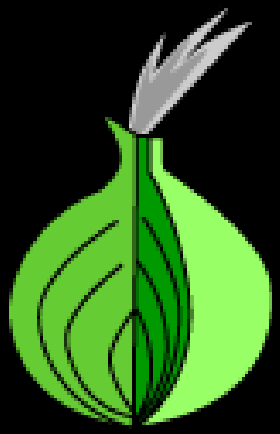
Internet Dagarna 2009:
Allt du gör kan användas mot dig



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

Tor: Big Picture

- Freely available (Open Source), unencumbered.
- Comes with a spec and full documentation: Dresden and Aachen implemented compatible Java Tor clients; researchers use it to study anonymity.
- 1500 active relays, 200000+ active users, >1Gbit/s.
- Official US 501(c)(3) nonprofit. Eight funded developers, dozens more dedicated volunteers.
- Funding from US DoD, Electronic Frontier Foundation, Voice of America, Human Rights Watch, Google, NLnet, ...you?
- Privacy and anonymity by *Design!*

Tor & 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.
- Come join us; we'd love to have you on board.

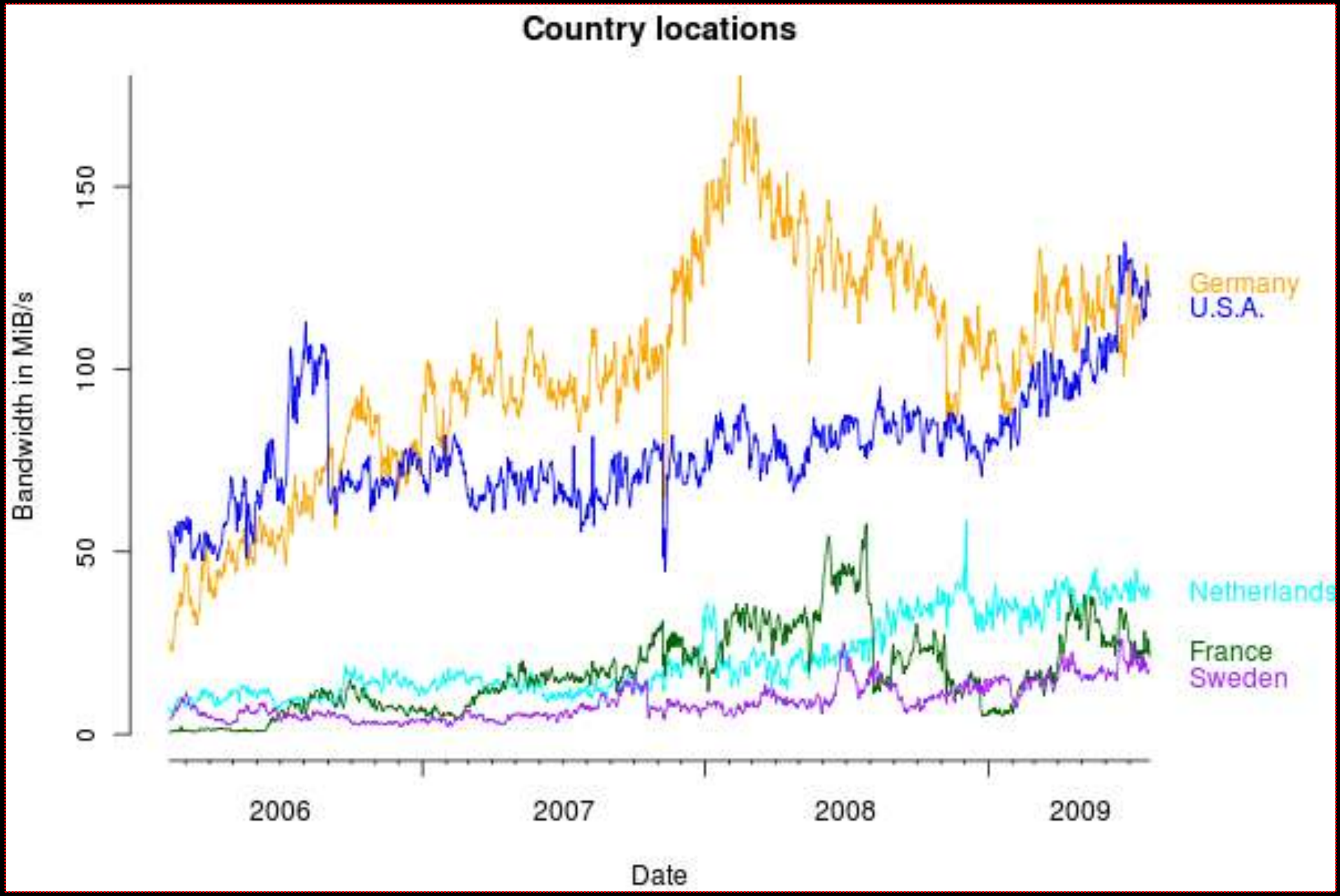
Privacy by Design
(http://www.privacybydesign.ca/)

The philosophical ideas of Privacy by Design:

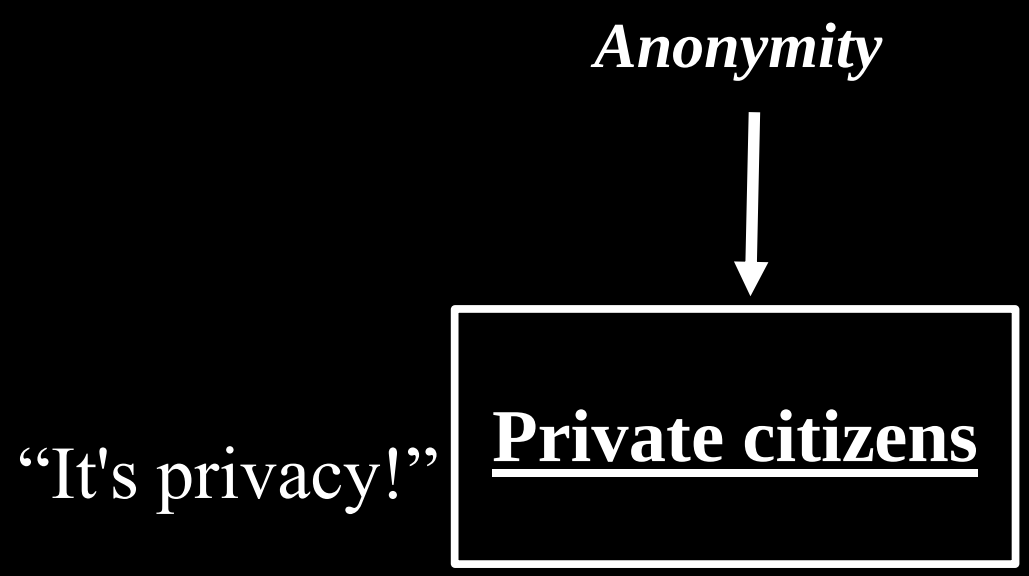
Proactive and Preventative
Privacy is *the* default
Privacy is a *core* component of design
Privacy does not limit functionality
Full protection during a products life cycle
Visibility and Transparency
Respect for a users privacy

