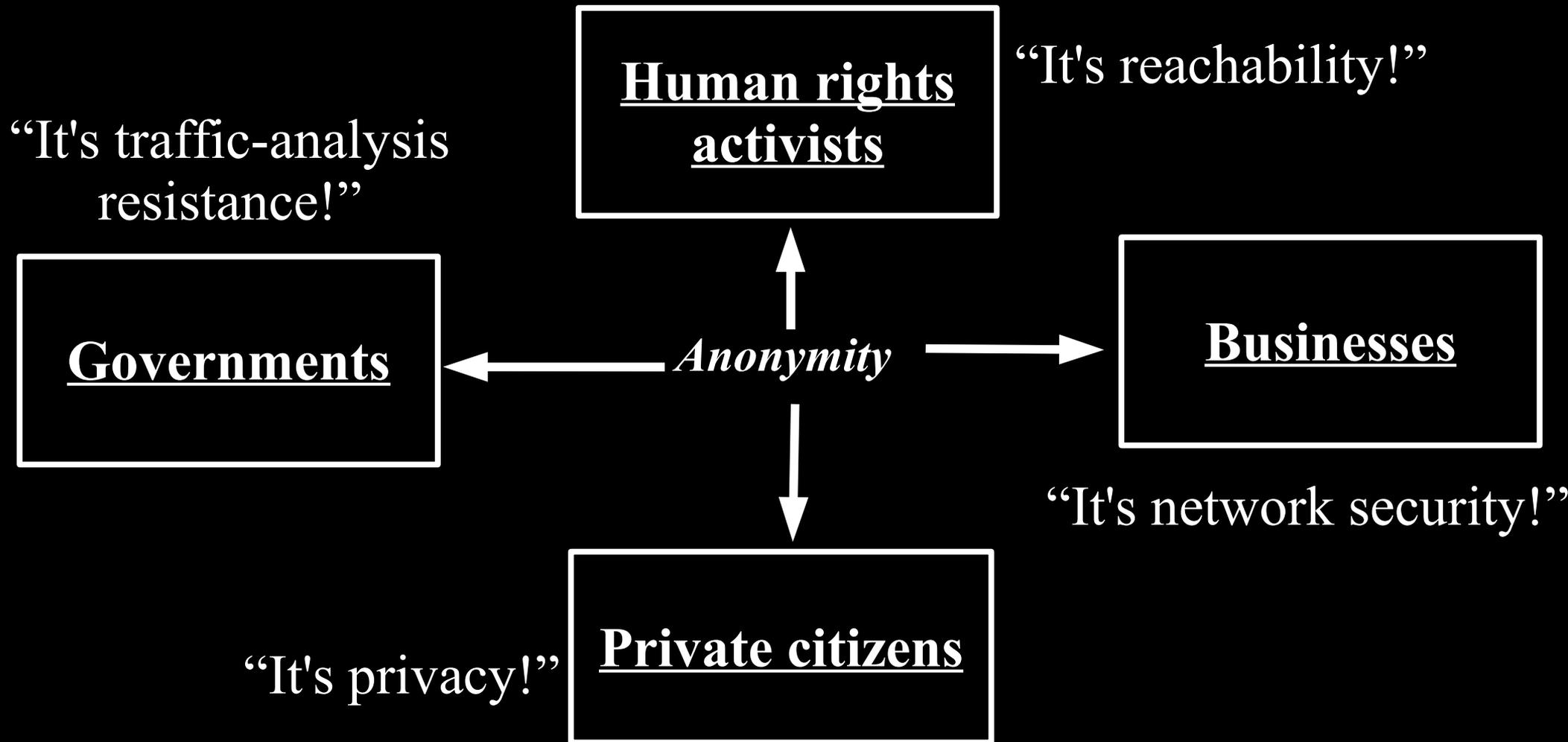


“It's network security!”

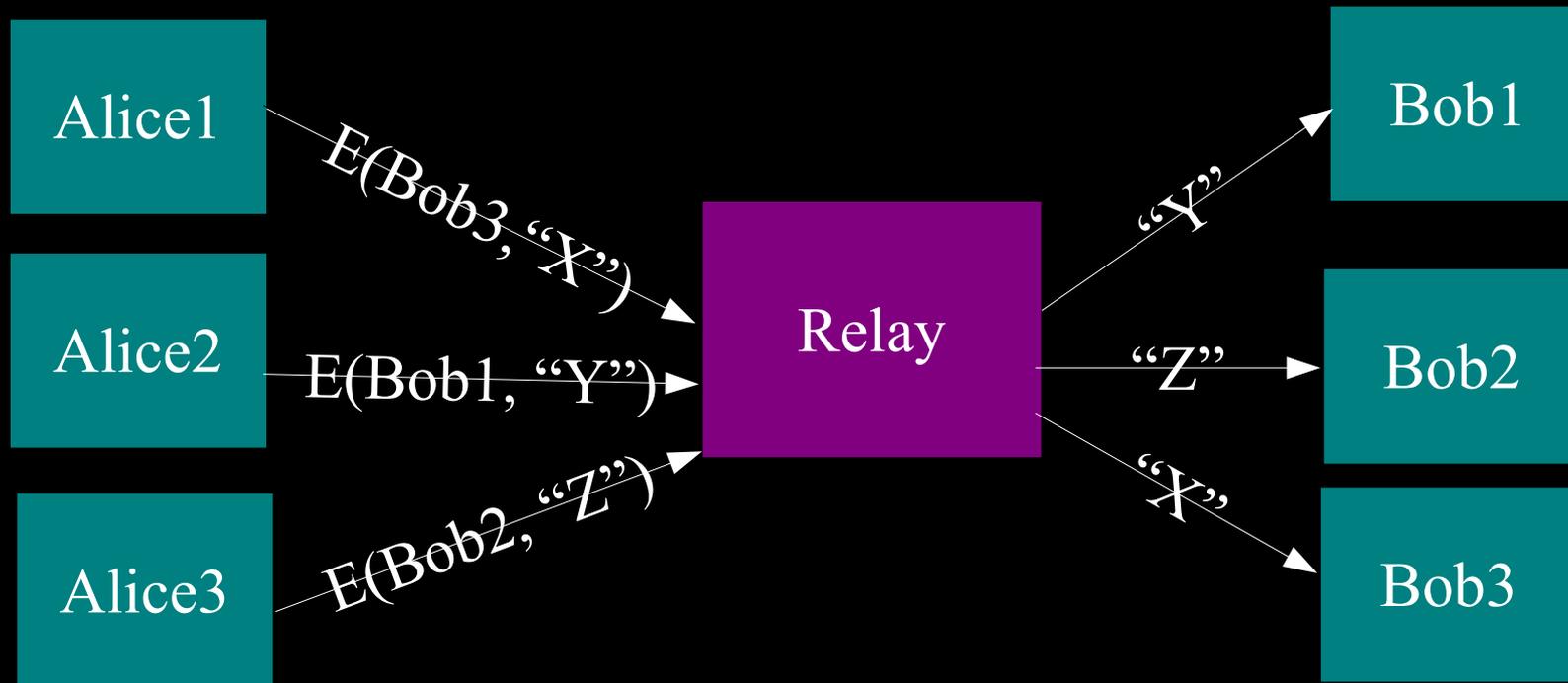
“It's privacy!”



Anonymity serves different interests for different user groups.

