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, ...
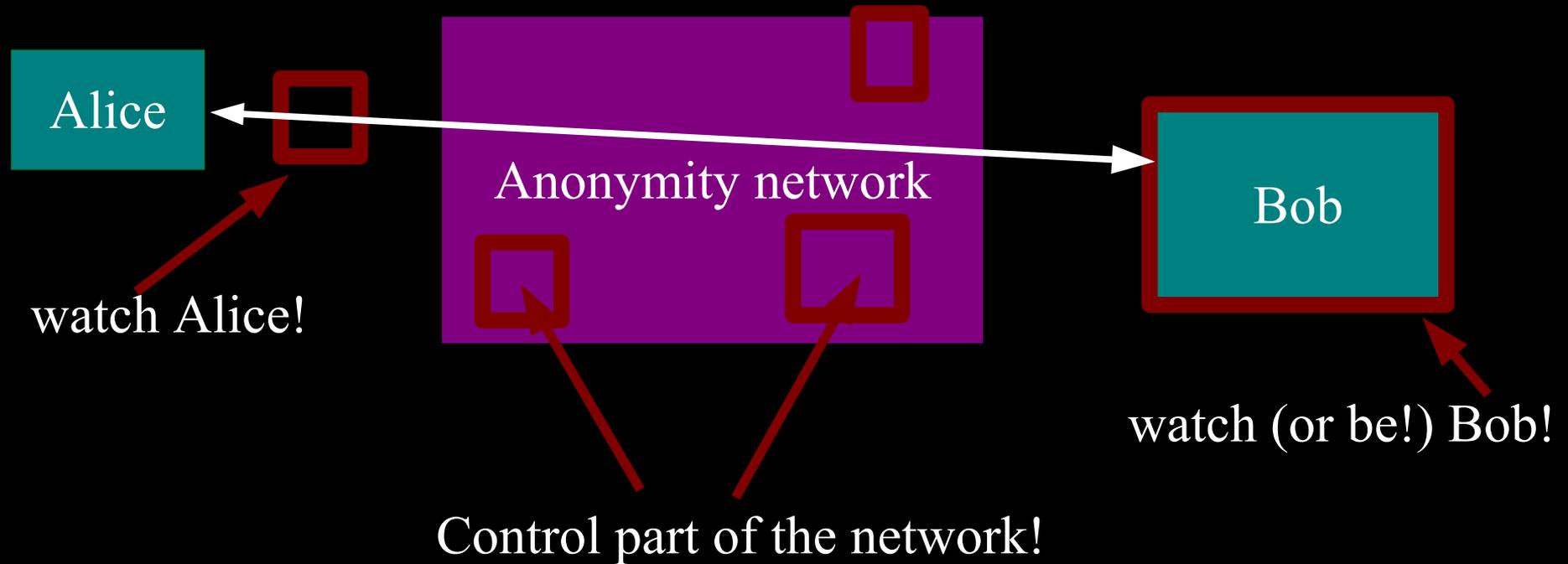
The Tor Project, Inc.

- 501(c)(3) non-profit organization dedicated to the research and development of tools for online anonymity and privacy
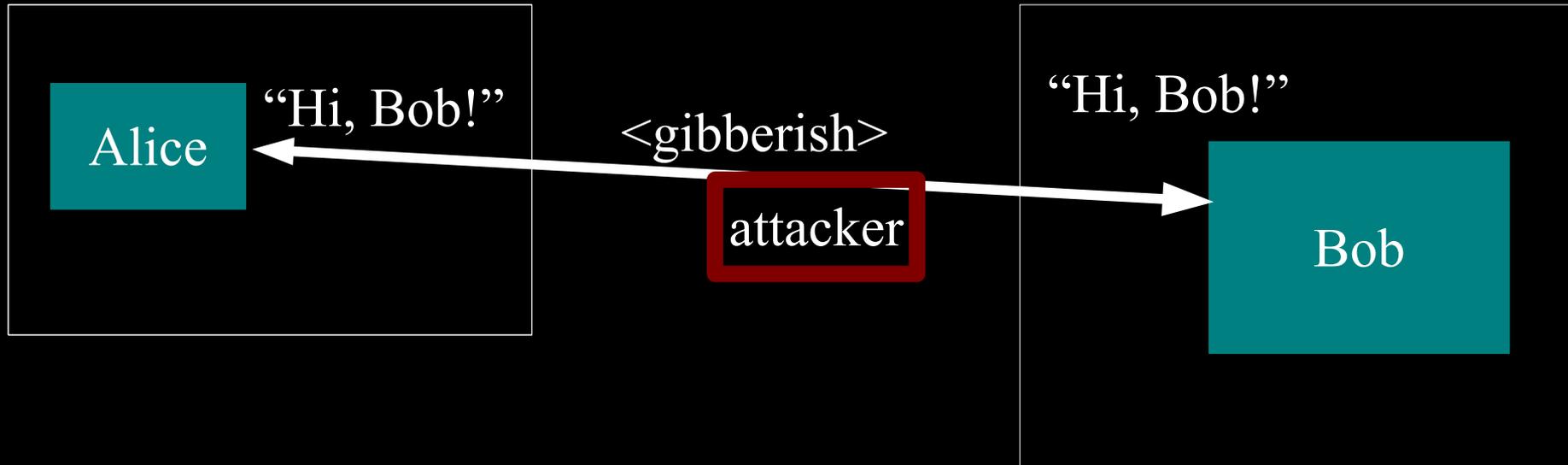
Estimated 500,000 daily Tor users

Threat model:
what can the attacker do?

Alice

Anonymity network

Bob

watch Alice!

Control part of the network!

watch (or be!) Bob!

Anonymity isn't cryptography: Cryptography just protects contents.

Alice — "Hi, Bob!" — <gibberish> — attacker — "Hi, Bob!" — Bob

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?"

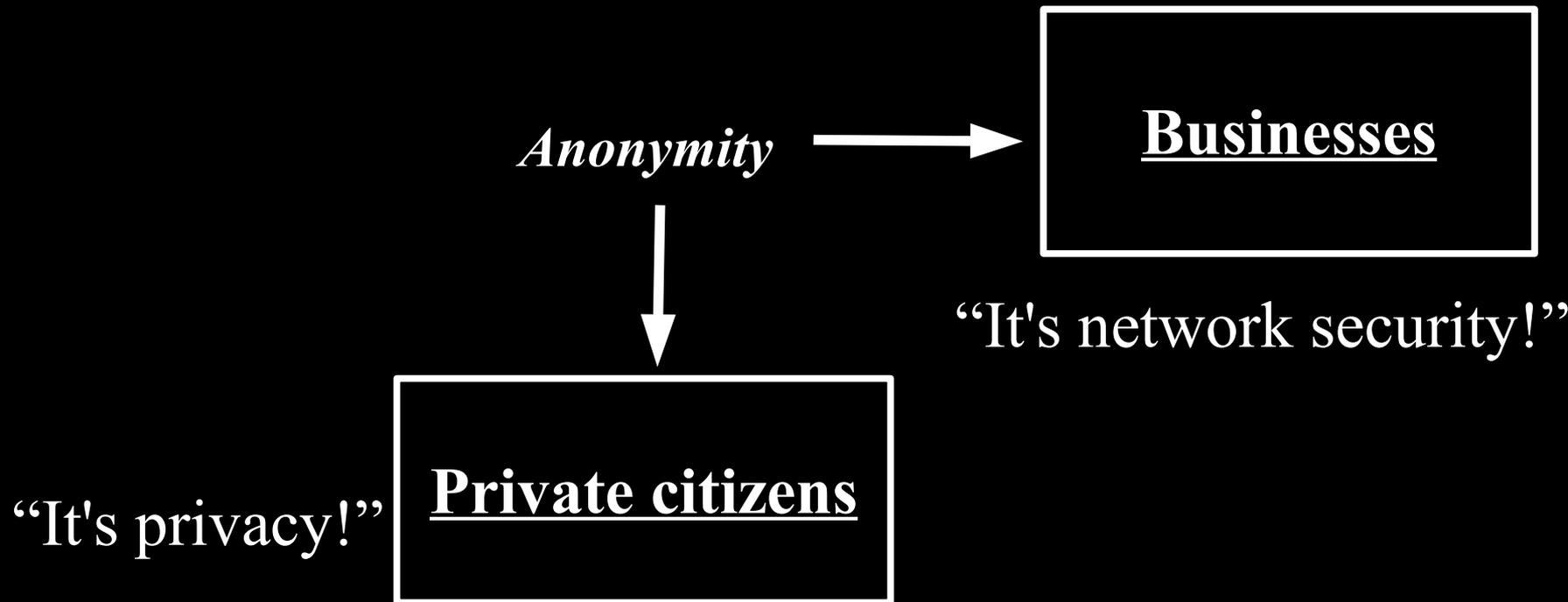# Anonymity serves different interests for different user groups.

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!"

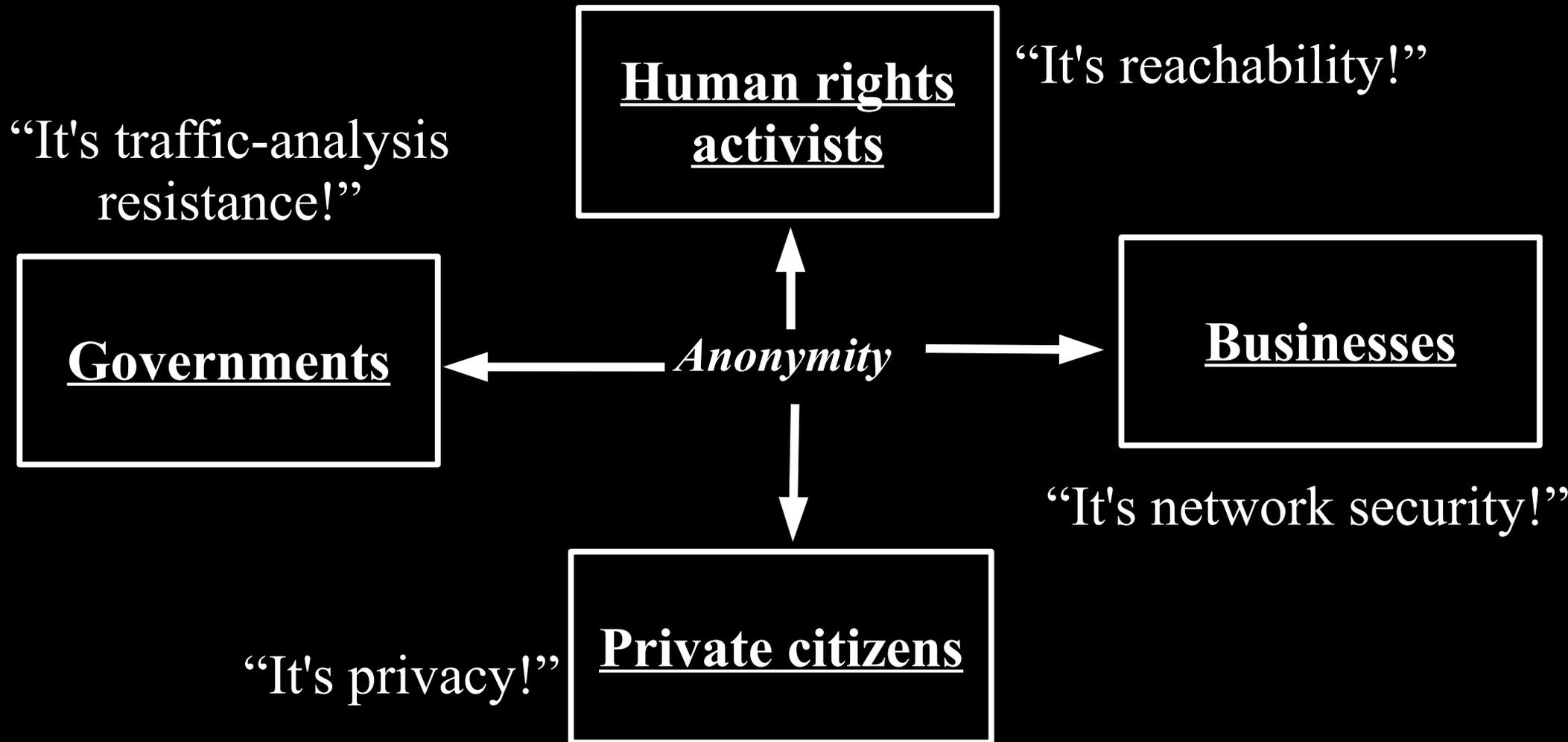Governments ← Anonymity → Businesses

"It's network security!"