Tor: The Swedish Picture

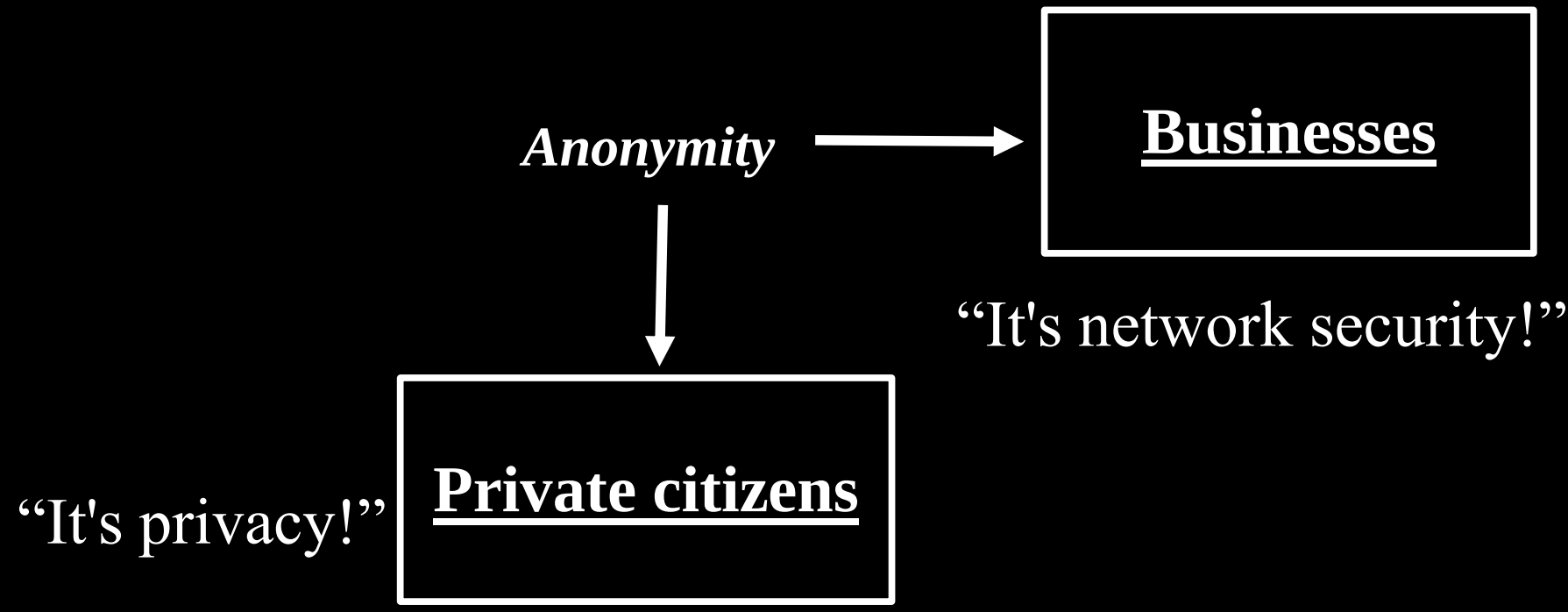
- Sweden has a world wide reputation of respecting, promoting and enhancing human rights.
- As of Nov 4th, 2009 there are currently ~63 *relays* in Sweden.
- These relays account for ~20 - 25Mb/s of advertised bandwidth.
- Support comes from **private individuals**, *educational institutions* and many others; everyone decides their own level of participation.


Country locations
Bandwidth in MiB/s
0
50
100
150
2006
2007
2008
2009
Date
Germany
U.S.A.
Netherlands
France
Sweden

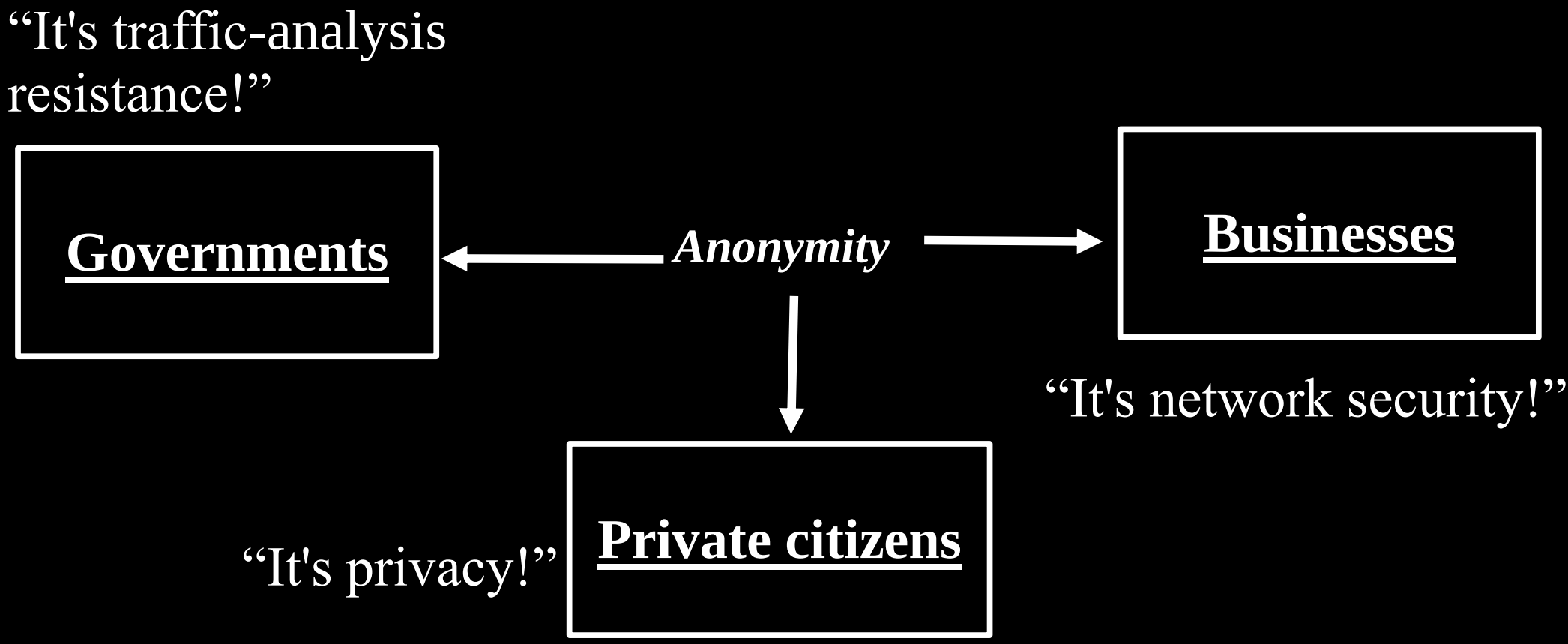
Anonymity serves different interests for different user groups.