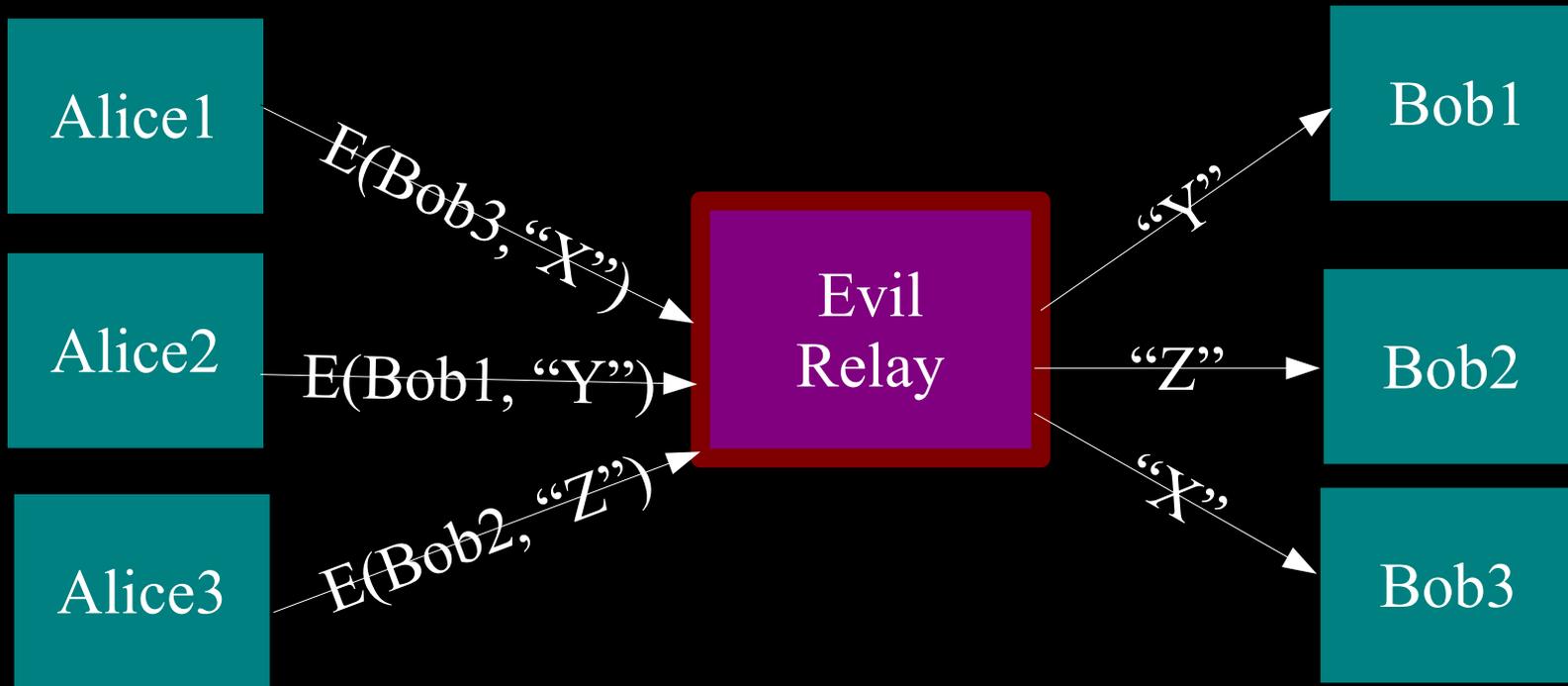


The simplest designs use a single relay to hide connections.

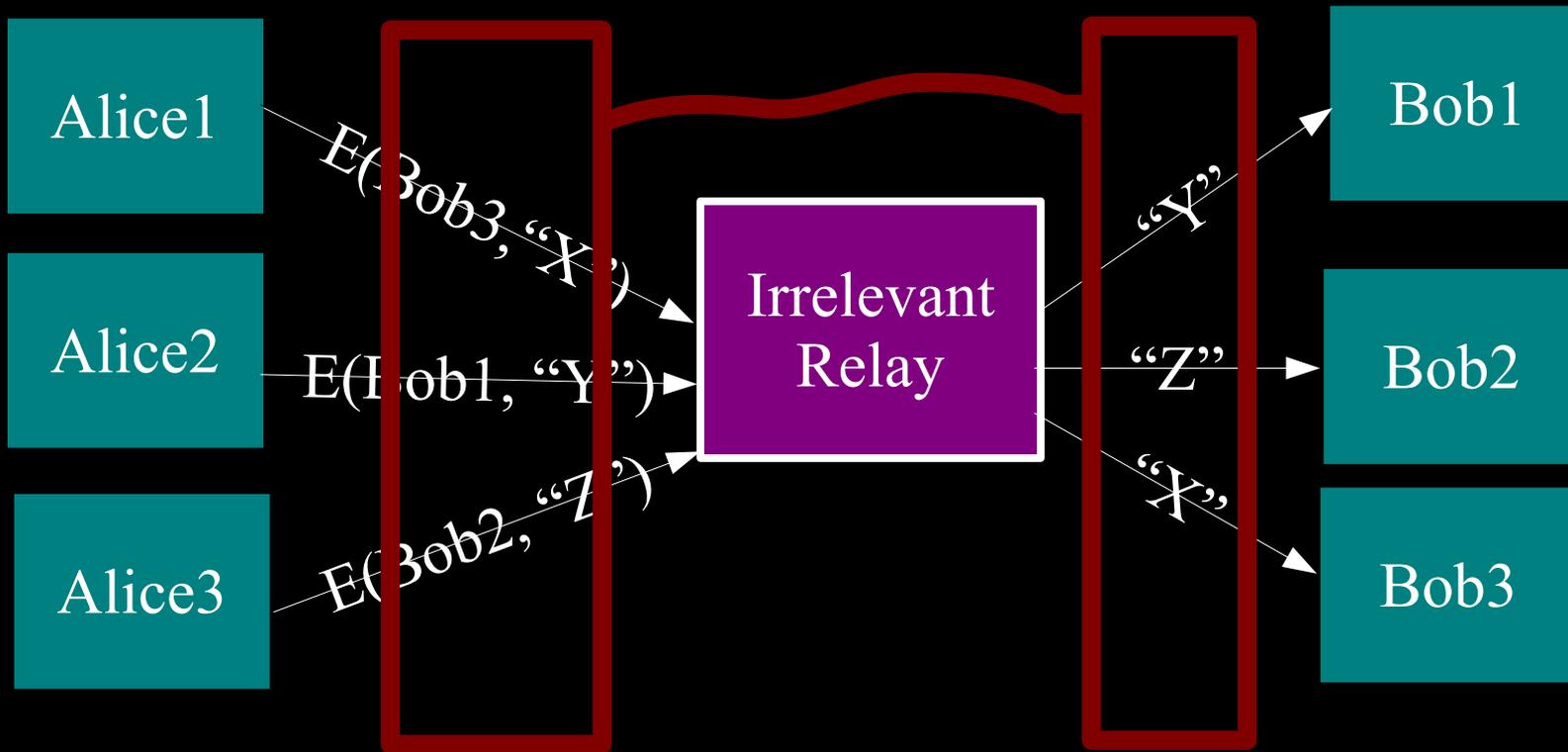


(example: some commercial proxy providers)