↓

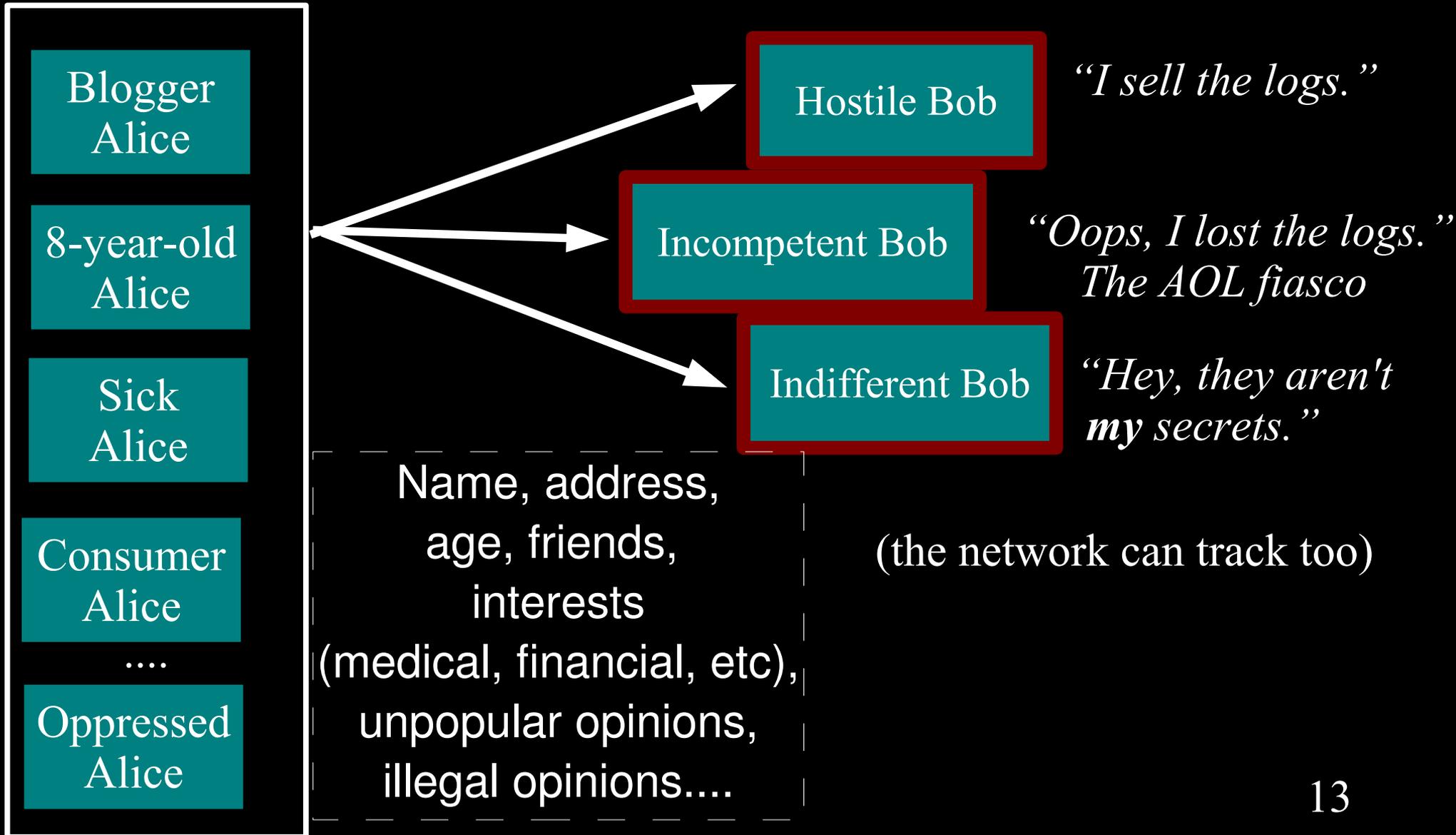Private citizens

"It's privacy!"

10

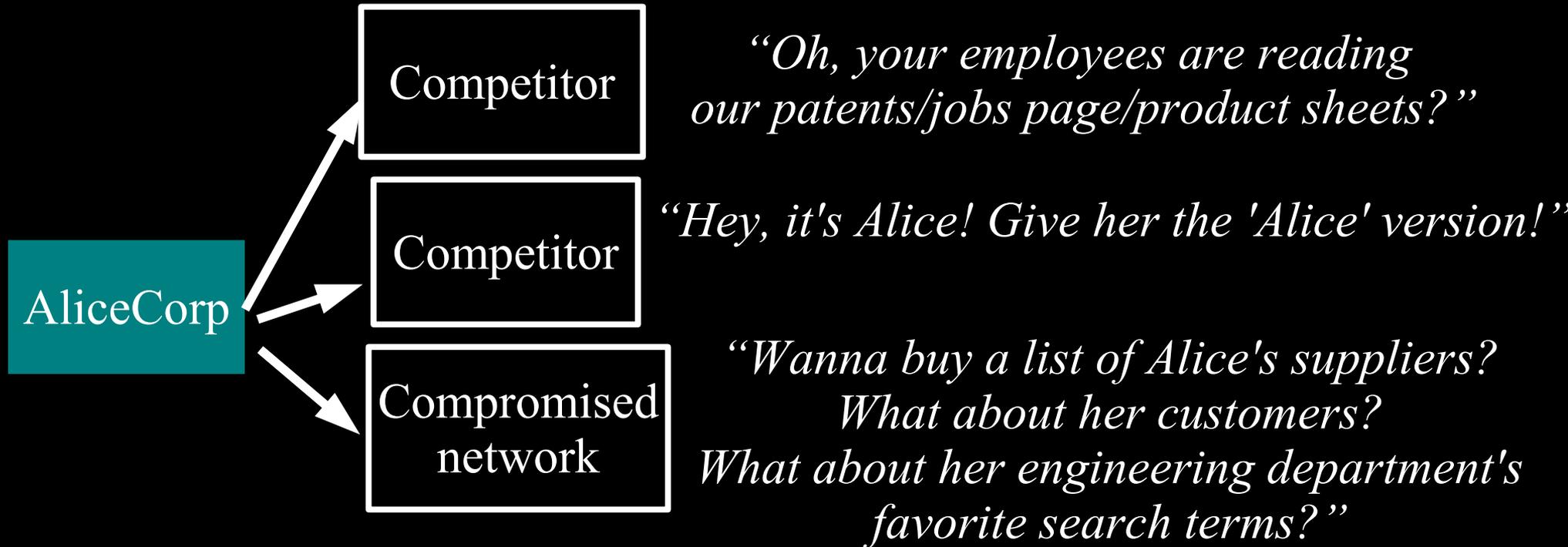# Anonymity serves different interests for different user groups.

Four pieces to today's talk

- 1) Who uses Tor and why?
- 2) The Tor design in a nutshell
- 3) Tor and censorship
- 4) We have data

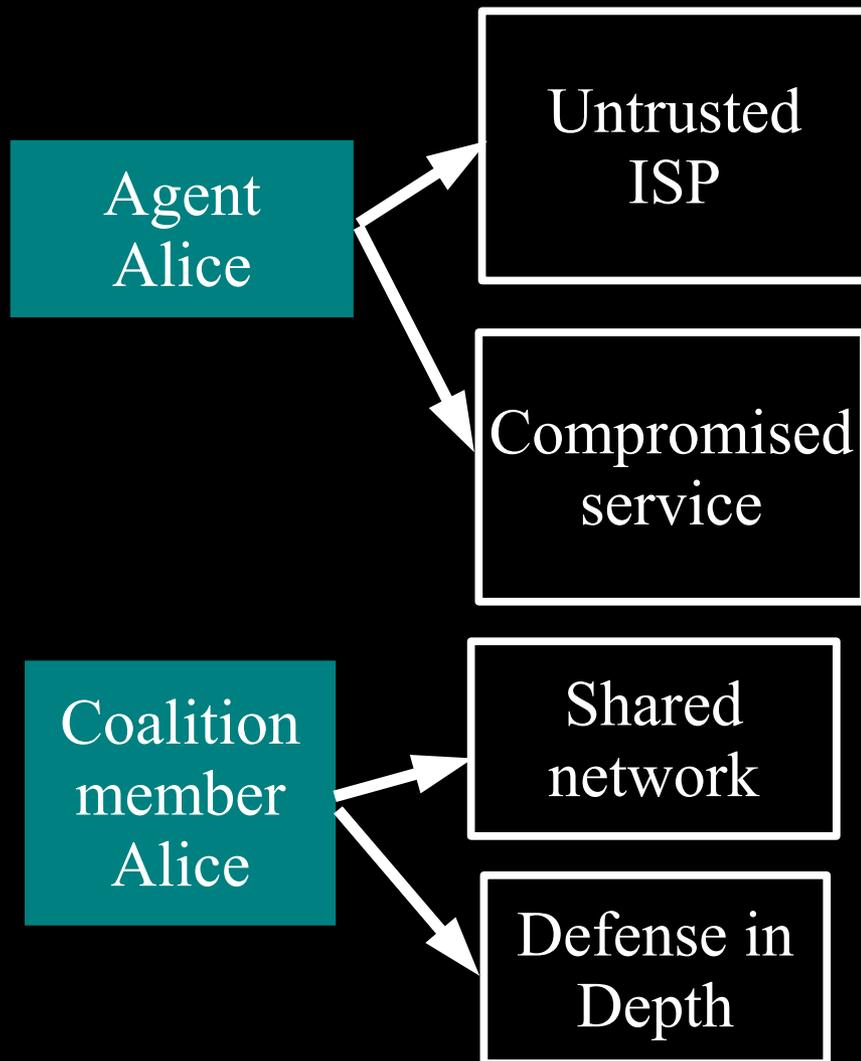# Regular citizens don't want to be watched and tracked.

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)

13

Businesses need to keep trade secrets.

Competitor

Competitor

AliceCorp

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

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

Agent Alice → Compromised service

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

"What does FBI Google for?"

Coalition member Alice → Shared network

"Do I really want to reveal my internal network topology?"

Coalition member Alice → Defense in Depth

"What about insiders?"

16

Journalists and activists need Tor for their personal safety

Activist/ Whistleblower Alice

Monitoring ISP

"Did you just post to that website?"

Monitored website

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

Blocked Alice

Filtered website

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

Monitored network

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

17

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!"*

18
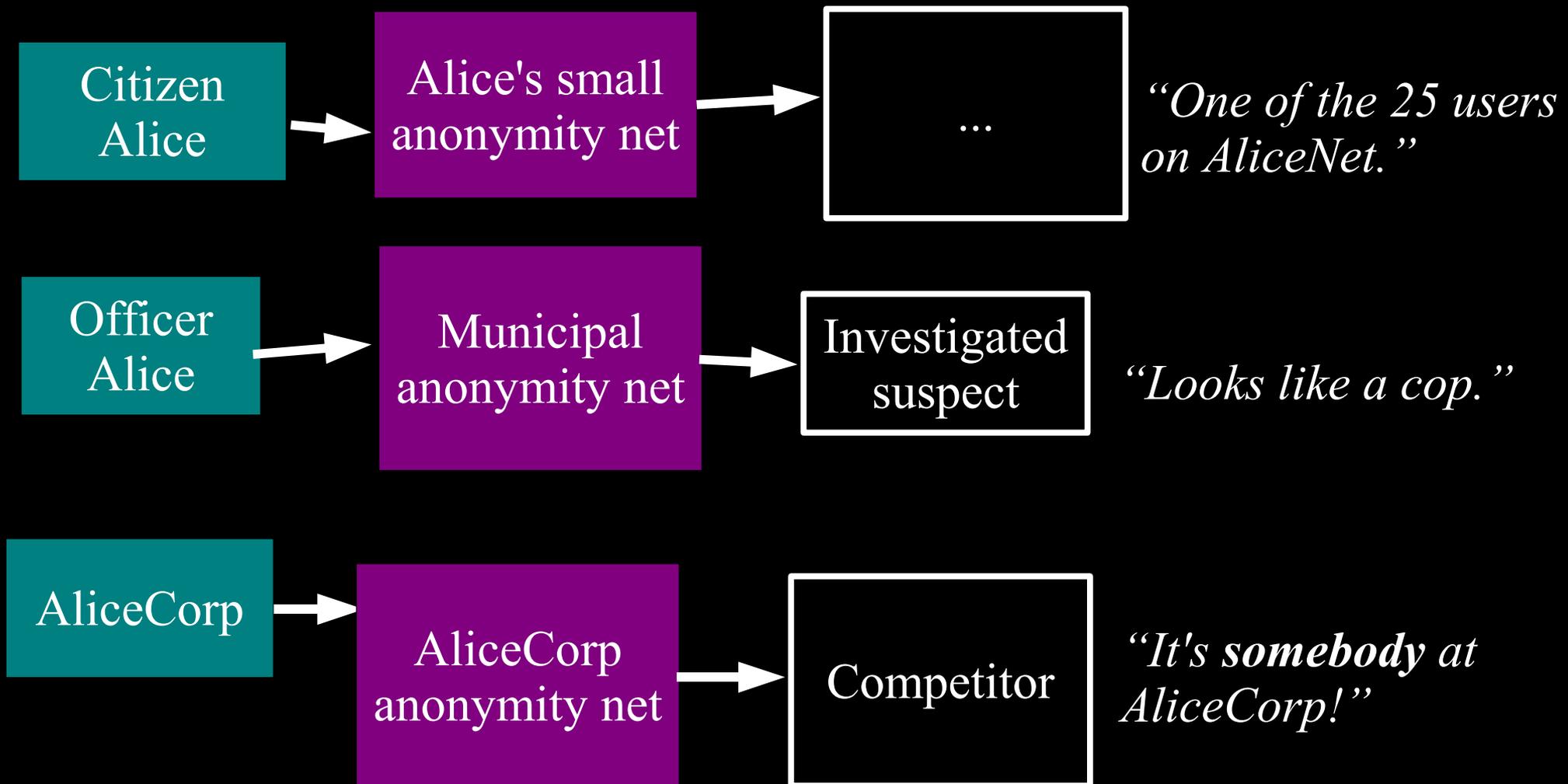
... so, anonymity loves company!

Citizen Alice → Shared anonymity net → ... "???"

Officer Alice → Shared anonymity net → Investigated suspect "???"