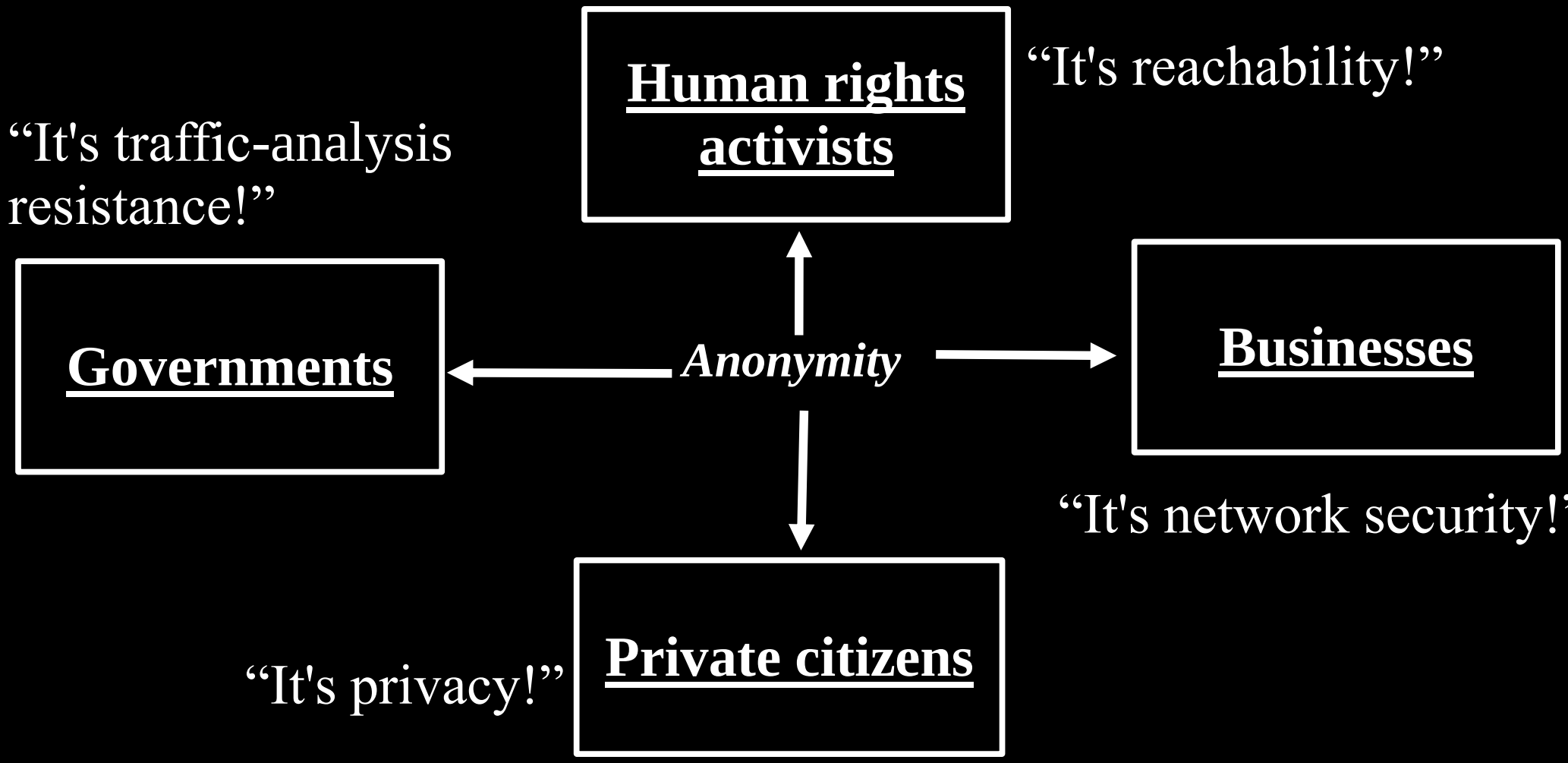
Anonymity serves different interests for different user groups.



Anonymity serves different interests for different user groups.



Anonymity serves different interests for different user groups.



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.

This is Privacy by Design in action!

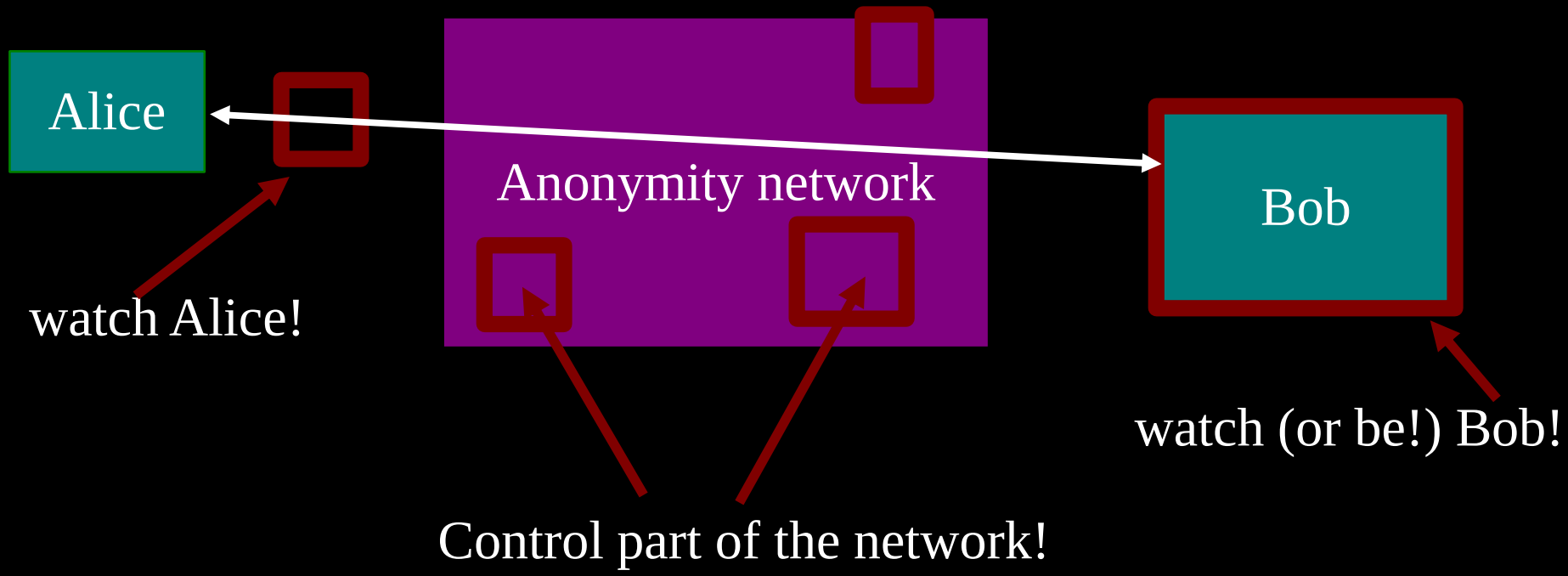
- As a user of Tor:
  - You do not need to trust us; You can verify.
  - You **do not** need a login or password.
  - You **do not** need to pay for this service.
  - You **do not** need to pay for the software.
  - You **help *contribute*** to the network.
    - You help the network by using it.
    - You can share your internet connection.