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

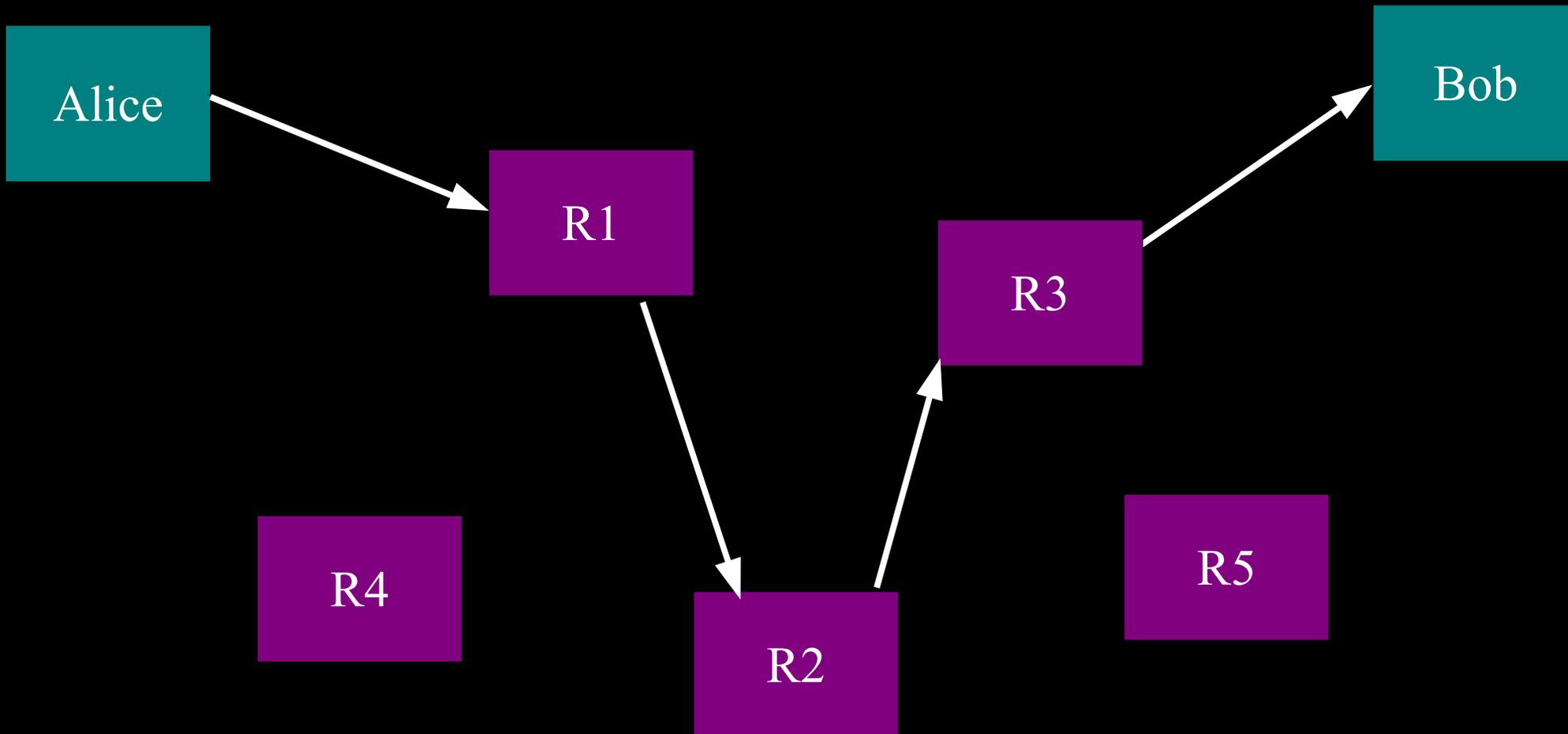


... or a single point of bypass.

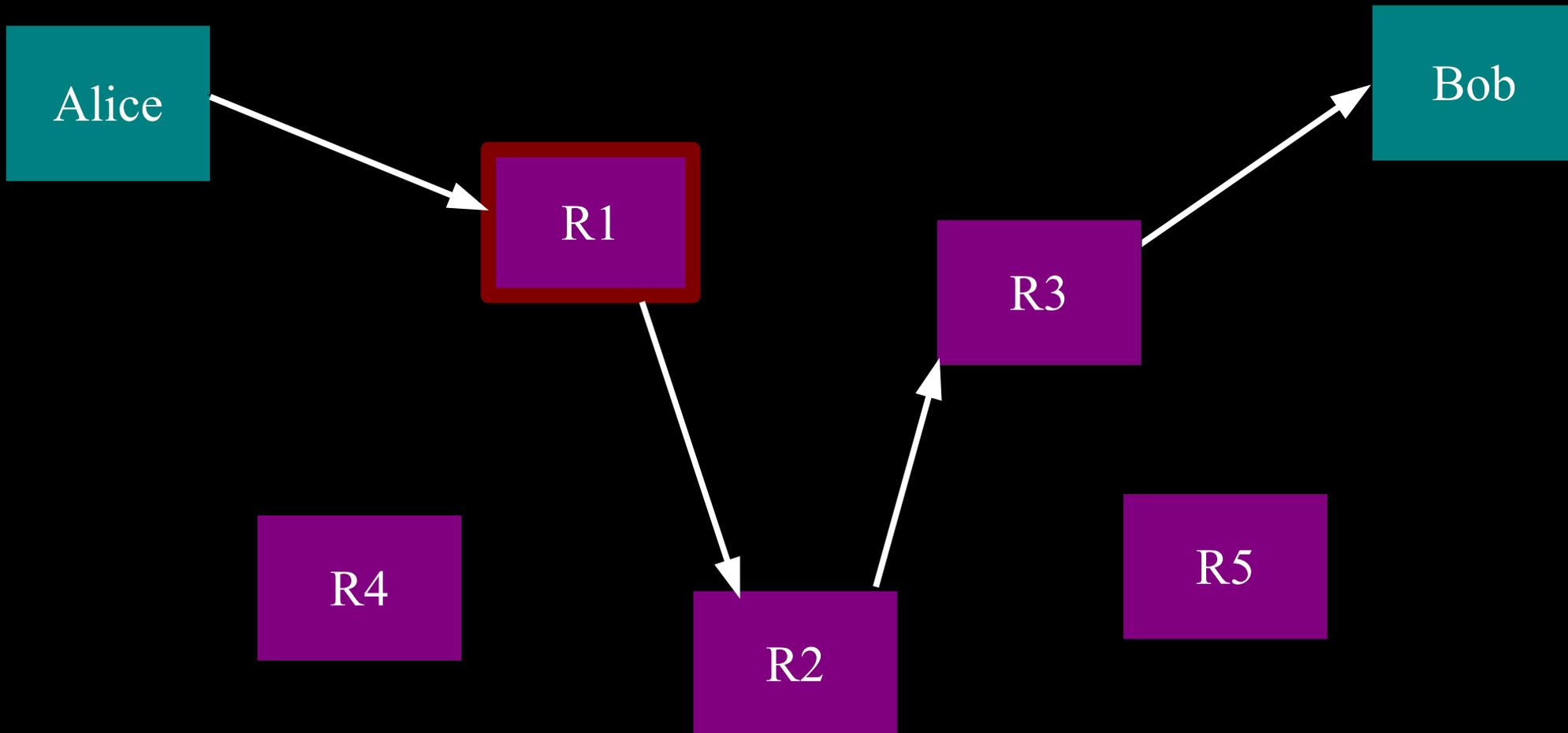


Timing analysis bridges all connections through relay \Rightarrow An attractive fat target