AliceCorp → Shared anonymity net → Competitor "???"
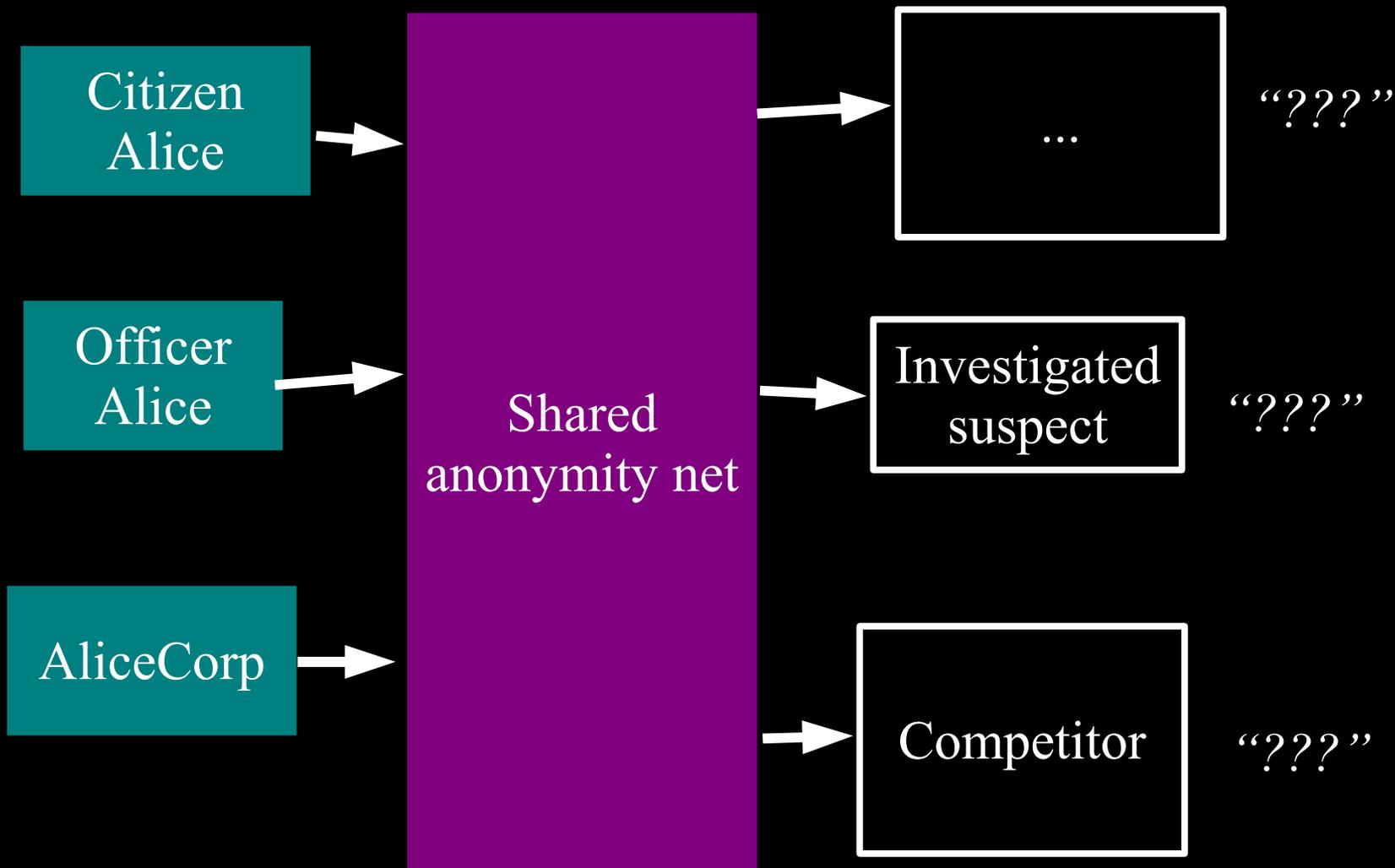
Yes, bad people need anonymity too. But they are *already* doing well.
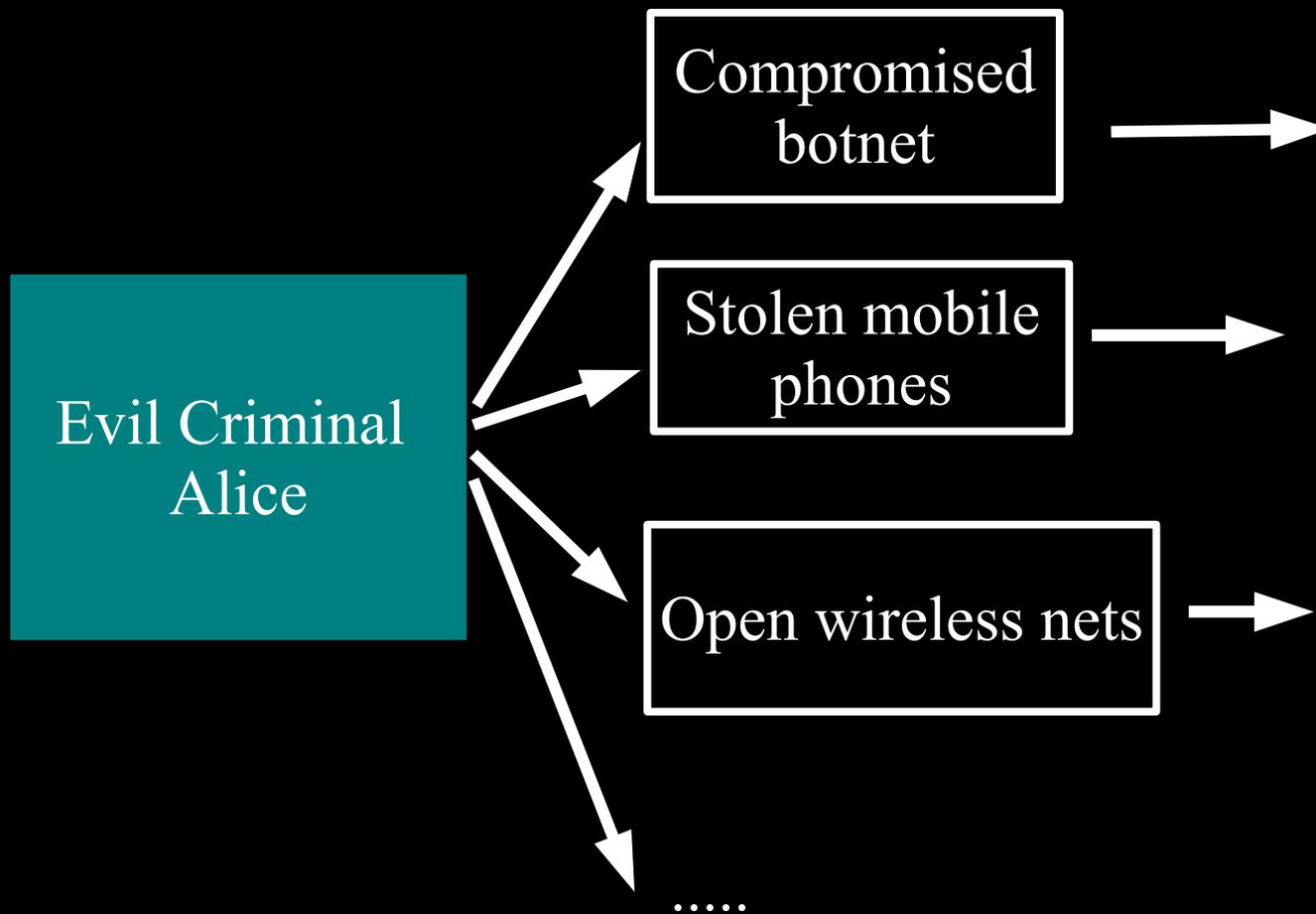
Current situation: Bad people on the Internet are doing fine

21
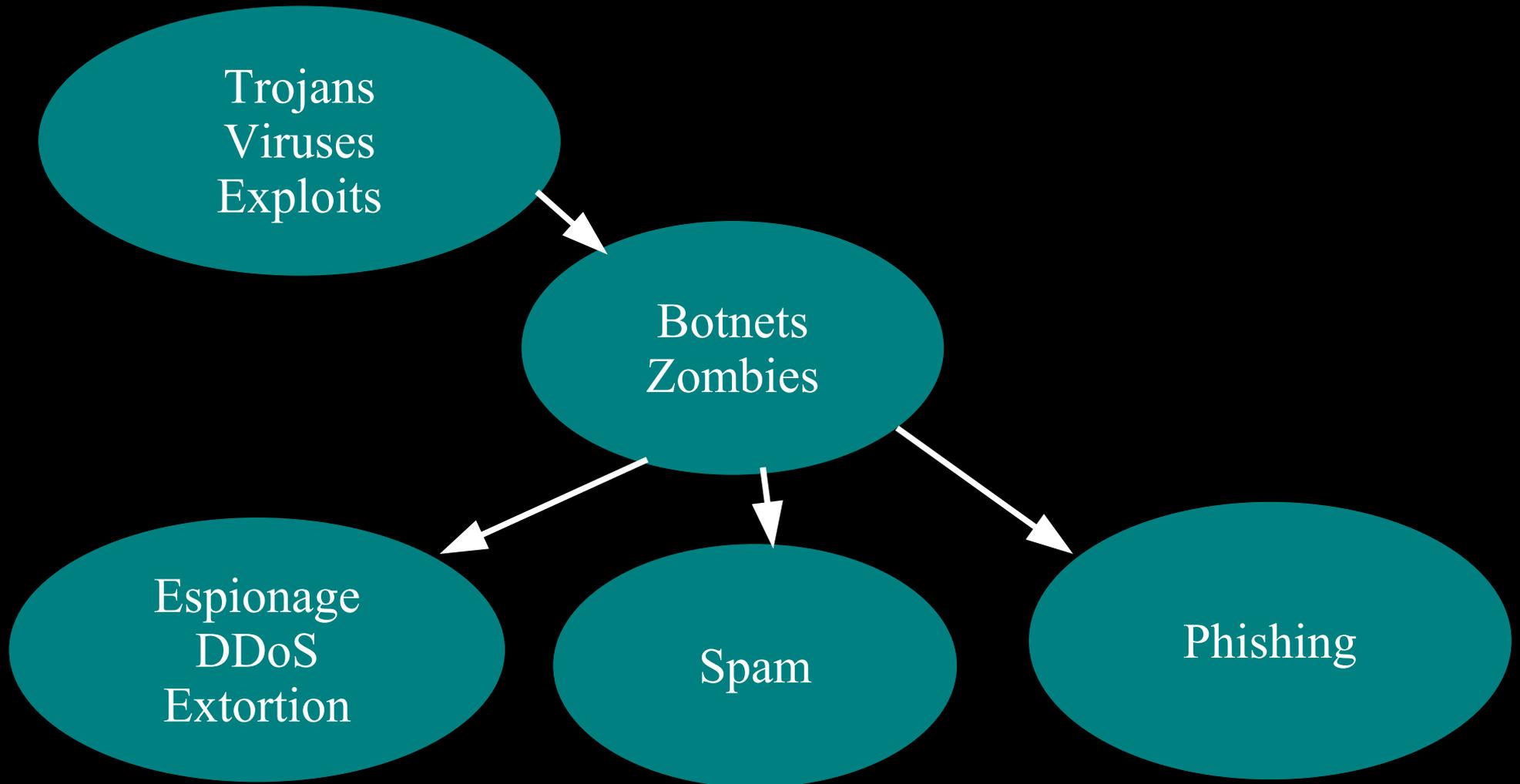
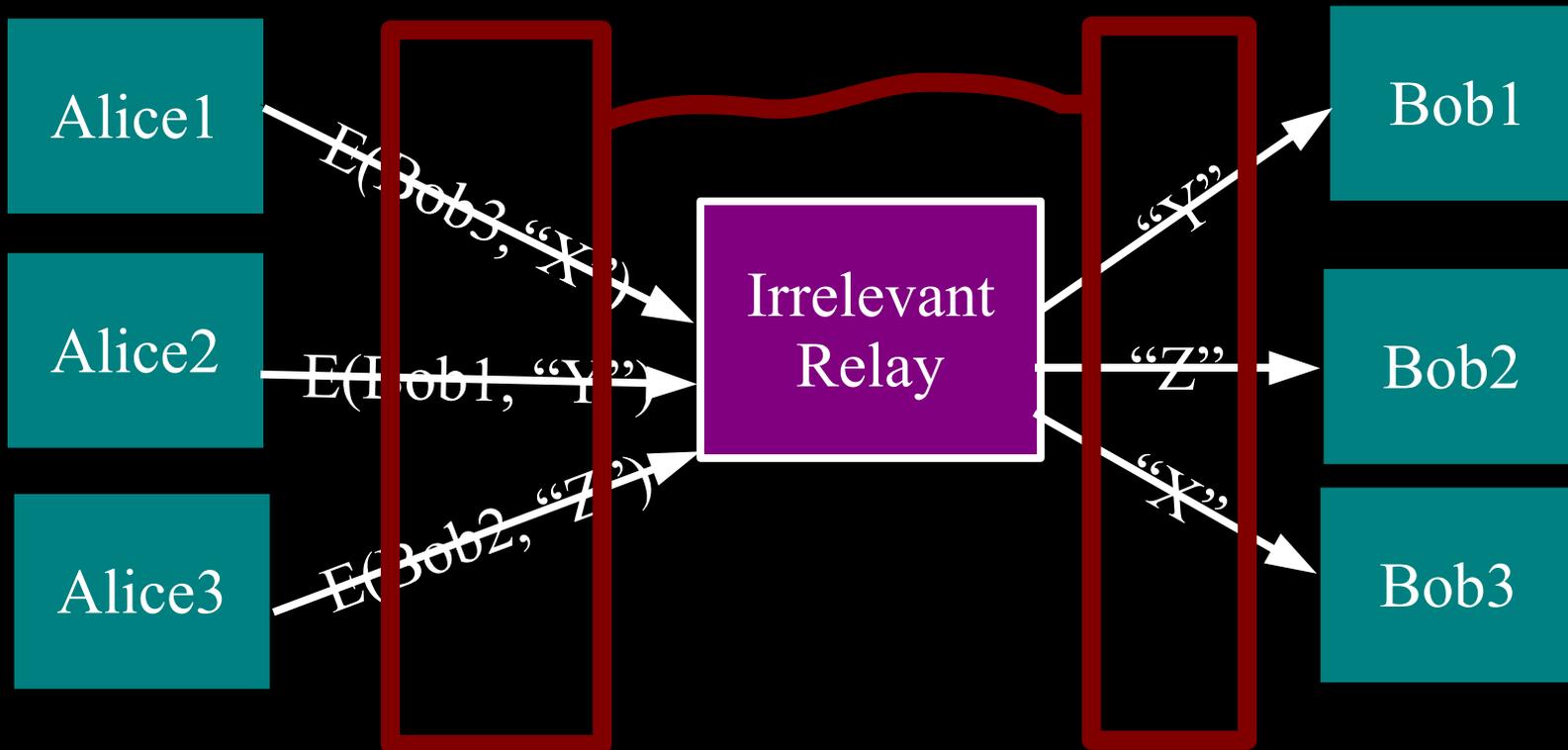# The simplest designs use a single relay to hide connections.
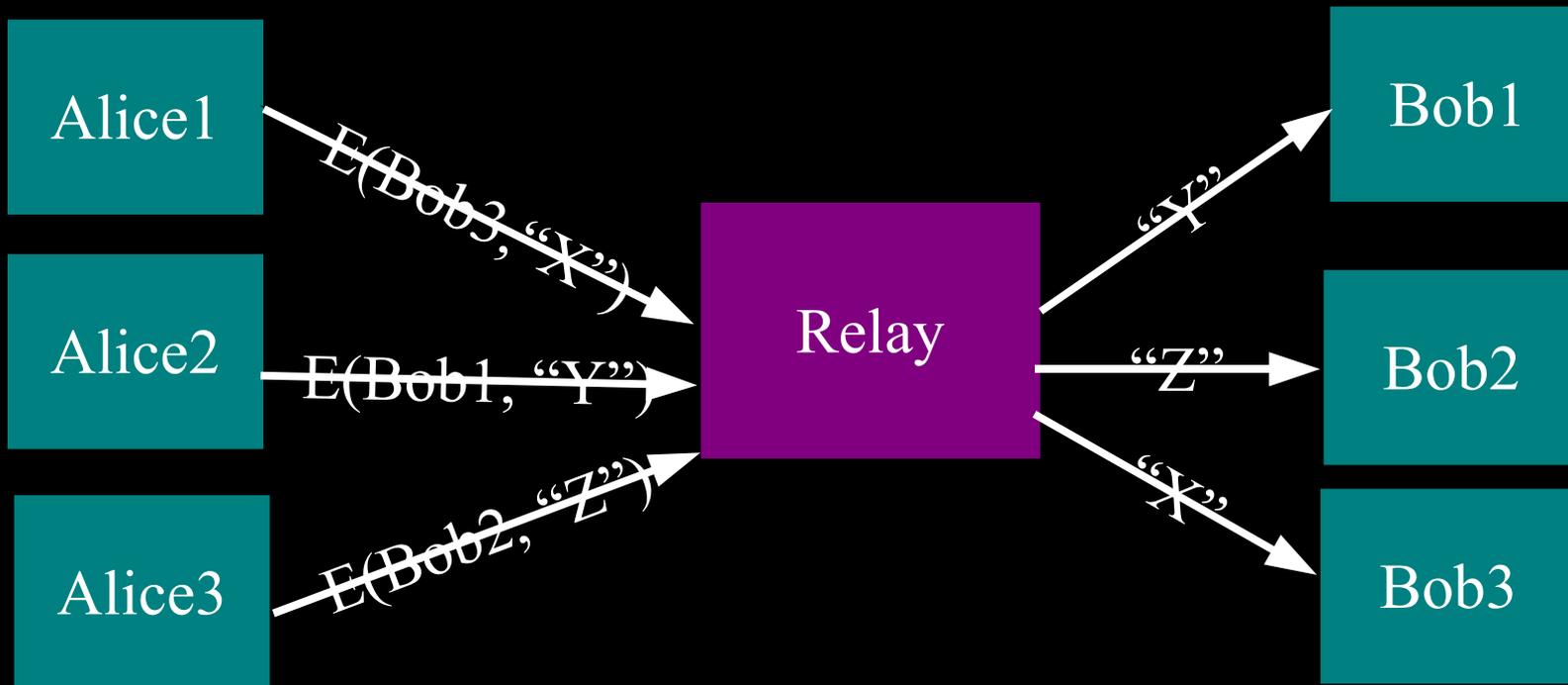
(example: some commercial proxy providers)