Who uses Tor?

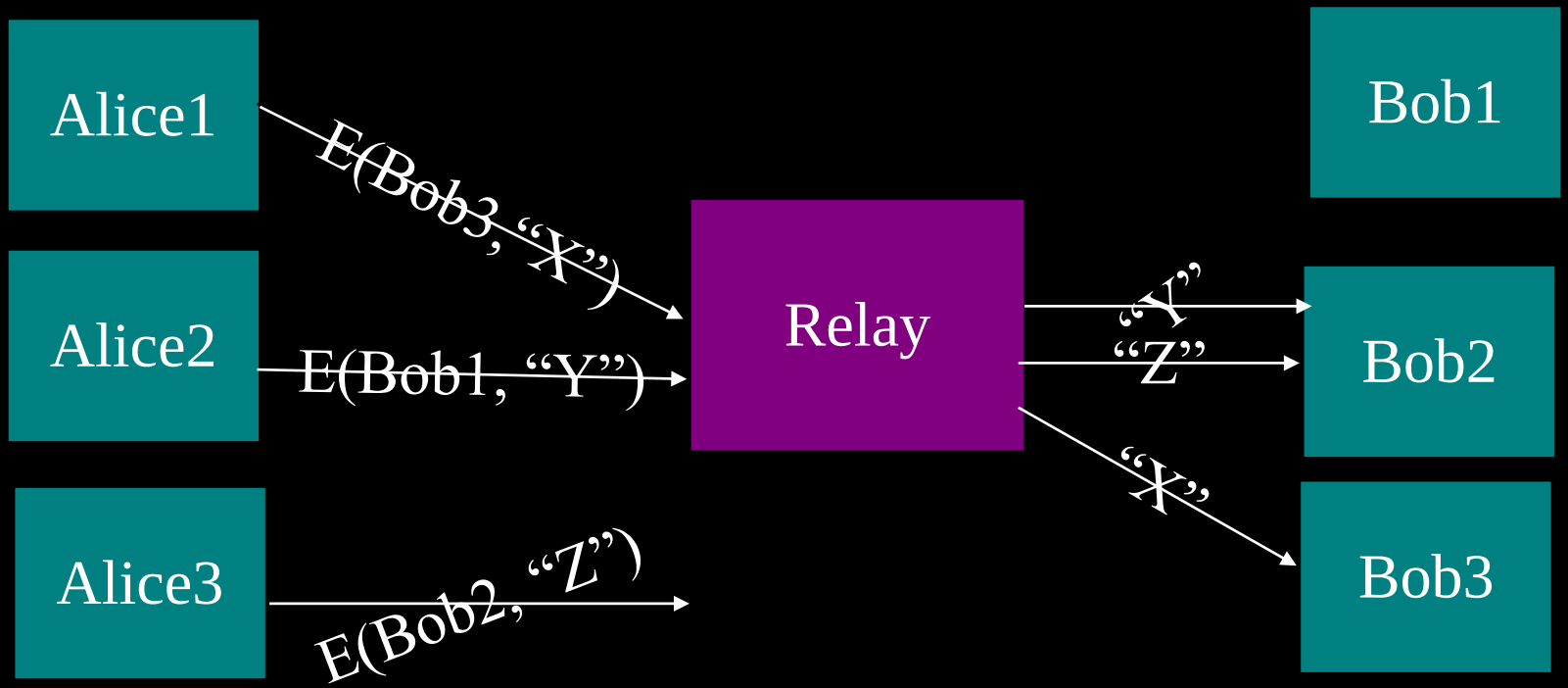
- People from nearly *every country* in the world.
- Normal people use Tor for privacy & security
- Various military forces
- Journalists
- Law enforcement
- Whistleblowers and other activists
- Business executives
- Bloggers
- IT professionals


WikiLeaks

Threat model: what can the attacker do?