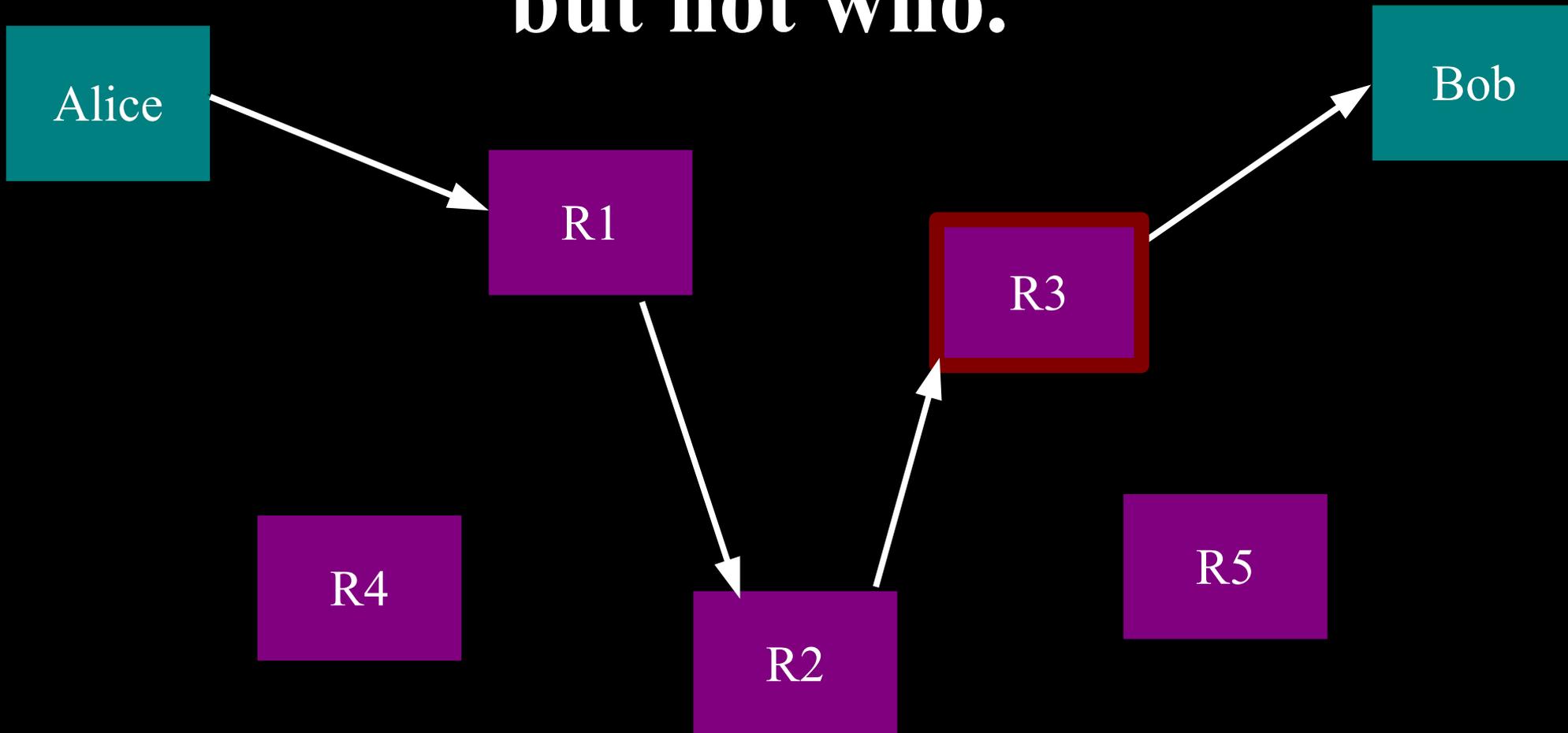
So, add multiple relays so that no single one can betray Alice.



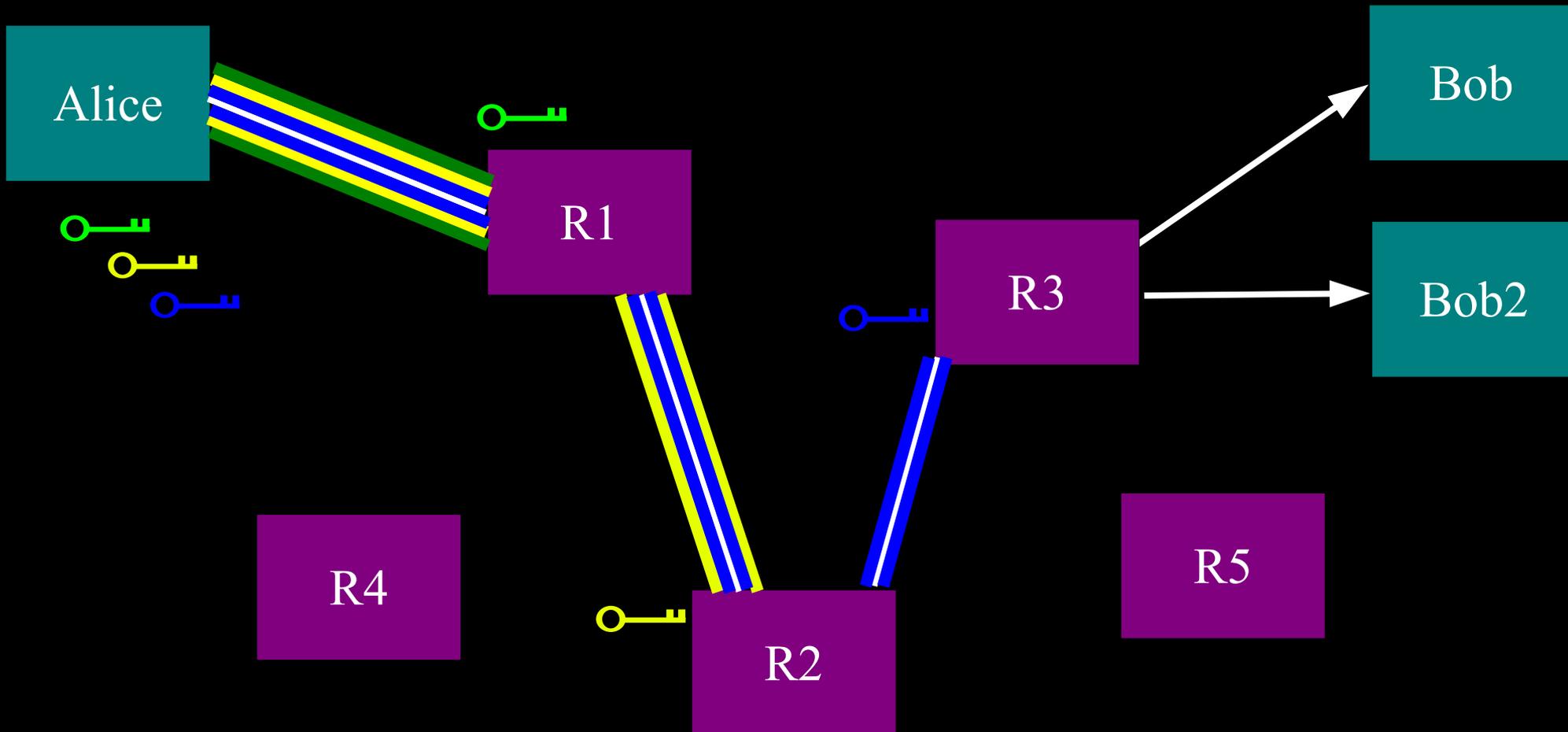
A corrupt first hop can tell that Alice is talking, but not to whom.