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

Alice1 — E(Bob3, "X") → Evil Relay — "Y" → Bob1

Alice2 — E(Bob1, "Y") → Evil Relay — "Z" → Bob2

Alice3 — E(Bob2, "Z") → Evil Relay — "X" → Bob3
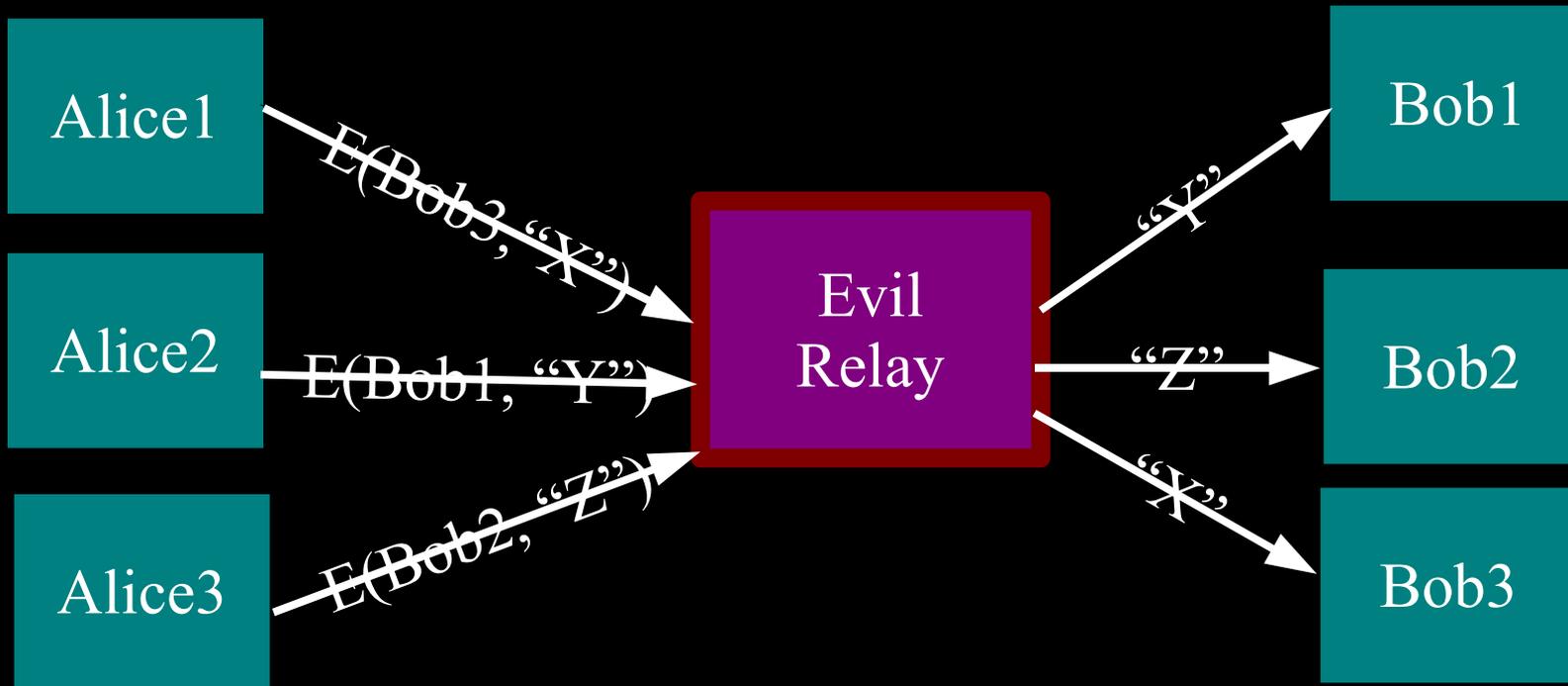
... or a single point of bypass.

Alice1

Alice2

Alice3

E(Bob3, "X")

E(Bob1, "Y")

E(Bob2, "Z")

Irrelevant Relay

"Y"

"Z"

"X"