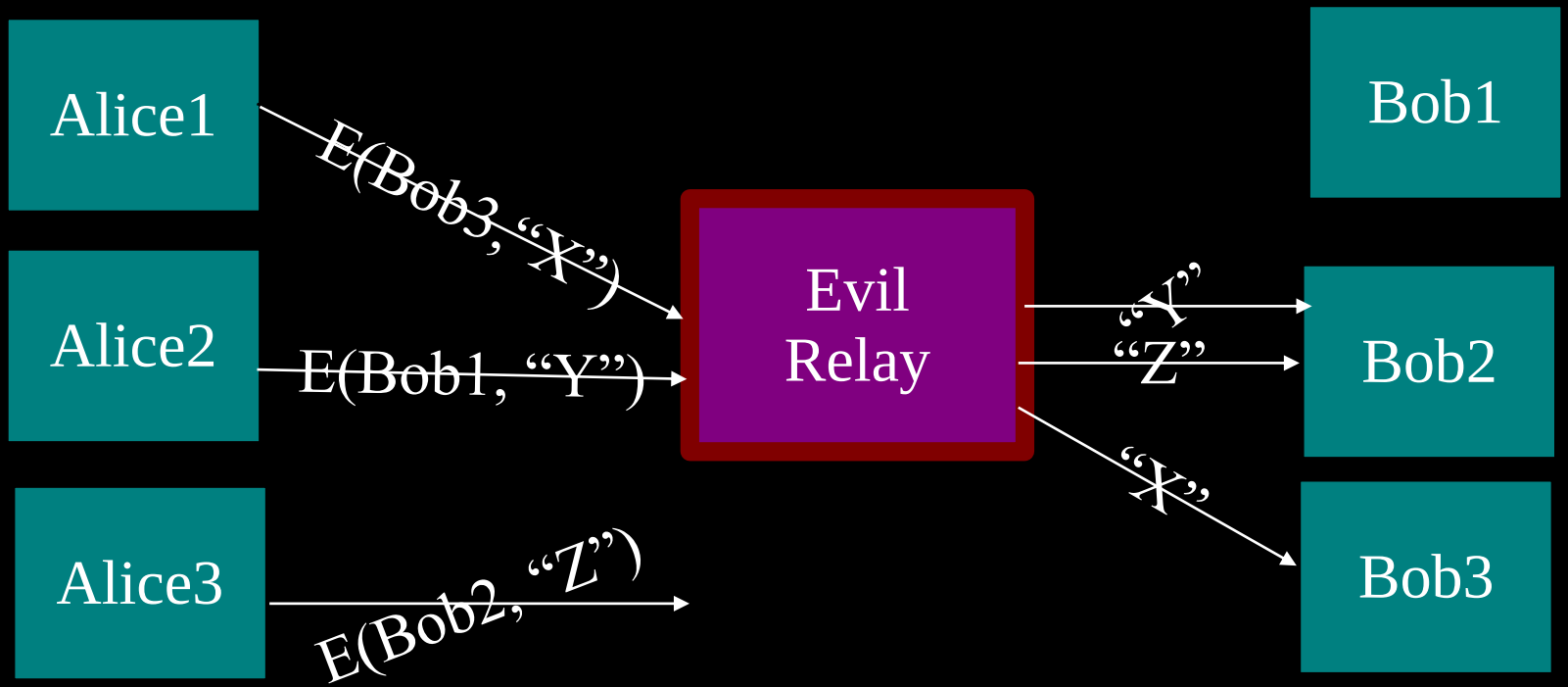


The simplest designs use a single relay to hide connections.

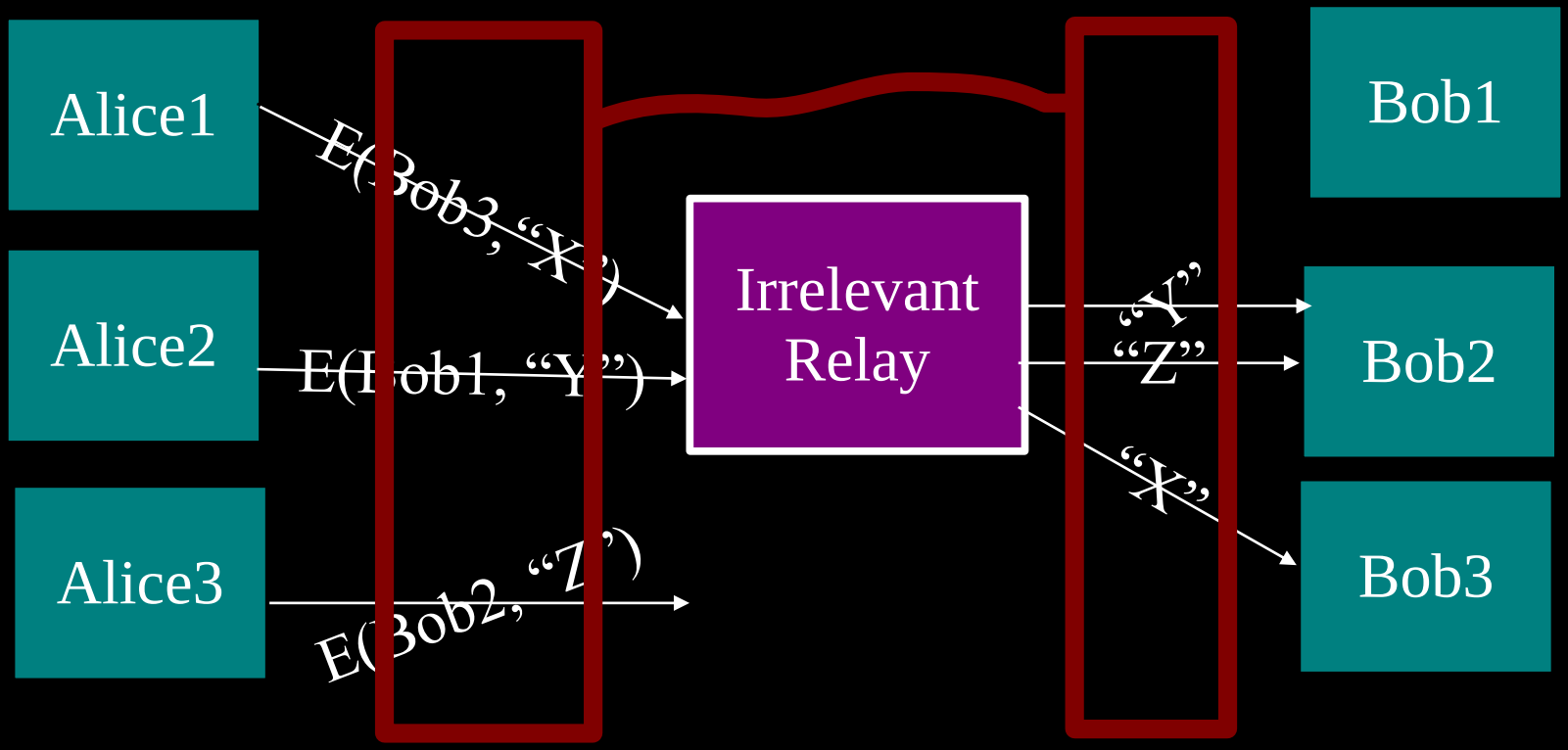


(example: some commercial proxy providers)