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



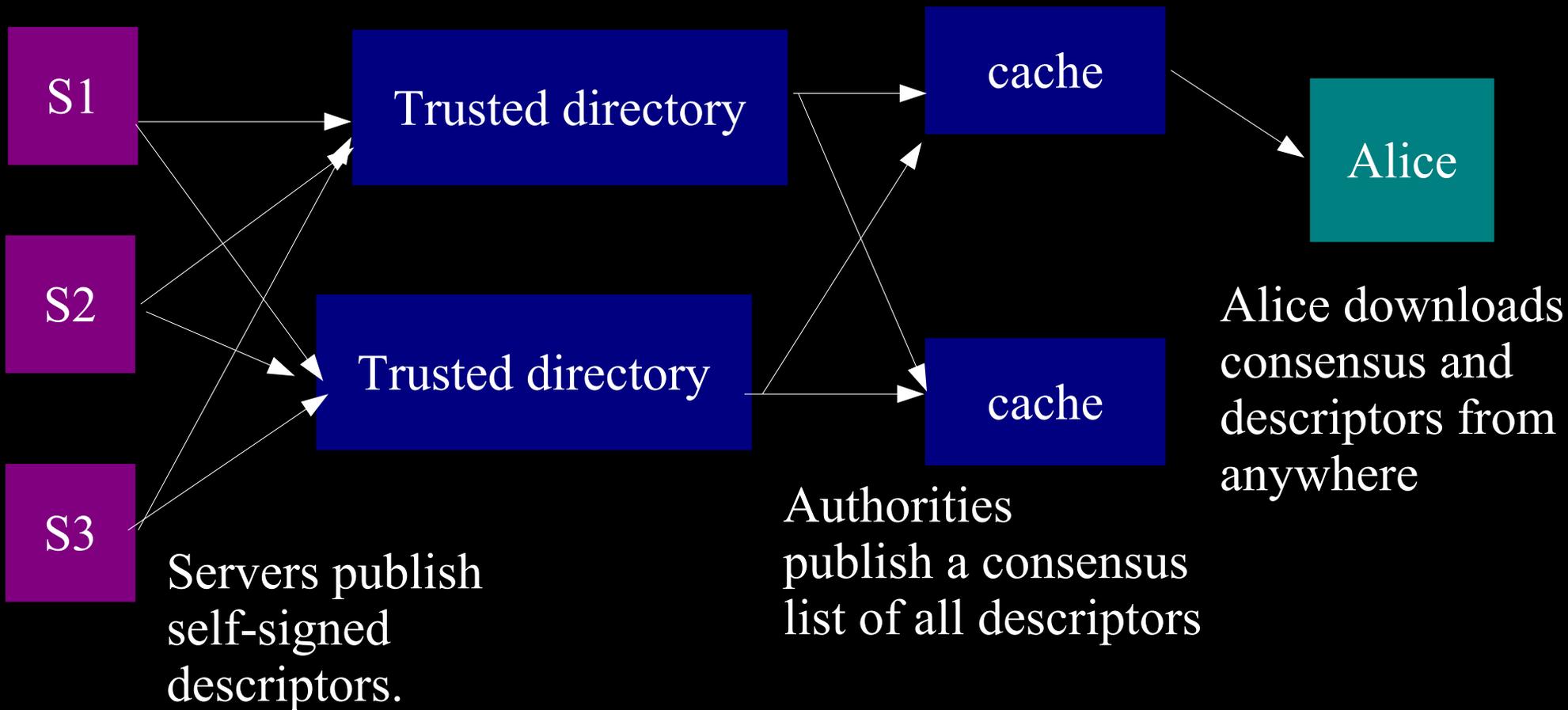
**Alice makes a session key with R1
...And then tunnels to R2...and to R3**



Relay versus Discovery

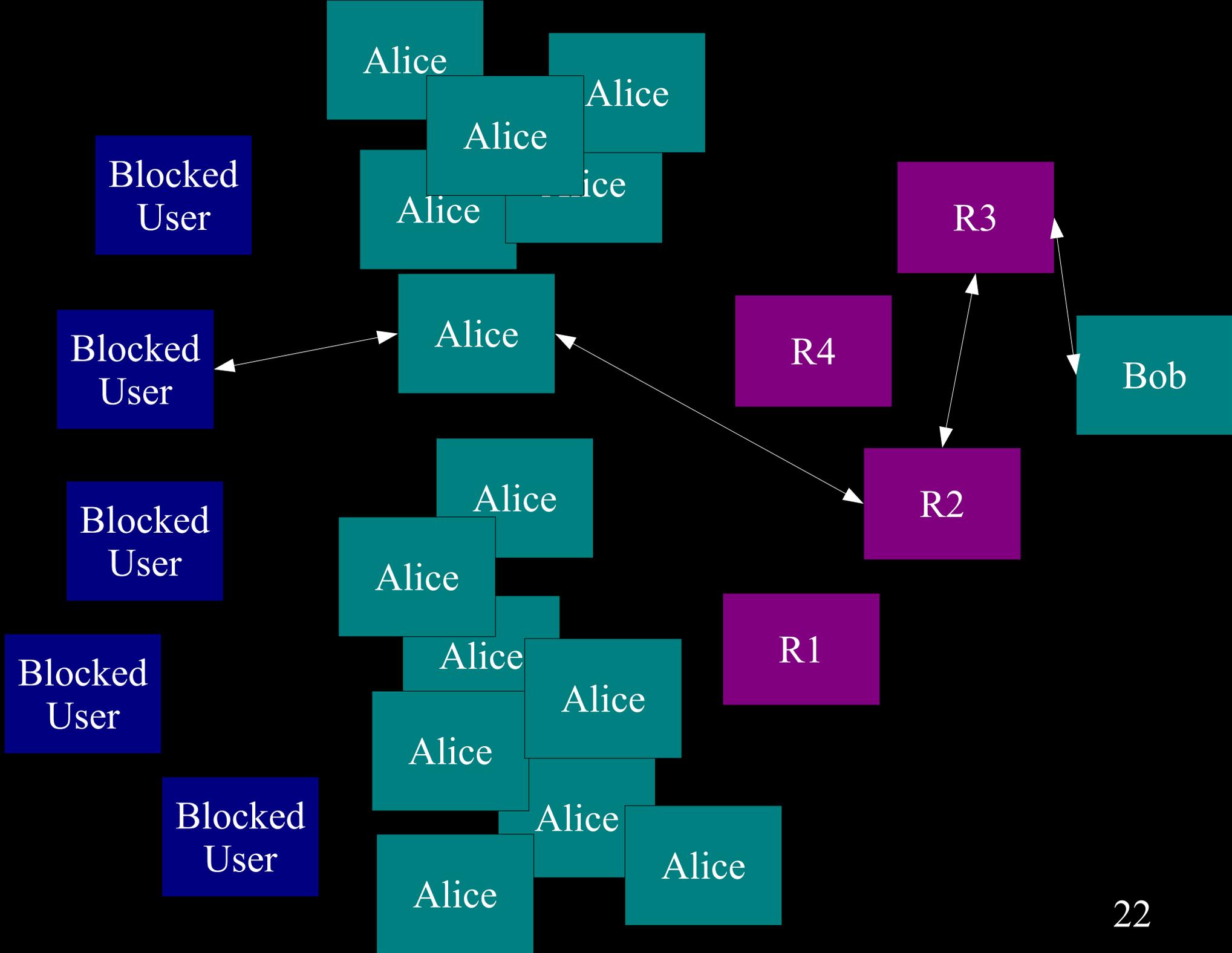
- There are two pieces to all these “proxying” schemes:
- a **relay** component: building circuits, sending traffic over them, getting the crypto right
- a **discovery** component: learning what relays are available

The basic Tor design uses a simple centralized directory protocol.