Bob1

Bob2

Bob3

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

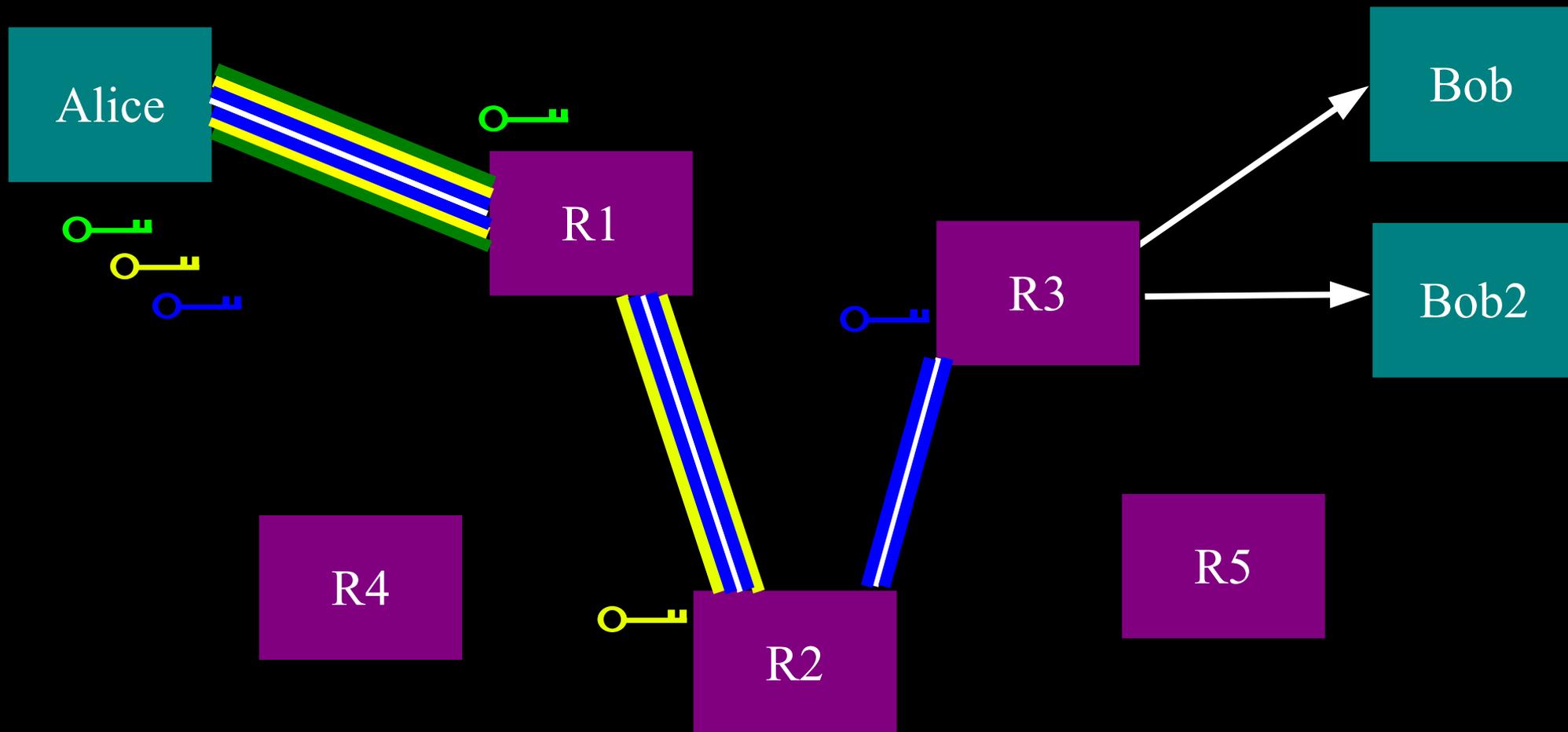# So, add multiple relays so that no single one can betray Alice.
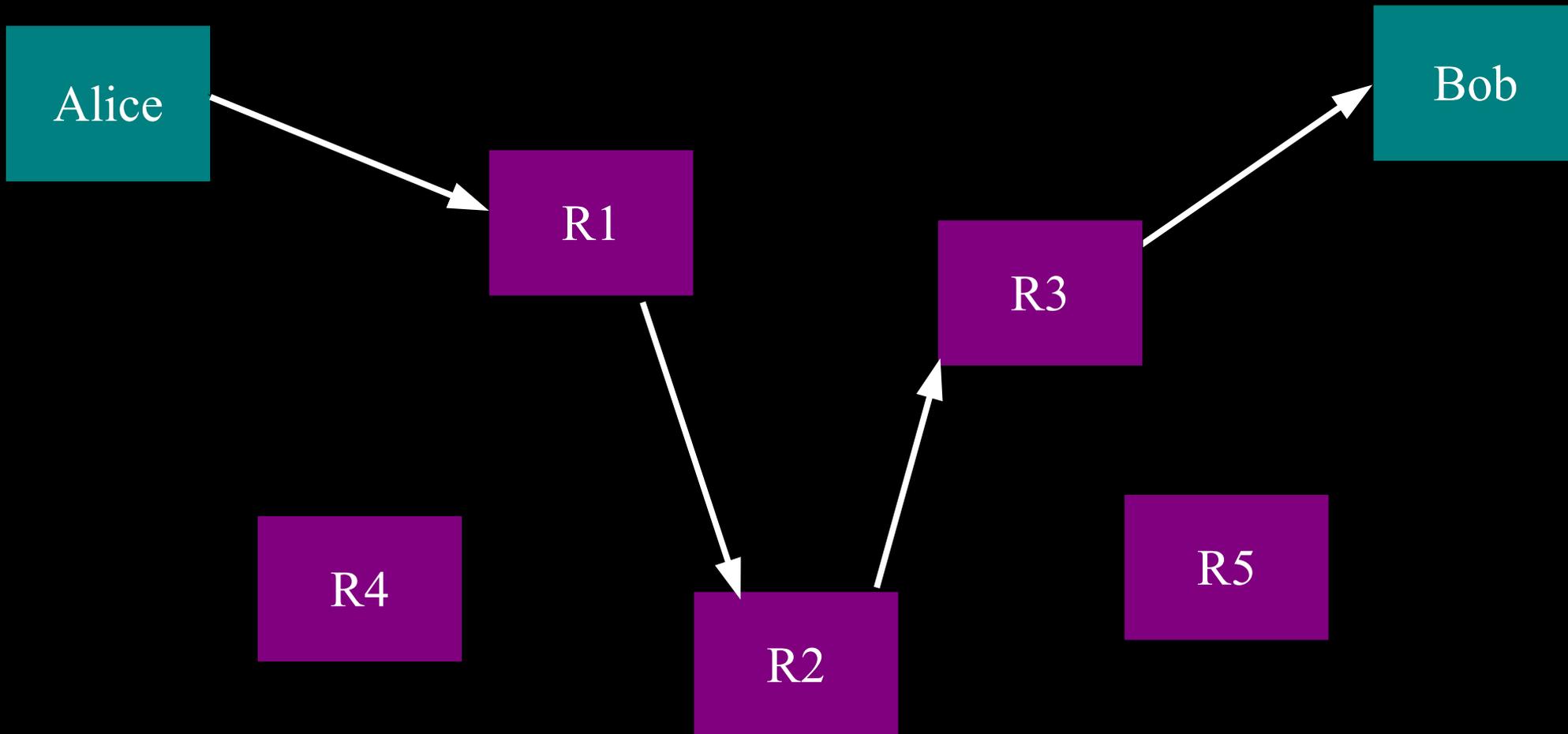
A corrupt first hop can tell that Alice is talking, but not to whom.
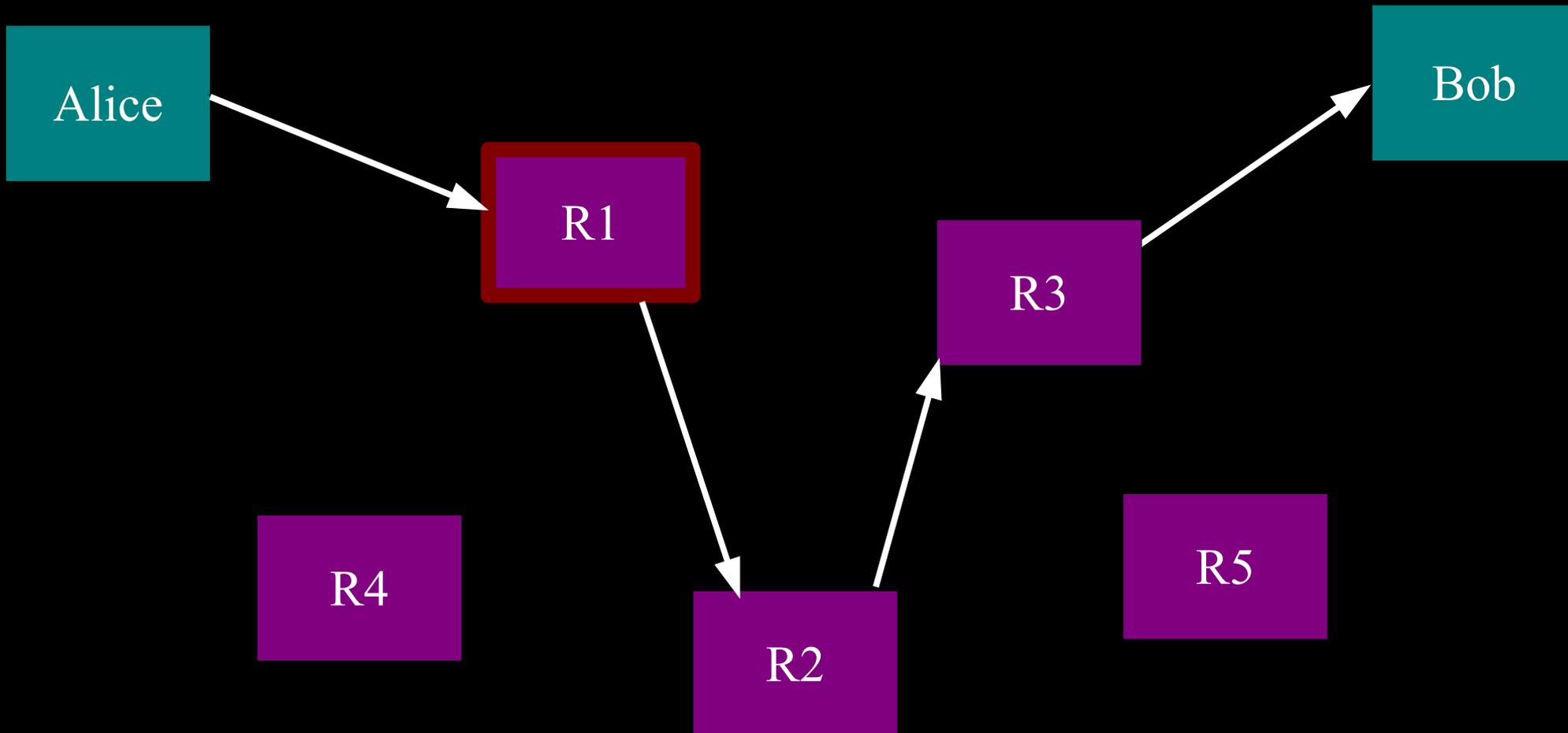
A corrupt final hop can tell that somebody is talking to Bob, but not who.

Alice

R1

R3

Bob

R4

R2

R5
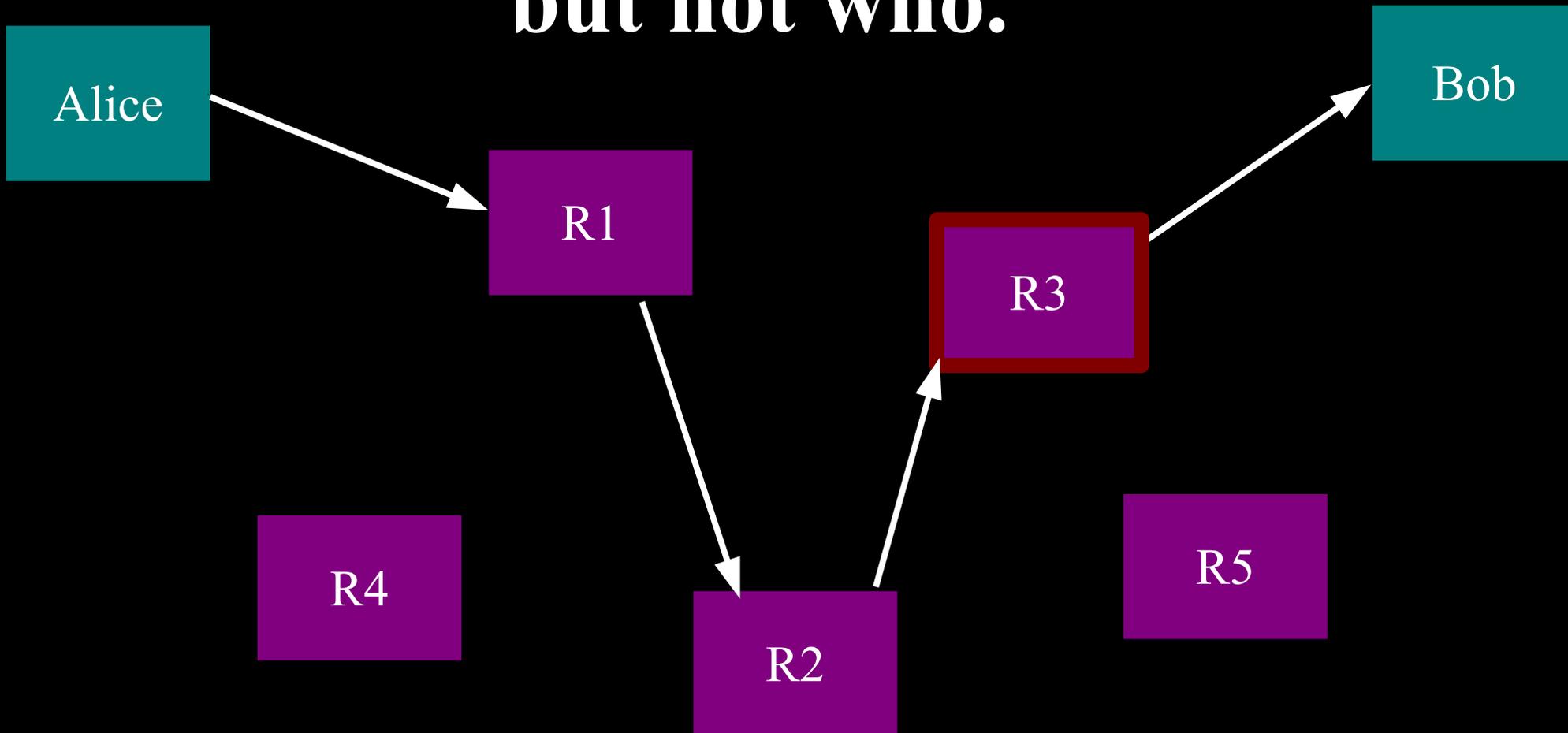
Alice makes a session key with R1 ...And then tunnels to R2...and to R3
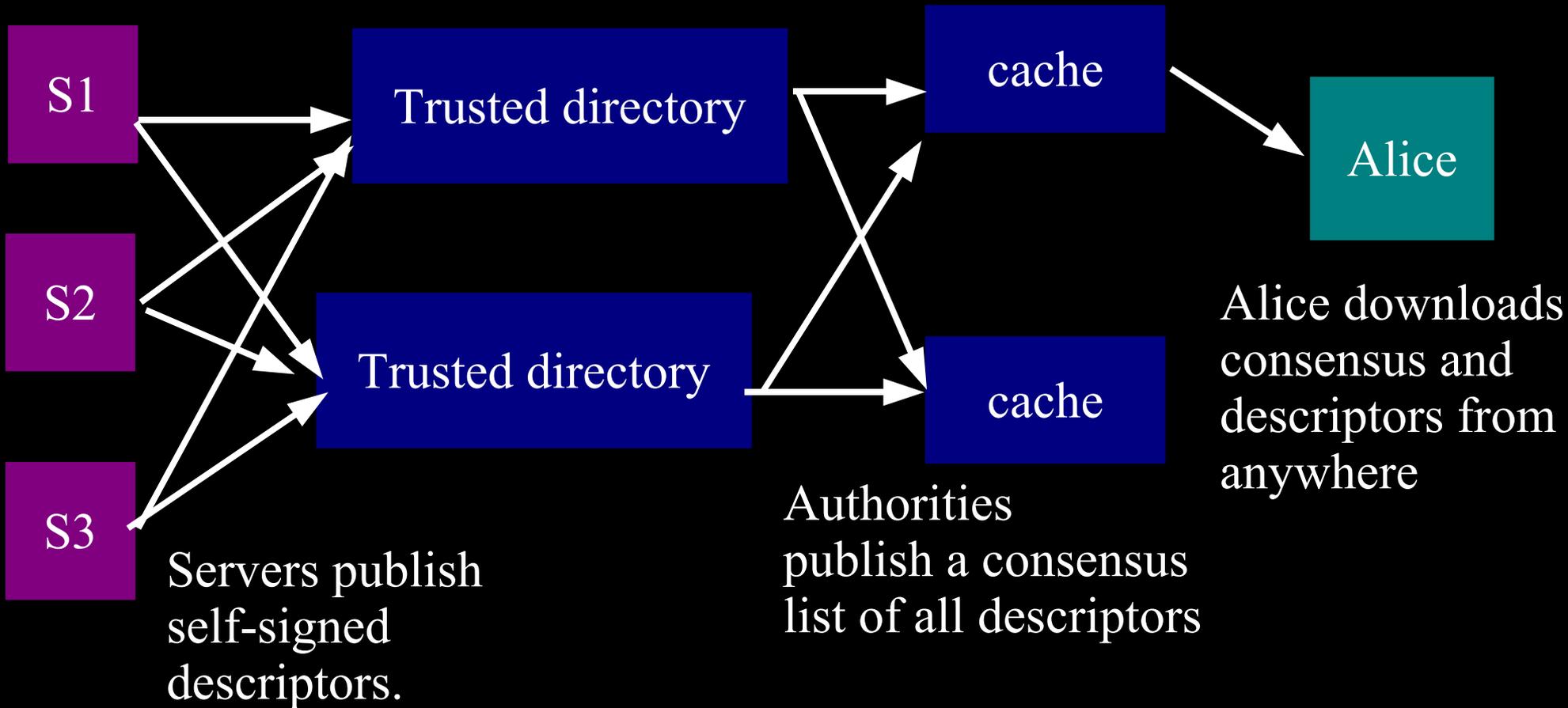
What we spend our time on

- 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

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.