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

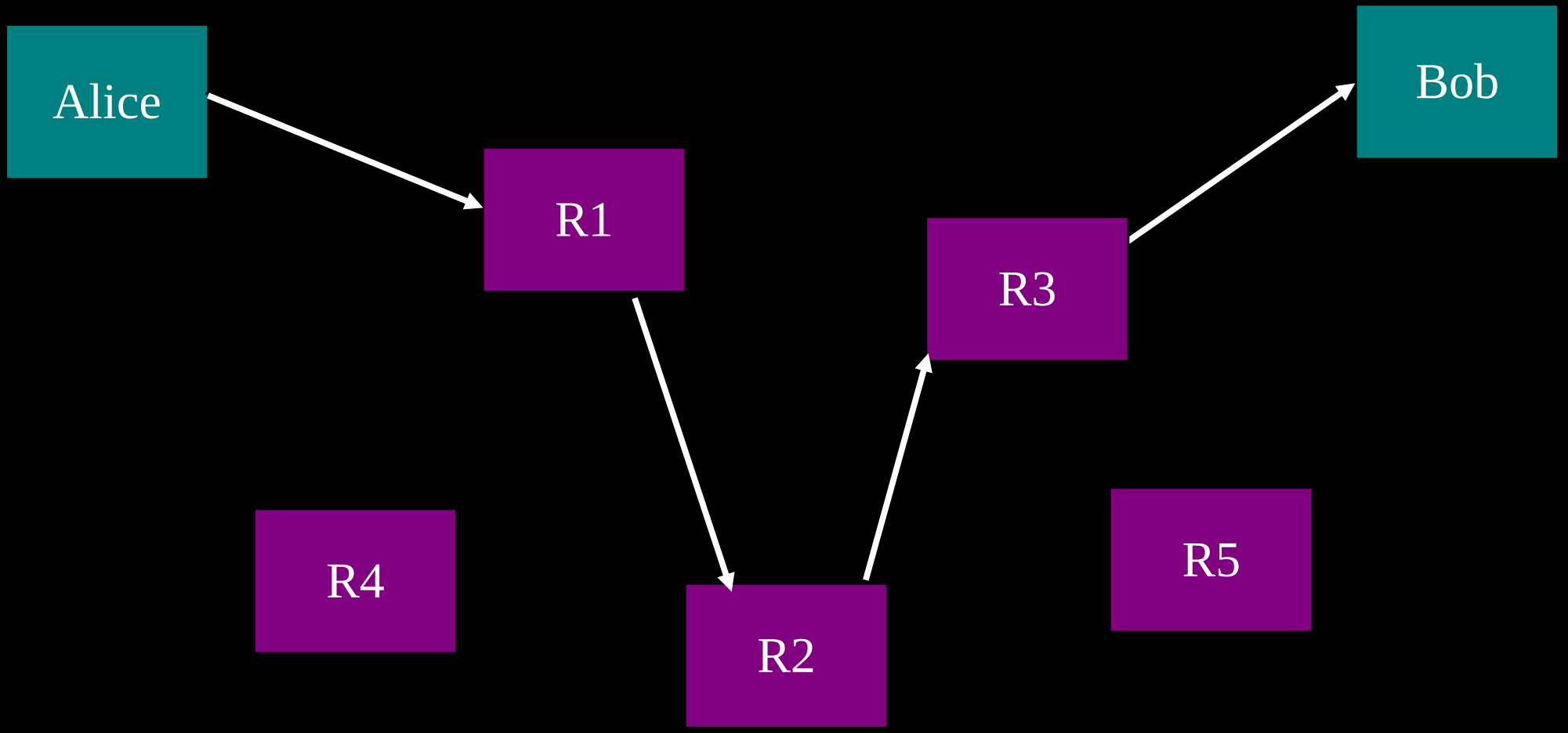


... or a single point of bypass.