Attackers can block users from connecting to the Tor network

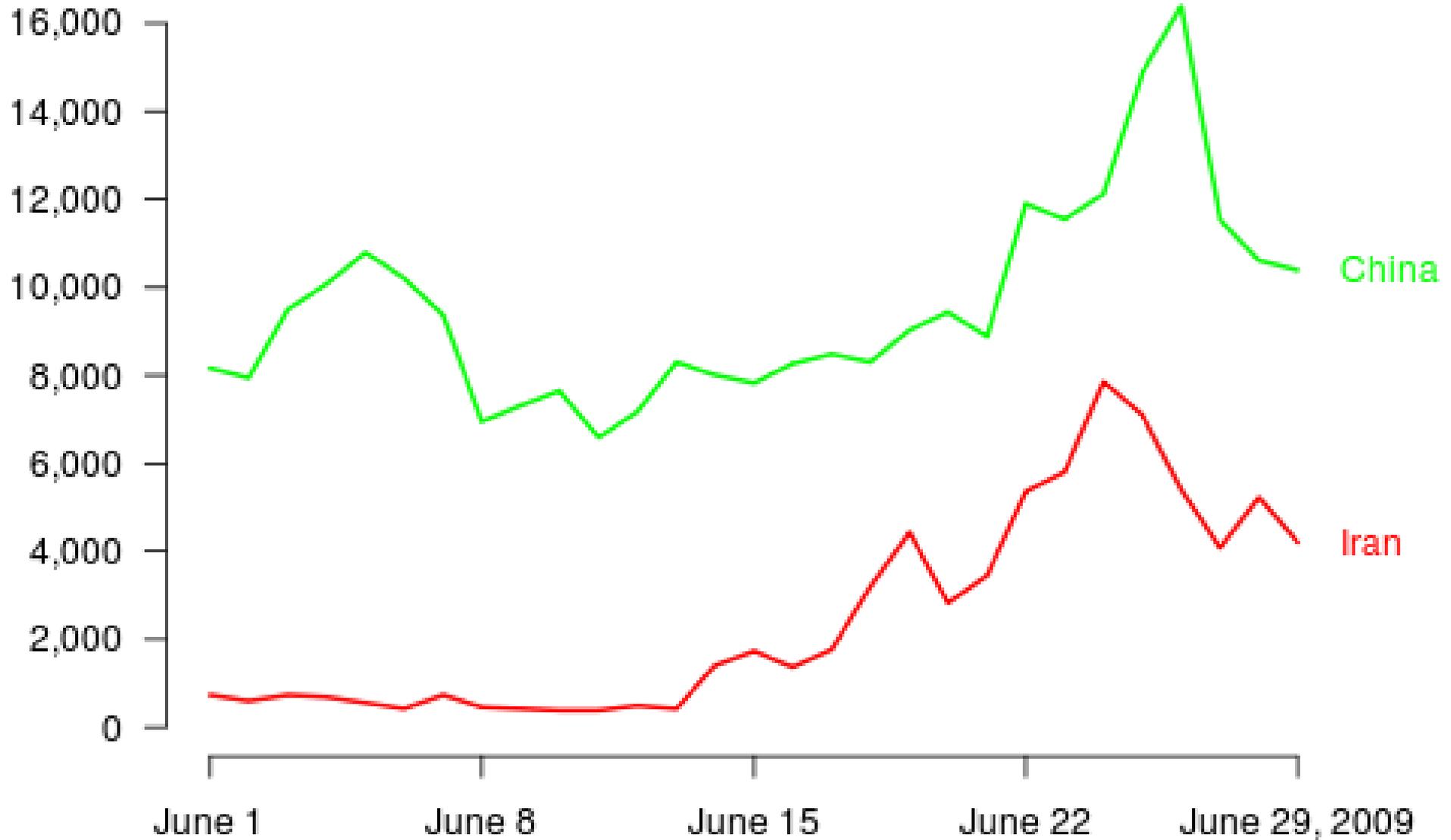
- By blocking the directory authorities
- By blocking all the relay IP addresses in the directory
- By filtering based on Tor's network fingerprint
- By preventing users from finding the Tor software



“Bridge” relays

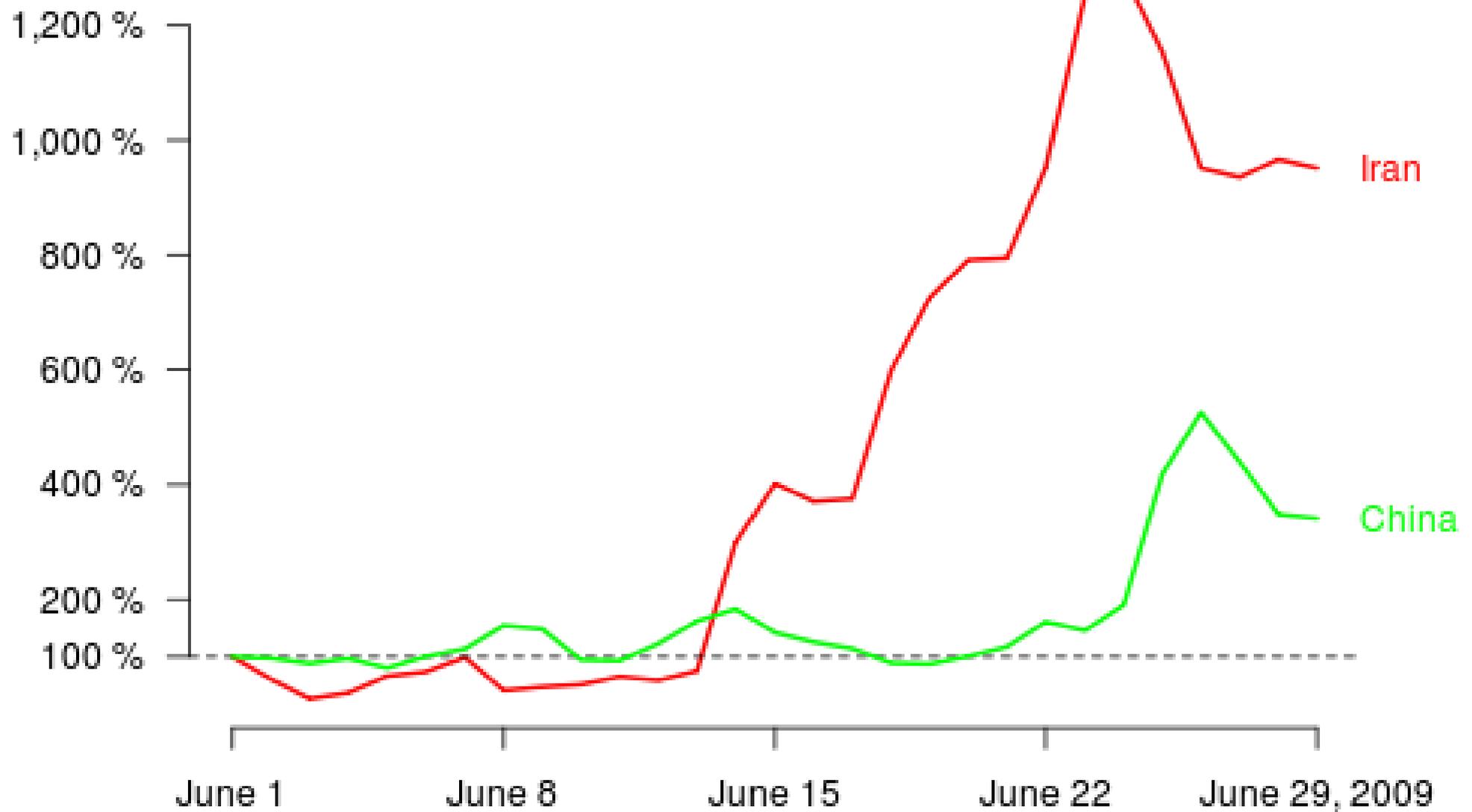
- Hundreds of thousands of Tor users, already self-selected for caring about privacy.
- Rather than signing up as a normal relay, you can sign up as a special “bridge” relay that isn't listed in any directory.
- No need to be an “exit” (so no abuse worries), and you can rate limit if needed
- Integrated into Vidalia (our GUI) so it's easy to offer a bridge or to use a bridge