S1

S2

S3

Trusted directory

Trusted directory

cache

cache

Alice

Servers publish self-signed descriptors.

Authorities publish a consensus list of all descriptors

Alice downloads consensus and descriptors from anywhere

# 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

33
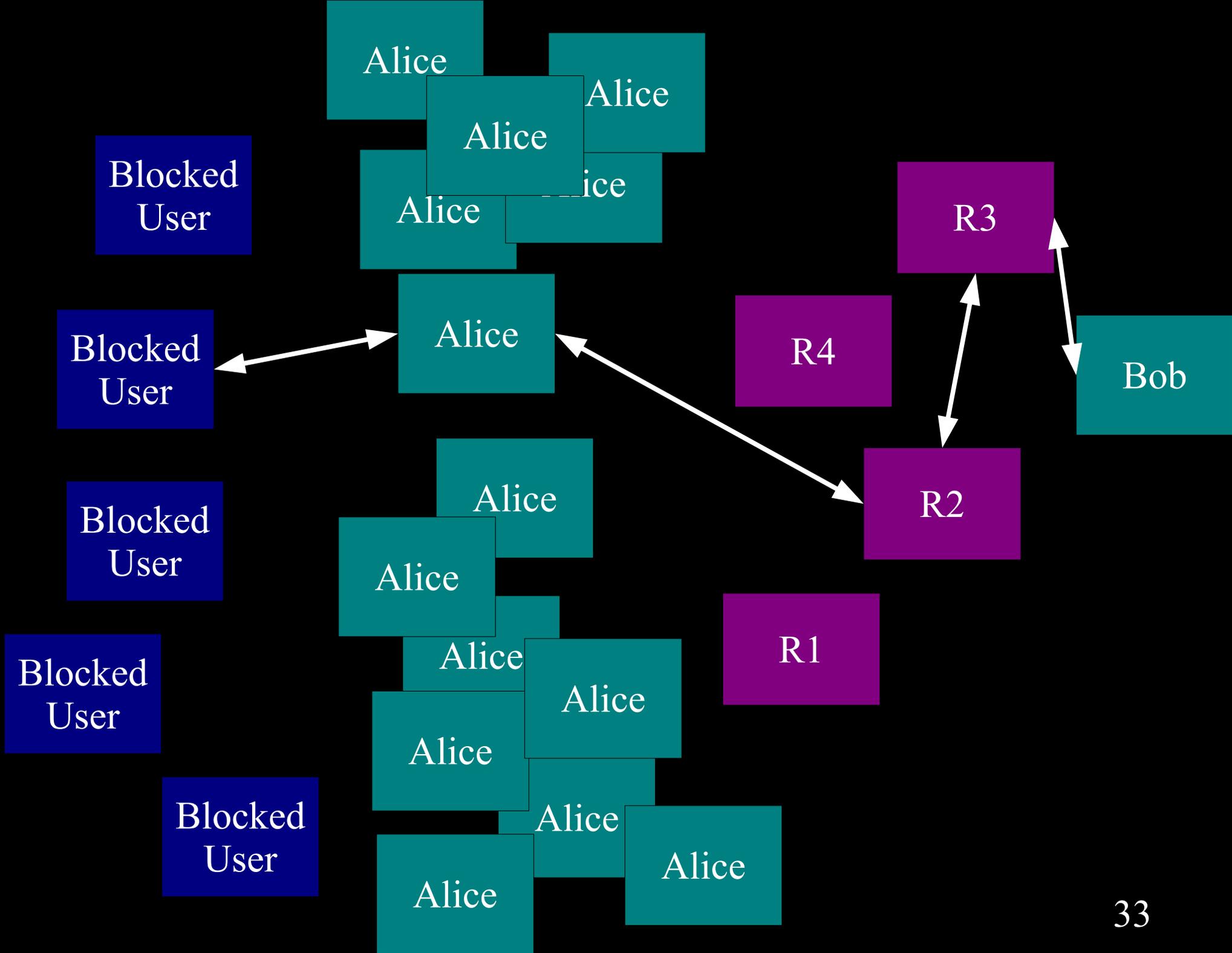
"Bridge" relays

- 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
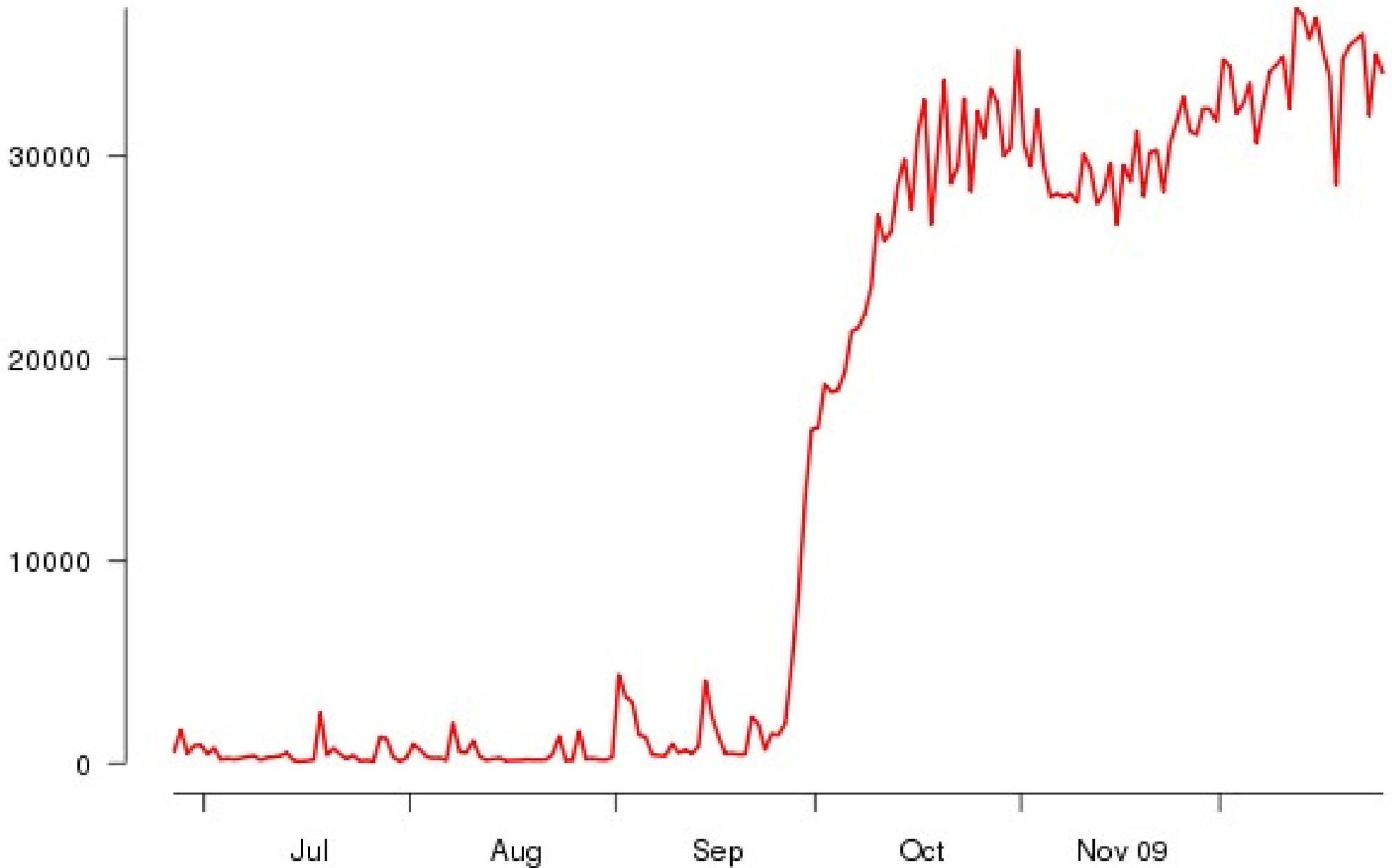
New or returning Tor clients per day

https://torproject.org

35
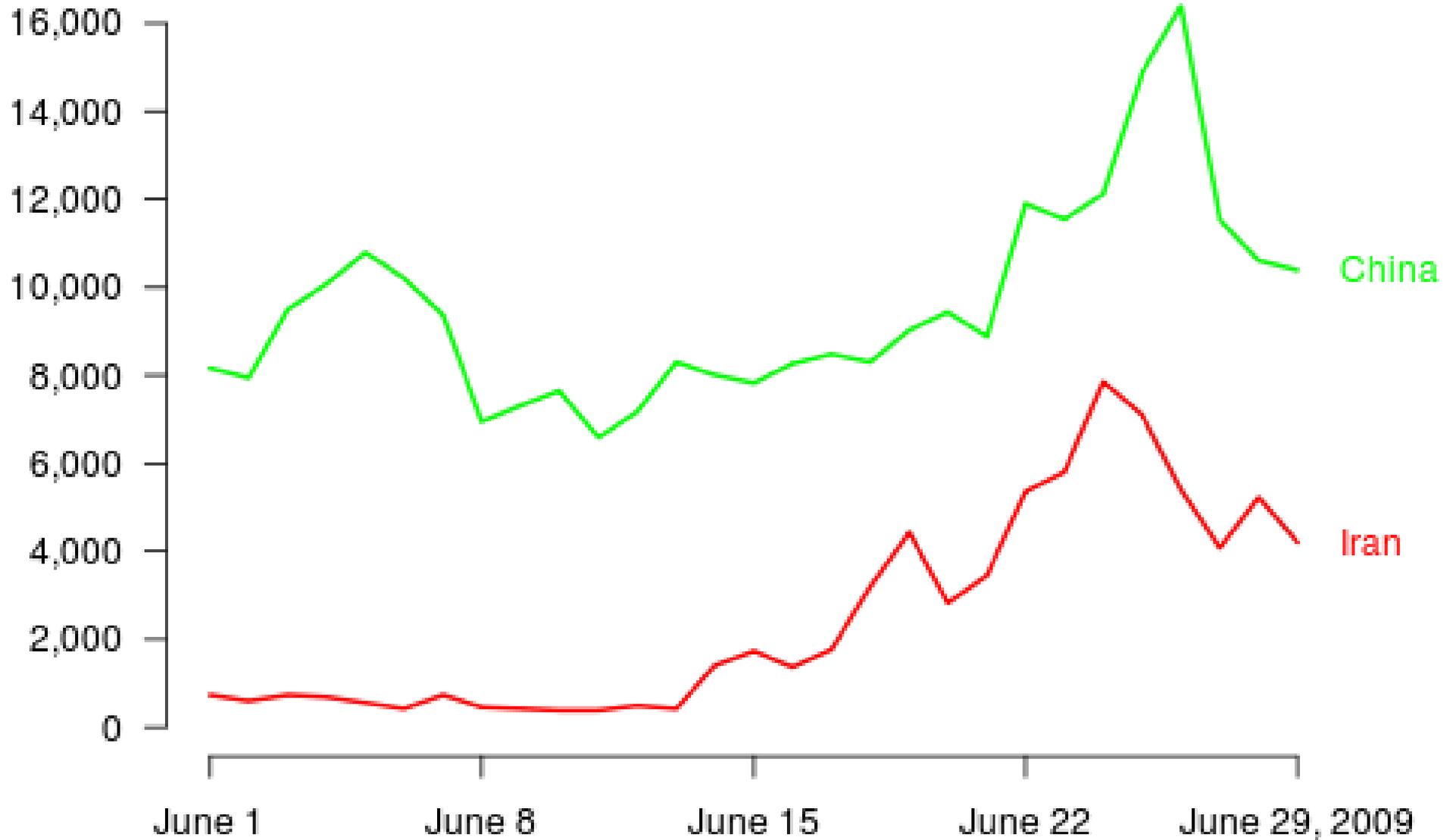
Number of directory requests to directory mirror trusted

China

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

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)

- 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

- 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?

Javascript, cookies, history, etc

- Javascript refresh attack
- Cookies, History, browser window size, user-agent, language, http auth, ...
- Mostly problems when you toggle from Tor to non-Tor or back
- Mike Perry's 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?

Choose how to install it

- Tor Browser Bundle: standalone Windows exe with Tor, Vidalia, Firefox, Torbutton, Polipo, e.g. for USB stick
- Vidalia bundle: Windows/OSX installer
- Tor VM: Transparent proxy for Windows
- "Net installer" via our secure updater
- Amnesia Linux LiveCD

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

- Users can fetch a genuine copy of Tor?

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 2009 were coming through Tor
  - 90% were coming from proxies in the Amazon cloud

Trust and reputation

- See Hal Roberts' January 2009 blog post about how some circumvention tools sell user data

- Many of these tools see circumvention and privacy as totally unrelated goals

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)

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 500.

- We'd love to help with some trainings, to help users and to make Tor better.