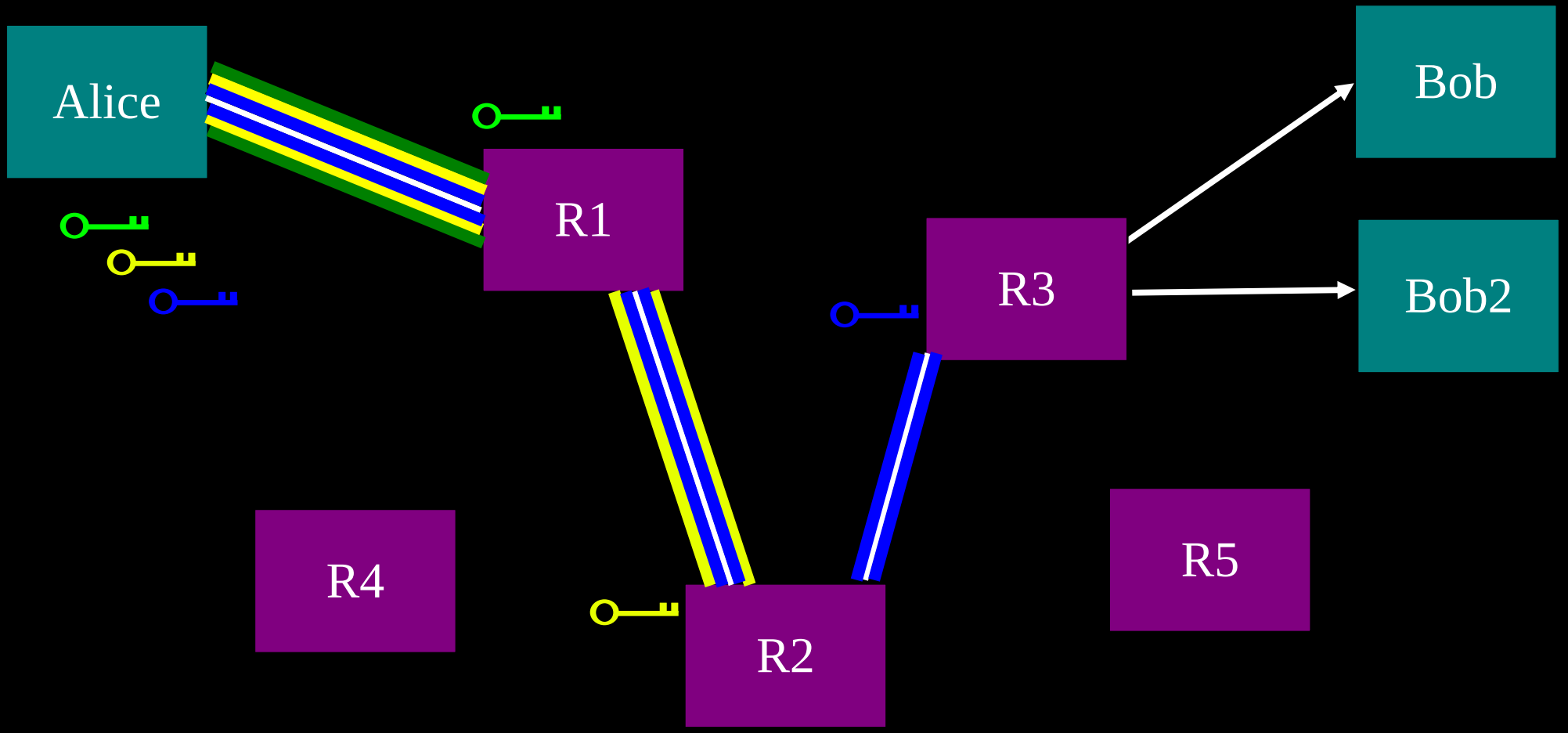


Timing analysis bridges all connections through relay ⇒ An attractive fat target

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



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

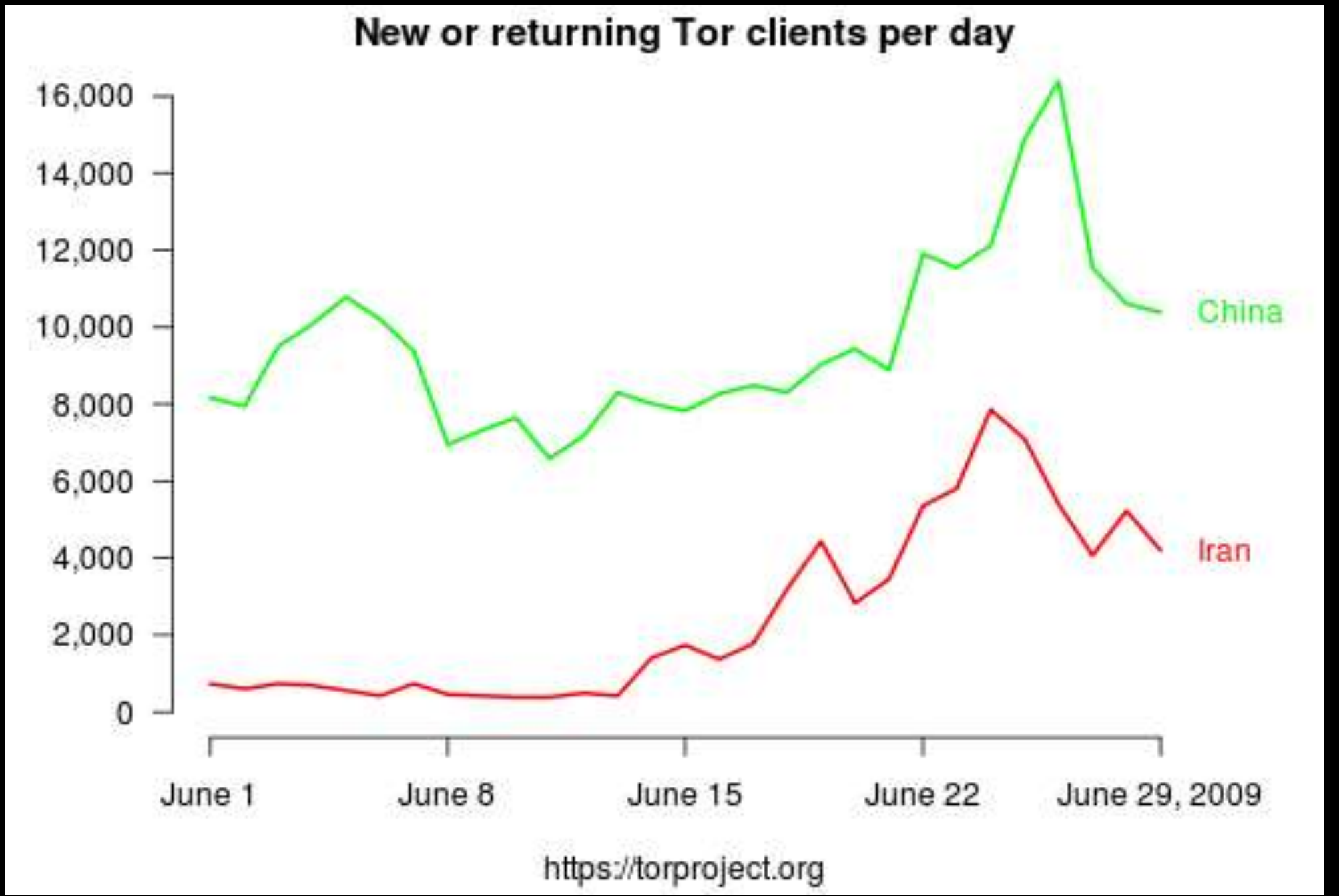


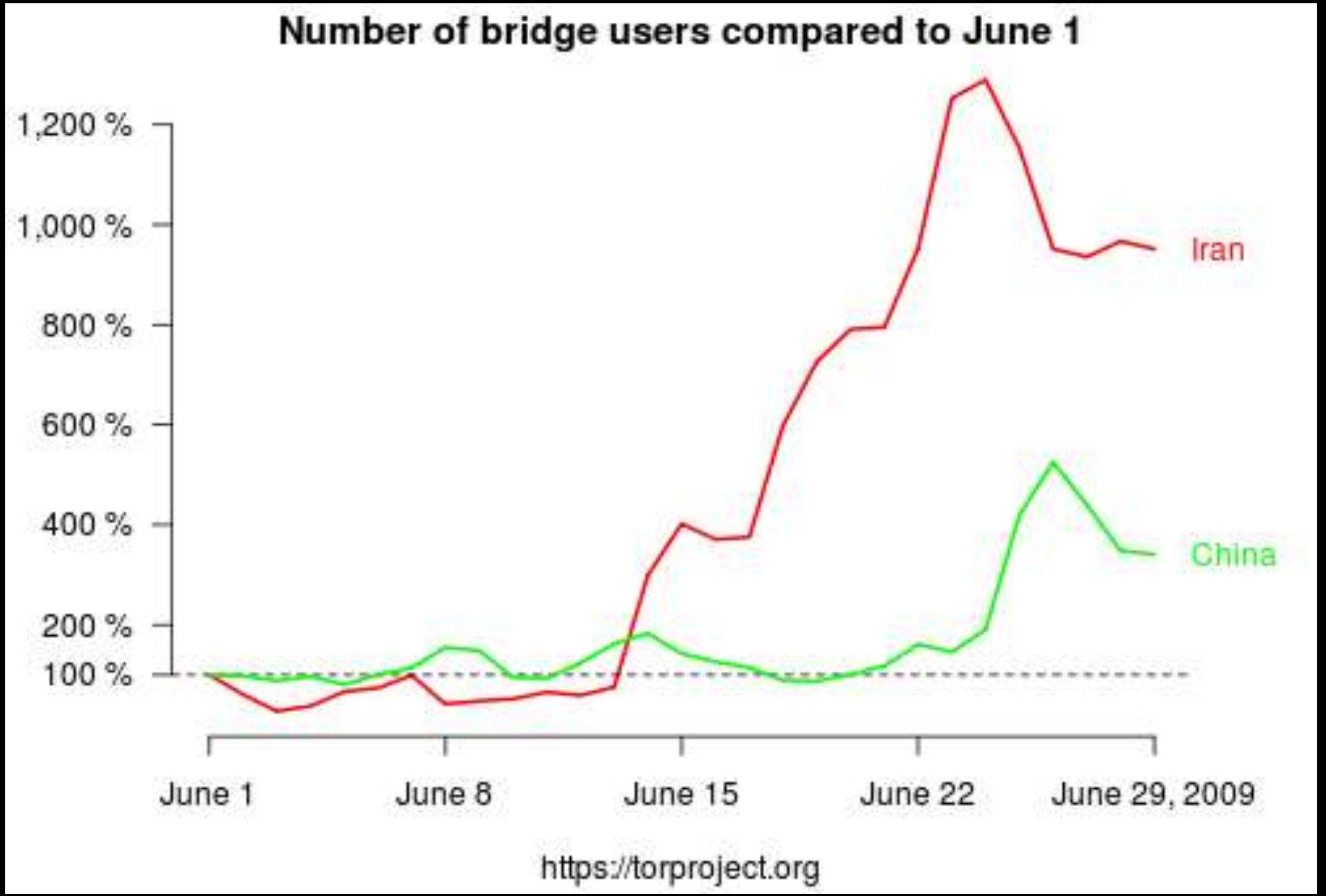
Attackers can block users from connecting to the Tor network