New or returning Tor clients per day



<https://torproject.org>

Number of bridge users compared to June 1



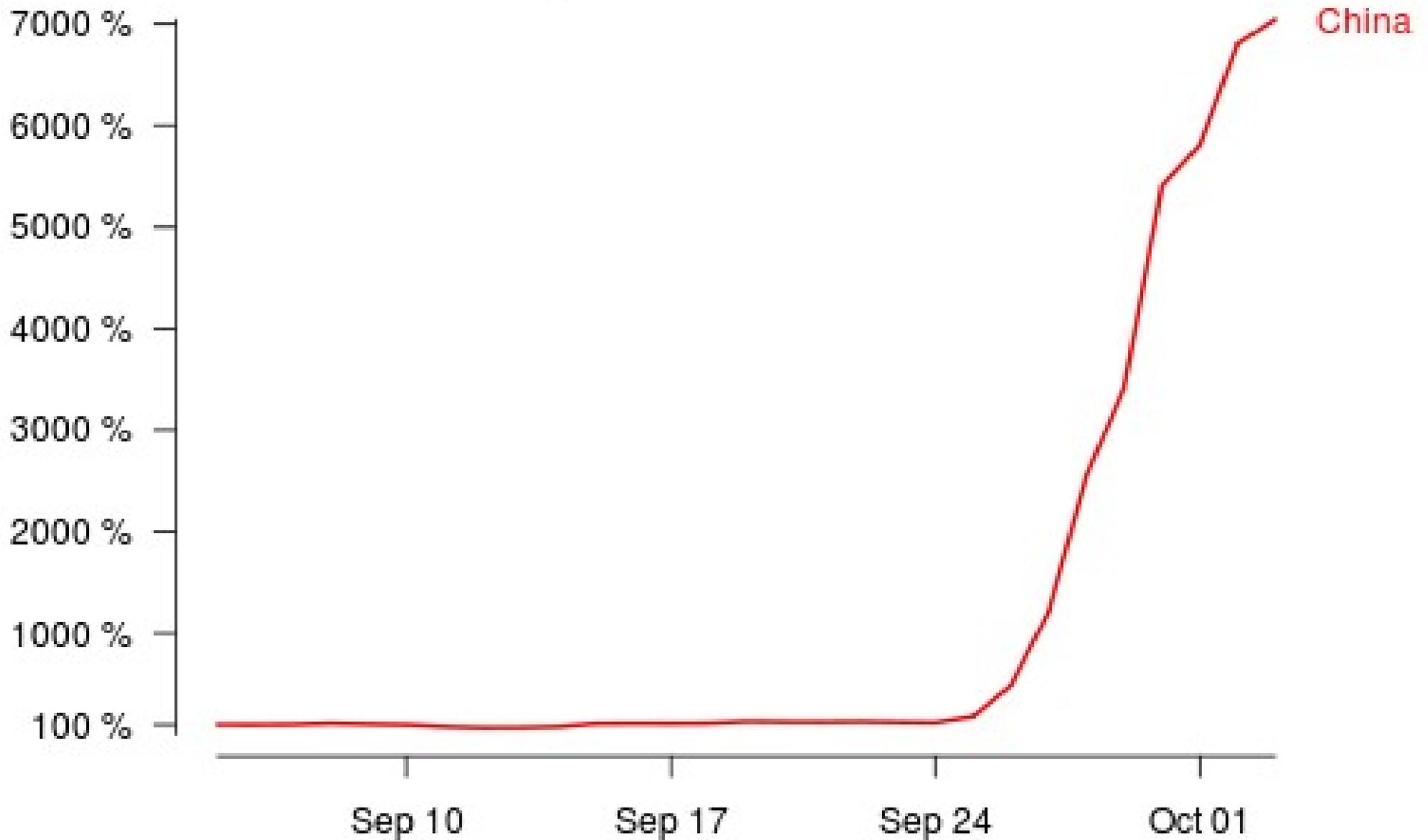
<https://torproject.org>

Number of directory requests to directory mirror trusted



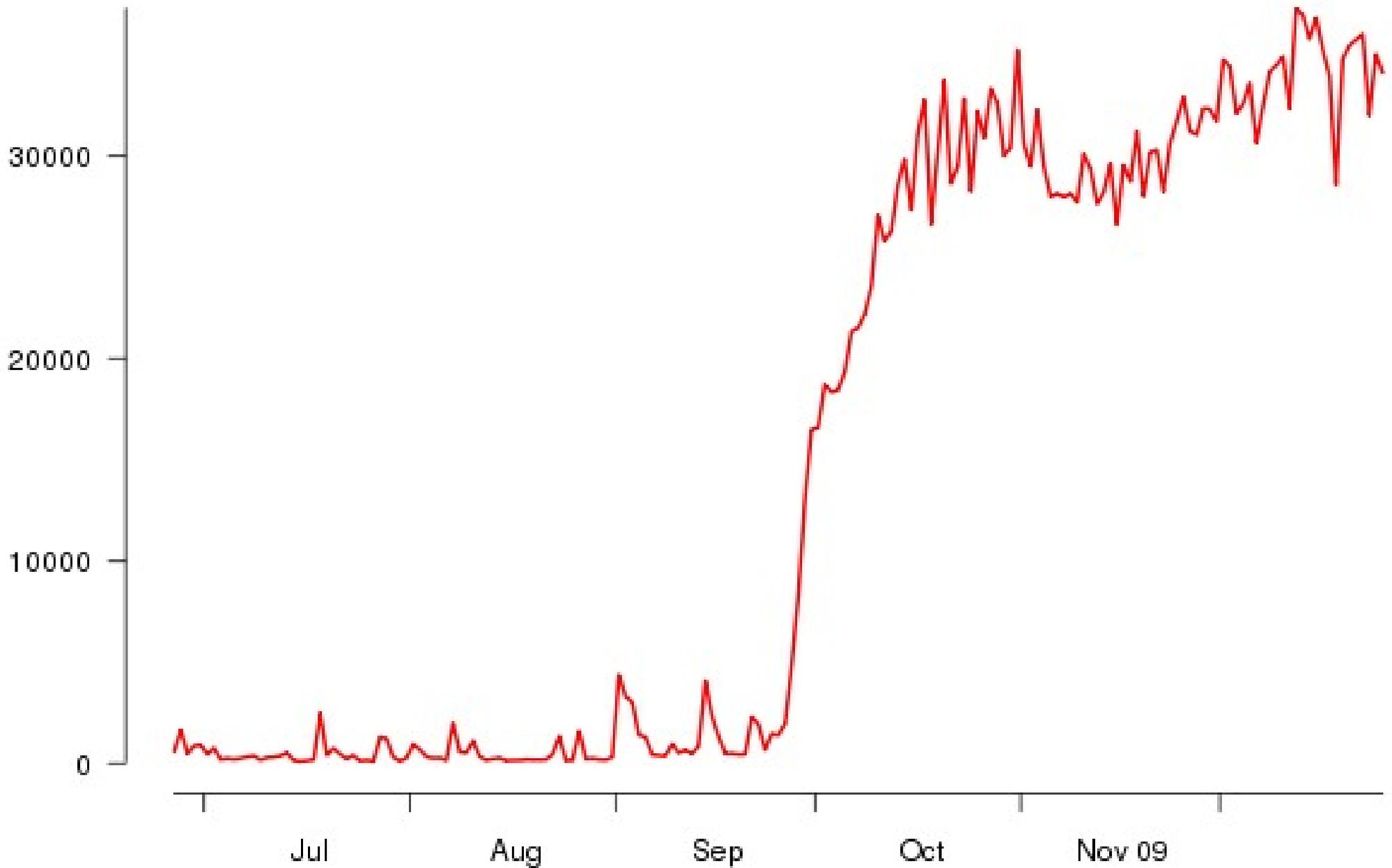
<https://torproject.org>

Number of bridge users compared to September 6



<https://torproject.org>

Chinese Tor users via bridges



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 and neighbors, like before

Bridge directory authorities

- Specialized dir authorities that aggregate and track bridges, but don't provide a public list:
 - You can keep up-to-date about a bridge once you know its key, but can't just grab list of all bridges.
- Identity key and address for default bridge authorities ship with Tor.
- Bridges publish via Tor, in case somebody is monitoring the authority's network.

One working bridge is enough

- Connect via that bridge to the bridge authority.
- ...and to the main Tor network.
- Remember, all of this happens in the background.
- “How to circumvent for all transactions (and trust the pages you get)”
is now reduced to
“How to learn about a working bridge”.

Hiding Tor's network fingerprint

- We got rid of plaintext HTTP (used by directories). Now clients tunnel their directory requests over the same TLS connection as their other Tor traffic.
- We've made Tor's TLS handshake look more like Firefox+Apache.
- When Iran kicked out Smartfilter in early 2009, Tor's old v2 dir design worked again!

Attacker's goals (1)

- Restrict the flow of certain kinds of information
 - Embarrassing (rights violations, corruption)
 - Opposing (opposition movements, sites that organize protests)
- Chill behavior by *impression* that online activities are monitored

Attacker's goals (2)

- Complete blocking is not a goal. It's not even necessary.
- Similarly, no need to shut down or block *every* circumvention tool. Just ones that are
 - popular and effective (the ones that work)
 - highly visible (make censors look bad to citizens -- and to bosses)

Attacker's goals (3)

- Little reprisal against passive consumers of information.
 - Producers and distributors of information in greater danger.
- Censors (actually, govts) have economic, political, social incentives not to block the whole Internet.
 - But they don't mind collateral damage.