Our NSF EAGER

- 1) Invent and deploy new privacy-preserving algorithms to collect data about the Tor network, its performance, and its users

- 2) Publish this data, plus tools to analyze it

- 3) Figure out what else to measure and do it

- 4) Work with other research groups to make sure they get the data they need to solve the problems Tor actually has

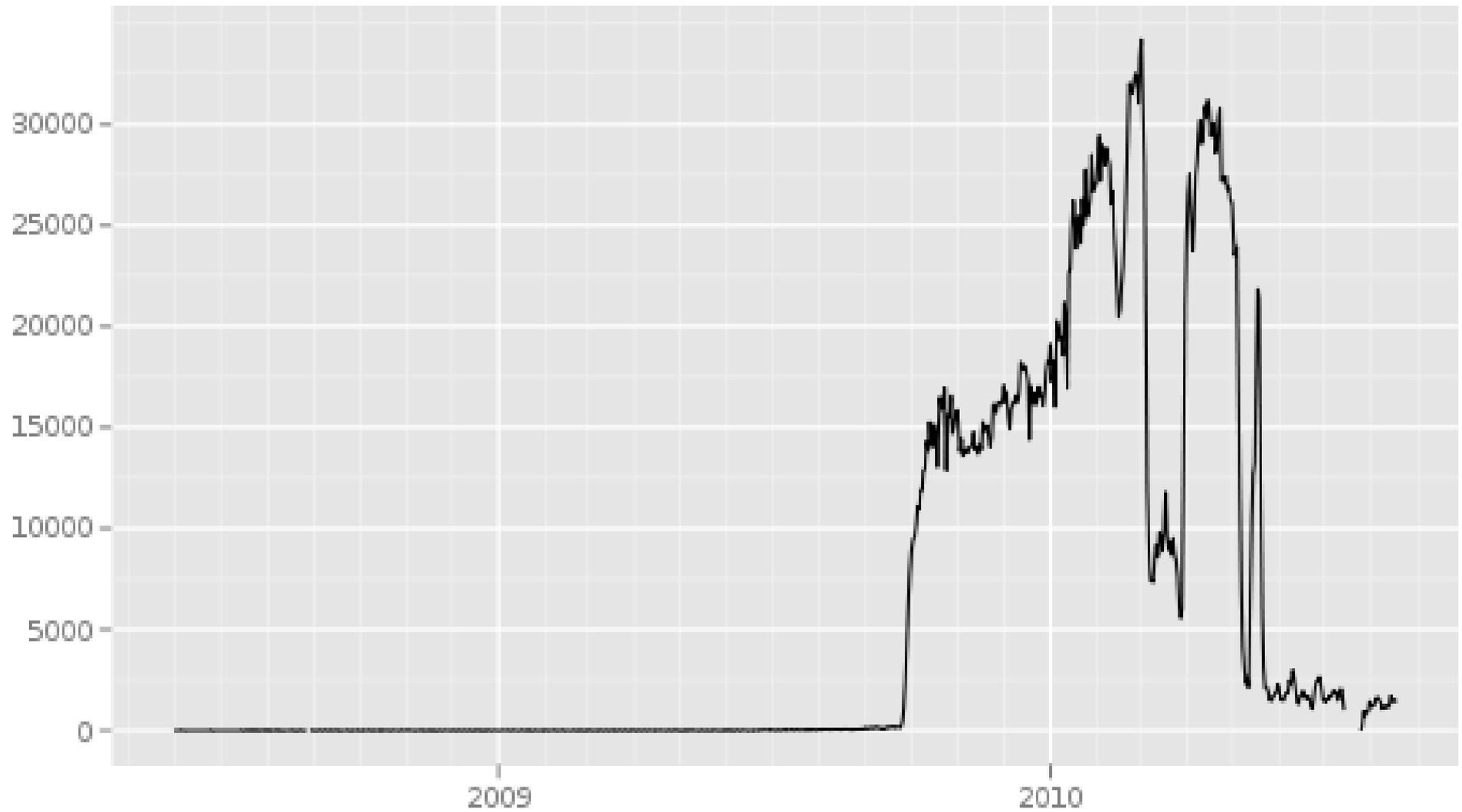# Recurring, directly connecting Chinese Tor users (all data)

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

58
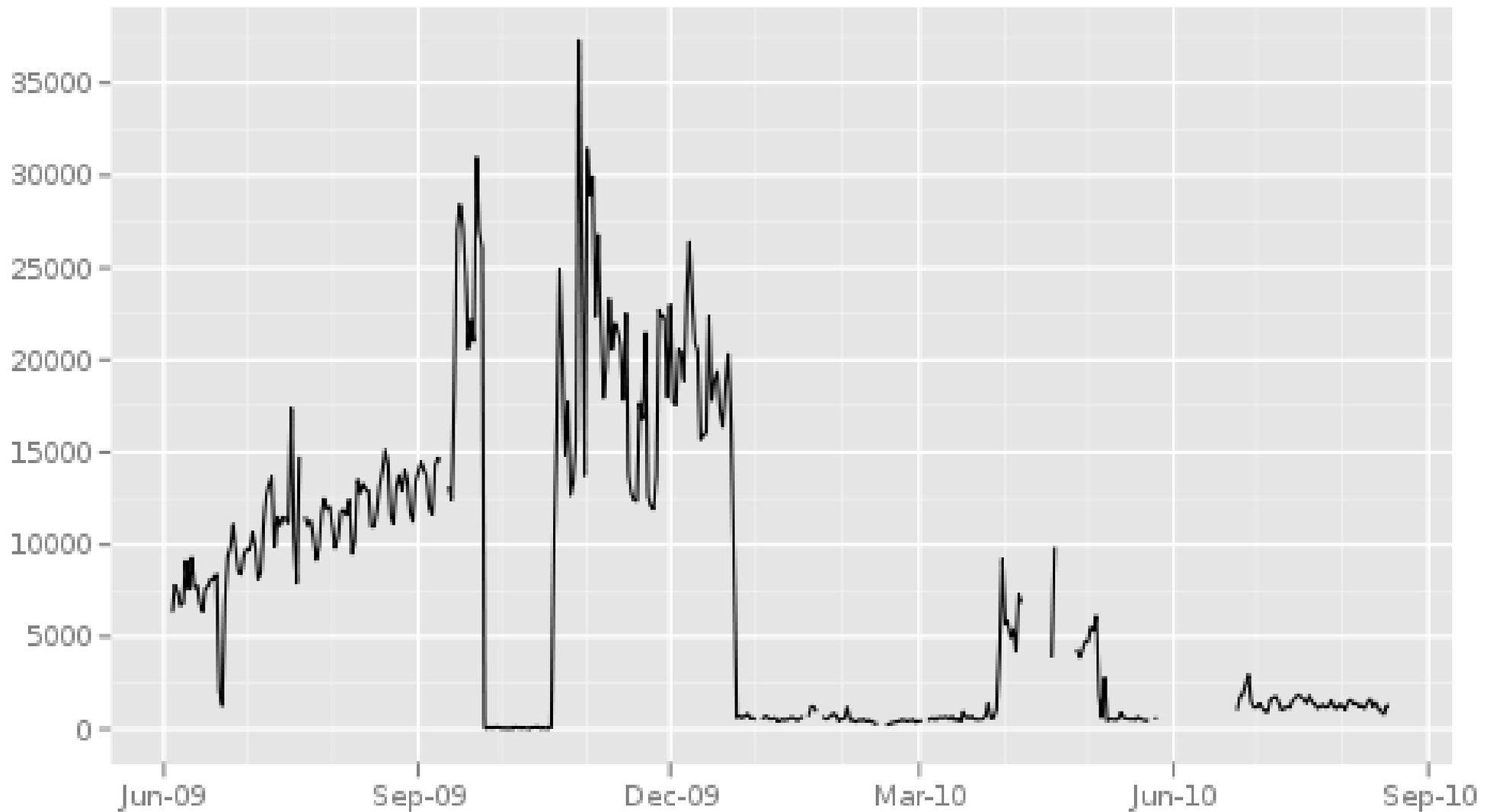
Recurring, directly connecting Iranian Tor users (all data)

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

Chinese Tor users via bridges (all data)

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

60
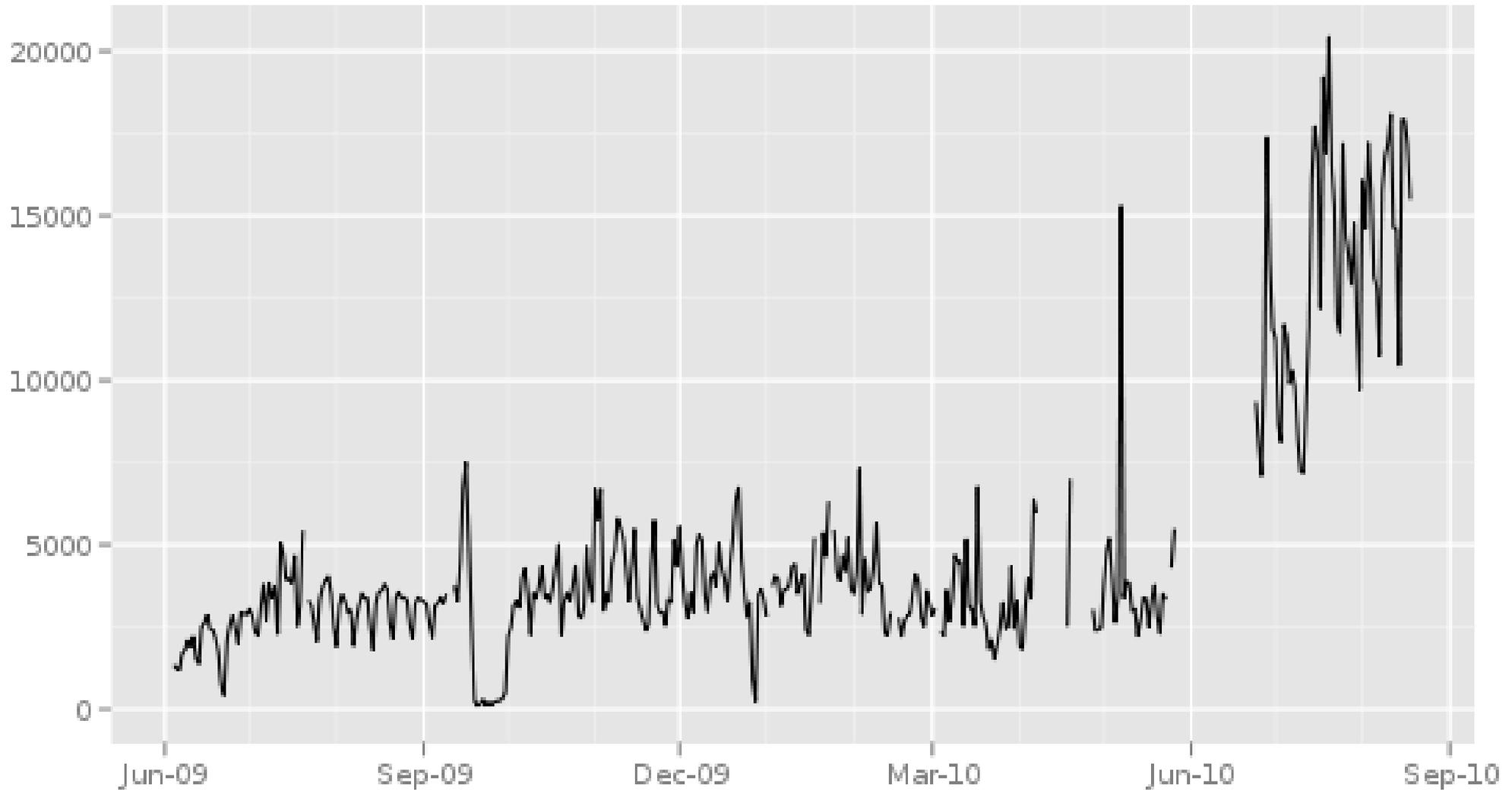
Iranian Tor users via bridges (all data)