- 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.
- We see this on the internet today.

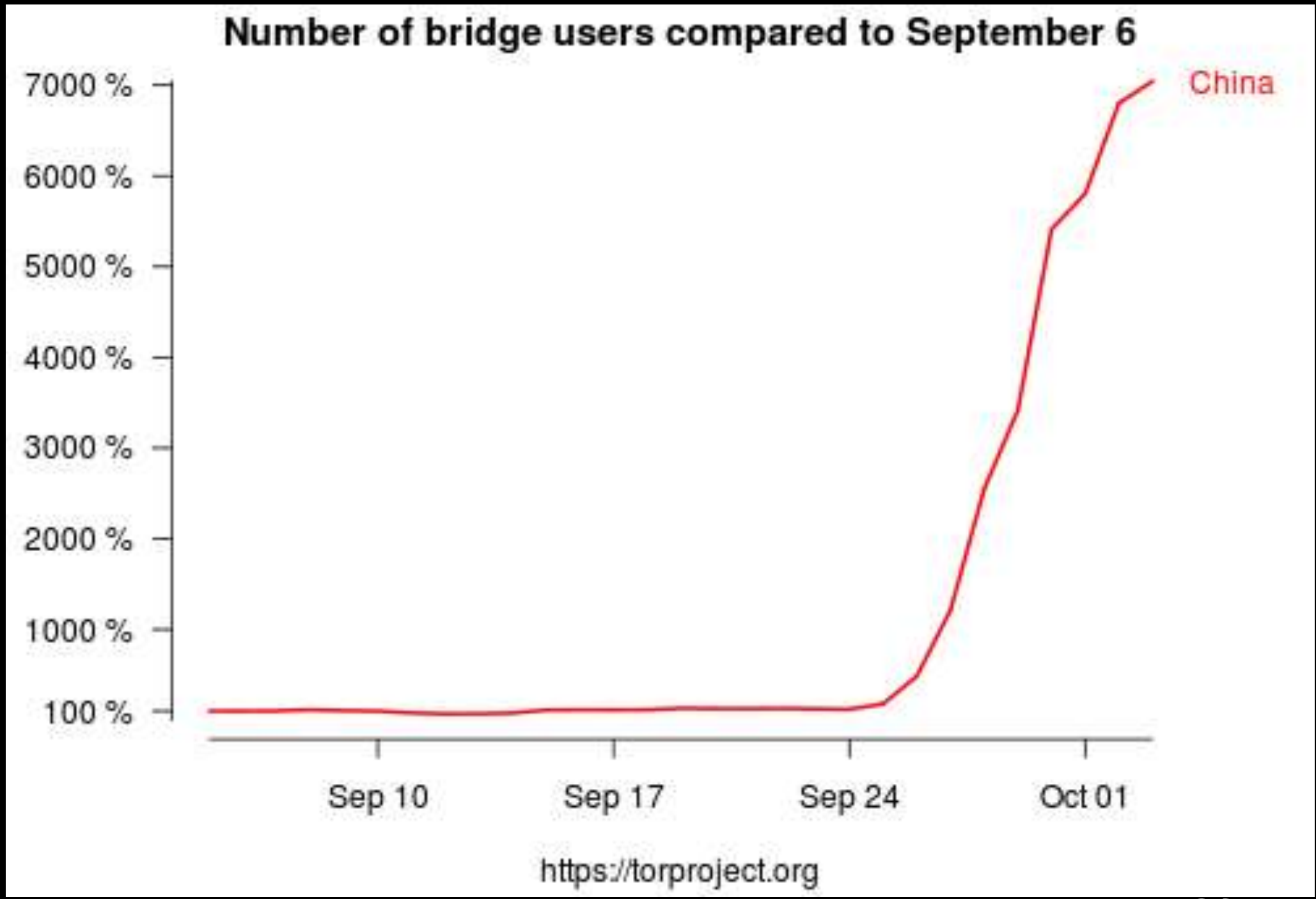
A tale of two countries told in graphs:

Iran & China


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


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


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
7000 %
6000 %
5000 %
4000 %
3000 %
2000 %
1000 %
100 %
China
Sep 10
Sep 17
Sep 24
Oct 01
https://torproject.org

Anonymity is useful for censorship-resistance too!

- If a Chinese worker blogs about a problem at her factory, and she routes through her uncle's computer in Ohio to do it, ...?
- If any relay can expose dissident bloggers or compile profiles of user behavior, attacker should attack relays.
- ...Or just spread suspicion that they have, to chill users.

Publicity attracts attention

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

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 in China bloggers: “Find new bridge” rather than “get software update”.

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?
- (Of course, that doesn't mean they won't try to block it.)

Lots of misinformation going around

- Many people set up open proxies for Iran. But no encryption means “they” get to learn what you're doing: twitter login, etc
- University student arrested “because of Tor”?
- Money brings the snakeoil vendors
- Best practice in Iran: don't stay in one place for very long

Other Iran user count

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

But this isn't just about two countries; This is an issue for Sweden as well.

- We can learn from China and Iran
- We should know that censorship can and *may* happen in every country if we are not vigilant.
- The Western world often thinks of itself as above and beyond this kind of censorship, blocking and control. Are we?
  - Who gains when we begin to monitor, block and control content?