Main network attacks

- Block by IP address / port at firewall
- Intercept DNS requests and give bogus responses or redirects
- China: Keywords in TCP packets
- Iran: DPI to filter SSL when they want
- Russia: Don't block, just pollute

What we're up against (1)

- 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 :(
- How to separate “oppressing employees” vs “oppressing citizens” arms race?

What we're up against (2)

- Censorship is not uniform even within each country, often due to different ISP policies
- Attacker can influence other countries and companies to help them censor or track users. We'll see if the GNI (Global Network Initiative) changes that.

Blocking goes both ways

- If China blackholes your IP address, you can't reach Chinese websites either.
- So if exit relays are blackholed, Tor users can't read Chinese websites. :(
- And if you use dynamic IP addresses, then more and more of your neighbors can't read Chinese websites?

Only a piece of the puzzle (1)

- Assume the users aren't attacked by their hardware and software
 - No spyware installed, no cameras watching their screens, etc
- Users need to know about SSL for gmail. Cookies. Etc.
- Many people in Iran in June were using plaintext proxies!

Only a piece of the puzzle (2)

- Users can fetch a genuine copy of Tor?
- GPG signatures are great, but nobody knows what that means, and nobody in Burma has my key.
- Gettor email autoresponder. USB key spread by hand.
- Our secure updater should help.

Tor gives three anonymity properties

- **#1:** A local network attacker can't learn, or influence, your destination.
 - Clearly useful for blocking resistance.
- **#2:** No single router can link you to your destination.
 - The attacker can't sign up relays to trace users.
- **#3:** The destination, or somebody watching it, can't learn your location.
 - So they can't reveal you; or treat you differently.

Sustainability

- Tor has a community of developers and volunteers.
- Commercial anonymity systems have flopped or constantly need more funding for bandwidth.
- Our sustainability is rooted in Tor's open design: clear documentation, modularity, and open source.

Responding to China blocks

- In late Sept, conflicting advice from experts:
- “Hit 'em in the nose, show that you care about your users”
- “Lie low and let it pass. You're about more than China.”
- Tor is a new approach to China bloggers: “Find new bridge” rather than “get software update”.

Publicity attracts attention

- Many circumvention tools launch with huge media splashes. (The media loves this.)
- But publicity attracts attention of the censors.
- We threaten their *appearance* of control, so they must respond.
- We can control the pace of the arms race.

Using Tor in oppressed areas

- Common assumption: risk from using Tor increases as firewall gets more restrictive.
- But as firewall gets more restrictive, more ordinary people use Tor too, for more mainstream activities.
- So the “median” use becomes more acceptable?

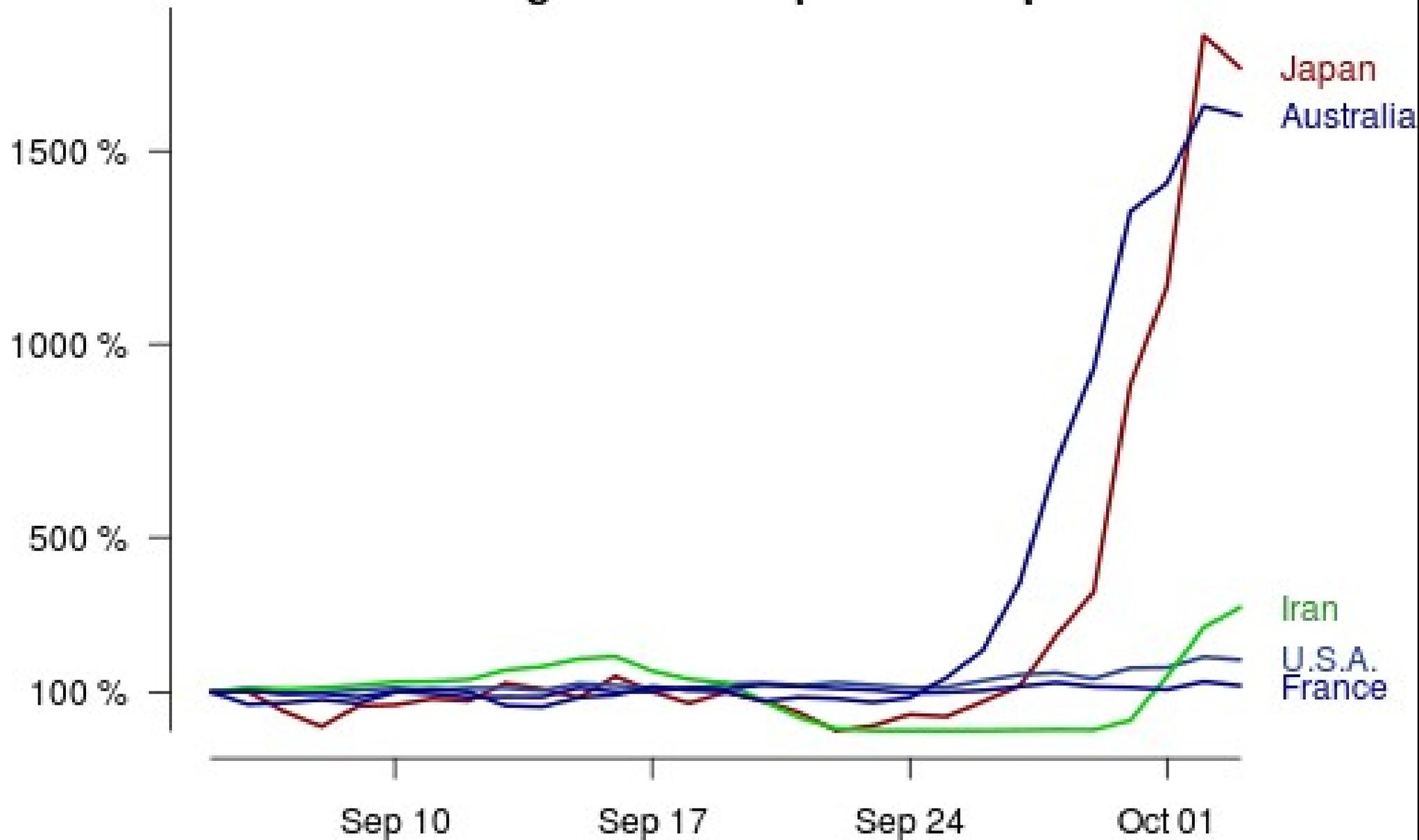
Other Iran user count

- Talked to chief security officer of one of the web 2.0 social networking sites:
 - 10% of their Iranian users in June were coming through Tor
 - 90% were coming from proxies in the Amazon cloud

Trust and reputation

- See Hal Roberts' blog post about how some circumvention tools sell user data
- Many of these tools see circumvention and privacy as totally unrelated goals

Number of bridge users compared to September 5



<https://torproject.org>

I CAN HAZ
FREEDOM?



Other ongoing questions

- How to detect if bridges are blocked (and what to do once we know)
- Better strategies for giving bridges out (Twitter, better use of social networks; Kaist design project)

Bridge communities

- Volunteers run several bridges at once, or coordinate with other volunteers.
- The goal is that some bridges will be available at any given time.
- Each community has a bridge authority, to add new bridges to the pool, expire abandoned or blocked bridges, etc.
- All automated by the Tor client.

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?

Next steps

- Technical solutions won't solve the whole censorship problem. After all, firewalls are *socially* very successful in these countries.
- But a strong technical solution is still a critical puzzle piece.
- You should run a bridge! We only have 400.
- We'd love to help with some trainings, to help users and to make Tor better.