The Tor Project - https://metrics.torproject.org/
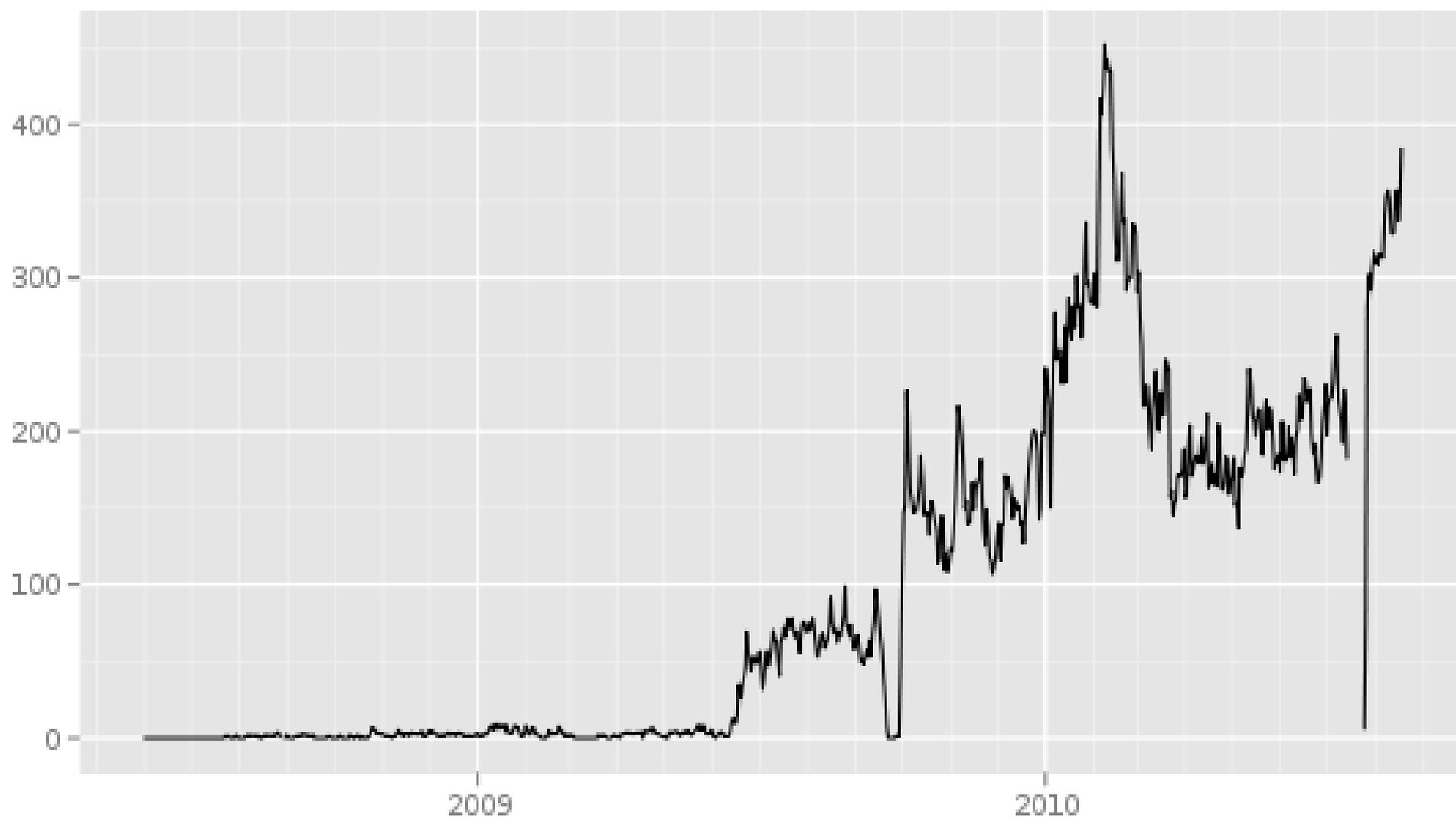
Recurring, directly connecting South Korean Tor users (past 90 days)

The Tor Project - https://metrics.torproject.org/
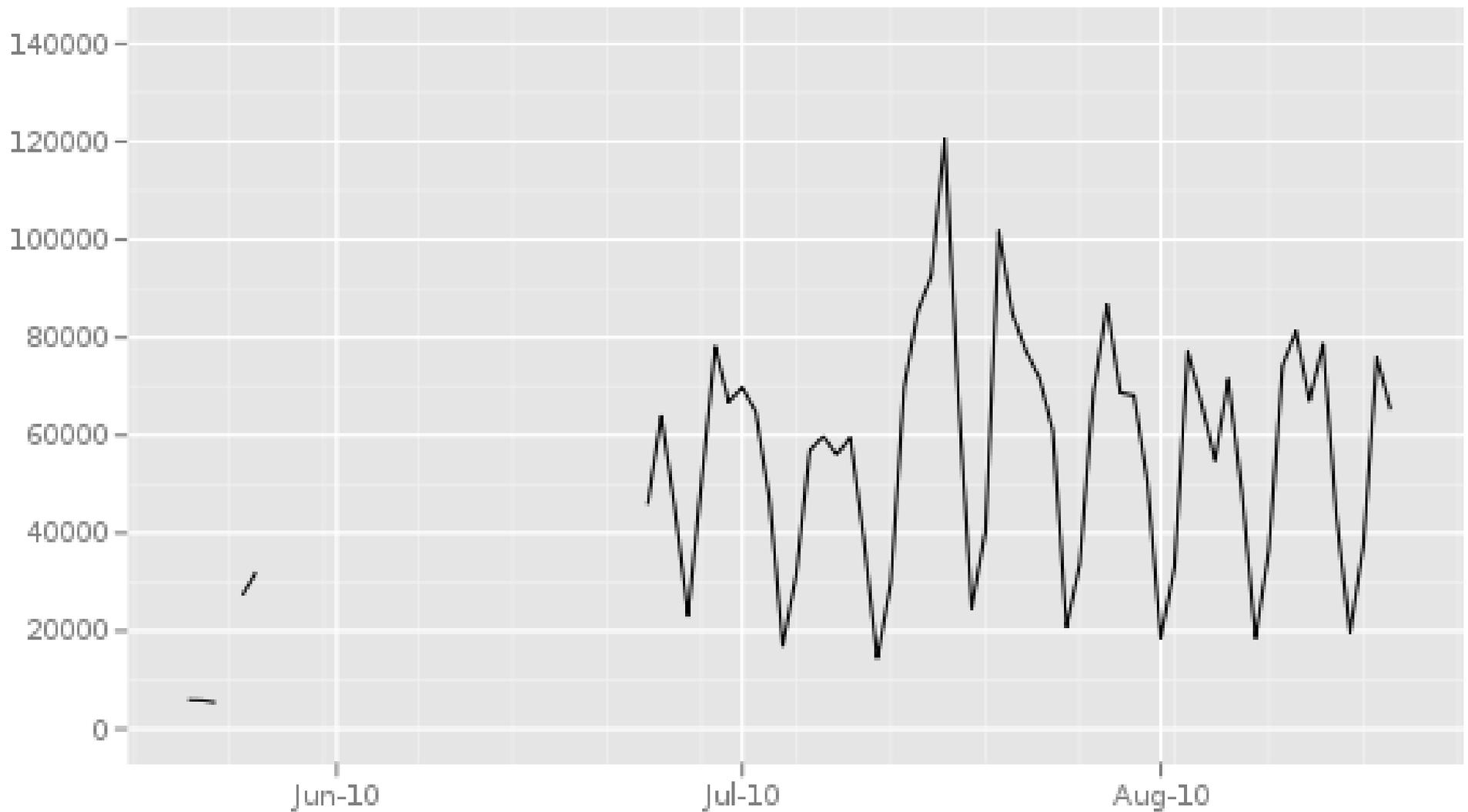
Number of relays and bridges (all data)

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

63
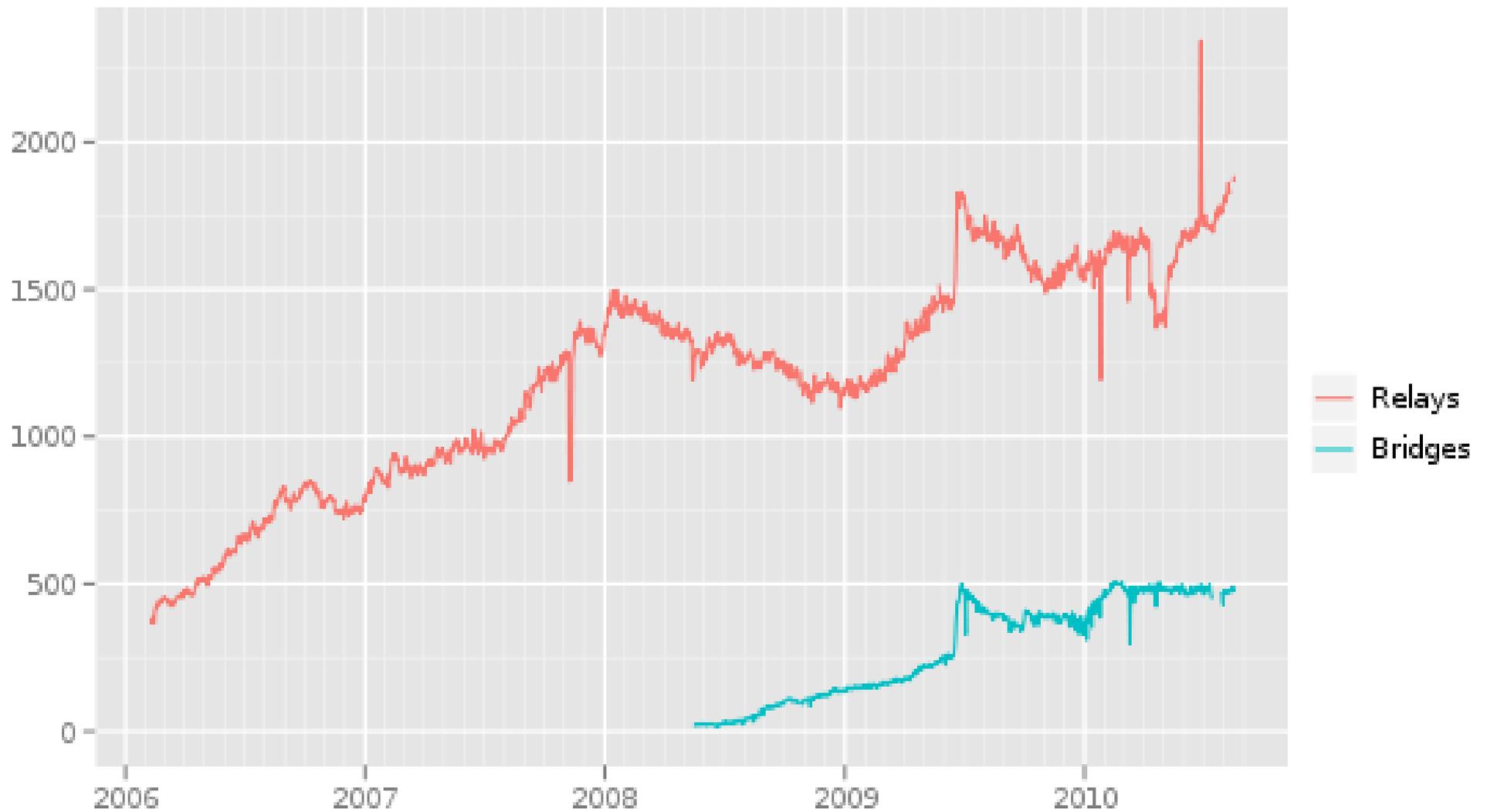
Time in seconds to complete 50 KiB request

Measured times on moria per day

Median

1st to 3rd quartile

The Tor Project - https://metrics.torproject.org/
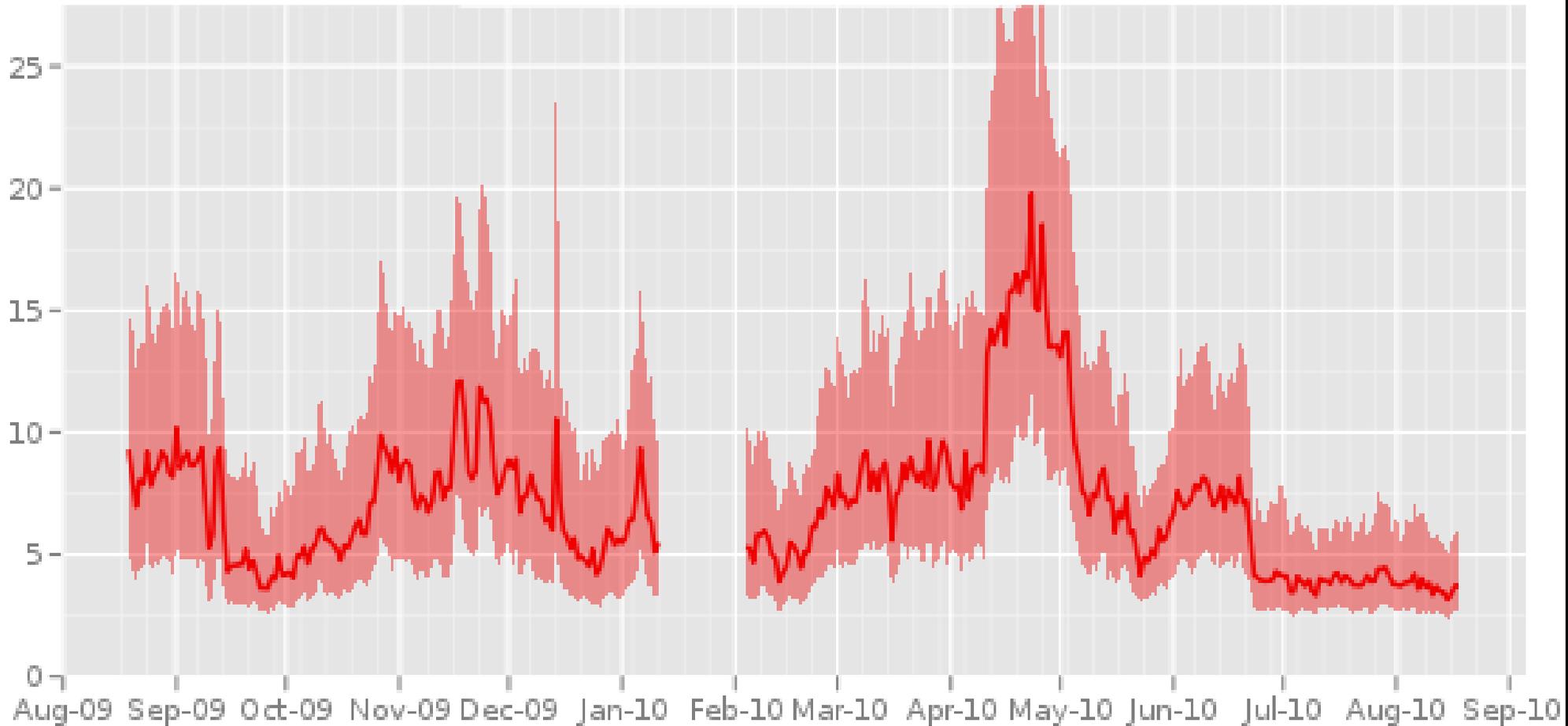
Download times for 50 KiB files