The Tor Project, Inc.

Our mission is to be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.

“Still the King of high secure, low latency Internet Anonymity”

Contenders for the throne:

- None

We're in a ~~war~~ conflict of perception

- For example, GCHQ is trying to kill Tor “because of child porn”
- We ***do*** know that people use Tor to fetch child porn...

We're in a ~~war~~ conflict of perception

- For example, GCHQ is trying to kill Tor "because of child porn"
- We ***do*** know that people use Tor to fetch child porn... the feds have told us they do

Trip report: Tor trainings for the Dutch and Belgian police

Posted February 5th, 2013 by arma in internet censorship, law enforcement, trip report

In January I did Tor talks for the Dutch regional police, the Dutch national police, and the Belgian national police. Jake and I also did a brief inspirational talk at Bits of Freedom, as well as the closing keynote for the Dutch National Cyber Security Centre's yearly conference.

You may recall that one of my side hobbies lately has been teaching law enforcement about Tor — see my previous entries about teaching the FBI about Tor in 2012 and visiting the Stuttgart detectives in 2008 back when we were discussing data retention in Germany. Before this blog started I also did several Tor talks for the US DoJ, and even one for the Norwegian Kripos.

Now is a good time to talk to the Dutch police, first because they're still smarting from the DigiNotar disaster in 2011, but second because of their 2012 ambitions to legalize breaking into foreign computers when they aren't sure what country they're in. (I say legalize because they already did it!)

Below are some discussion points that made an impression on me.

- I started the trip with a talk to about 80 people from the Dutch regional police. Apparently each regional police group has basically one cybercrime person, and pretty much all of them came to learn about Tor. These are the people who advise their police groups about how to handle Tor cases, so they're exactly the ones who need to know about services like ExoneraTor. (Afterwards, one of the national police thanked me heartily for teaching the regional police about Tor, since it makes *his* job easier.)
- One issue that came up repeatedly during the talks: what if a bad guy runs a Tor exit relay to provide plausible deniability when somebody shows up as his door? My first thought is that anybody who runs a Tor exit relay in order to attract *less* attention from

- Add a New
- Manage B
- Admin Co
- Manage U
- Add an Ev
- Manage E
- Manage F

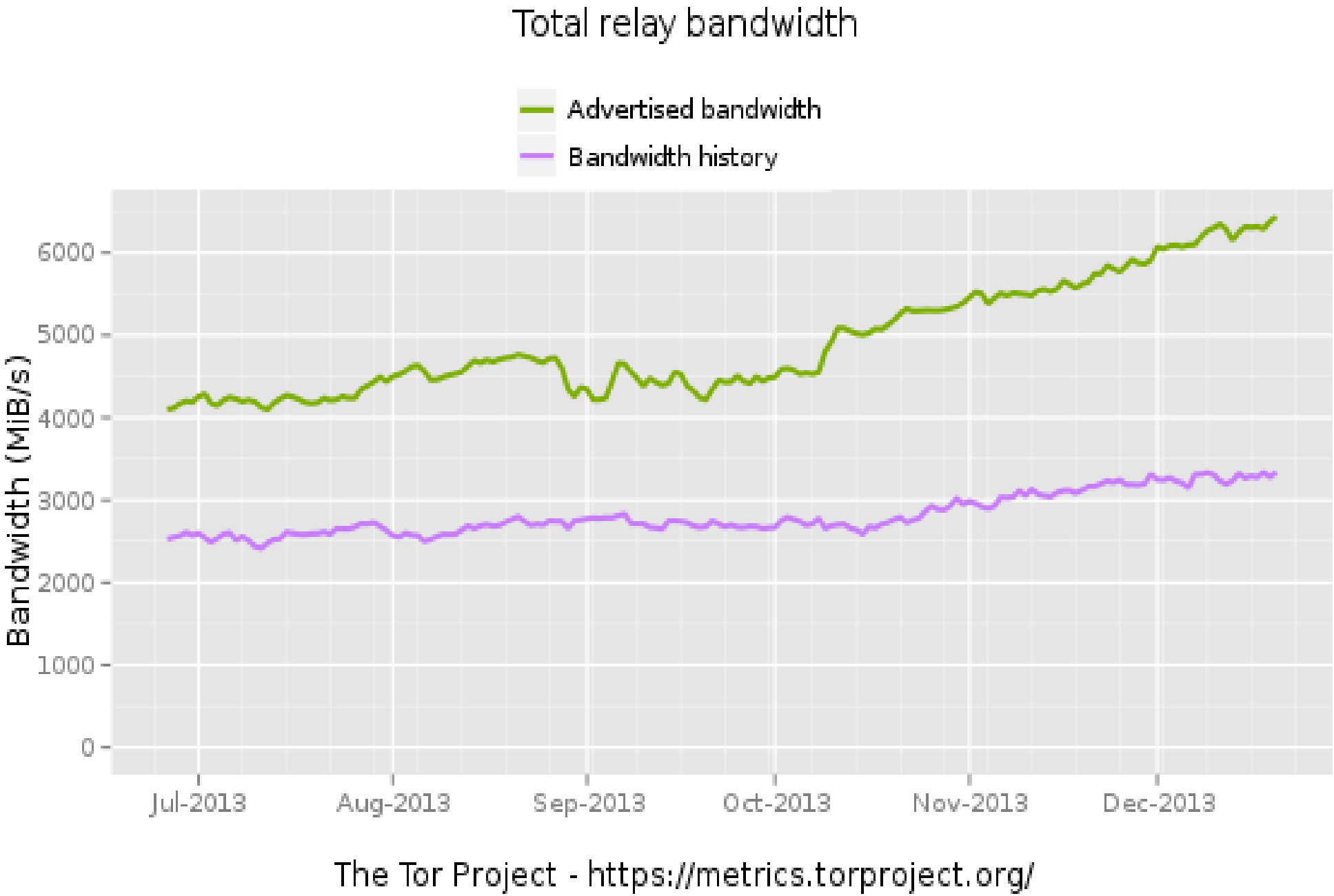
Search

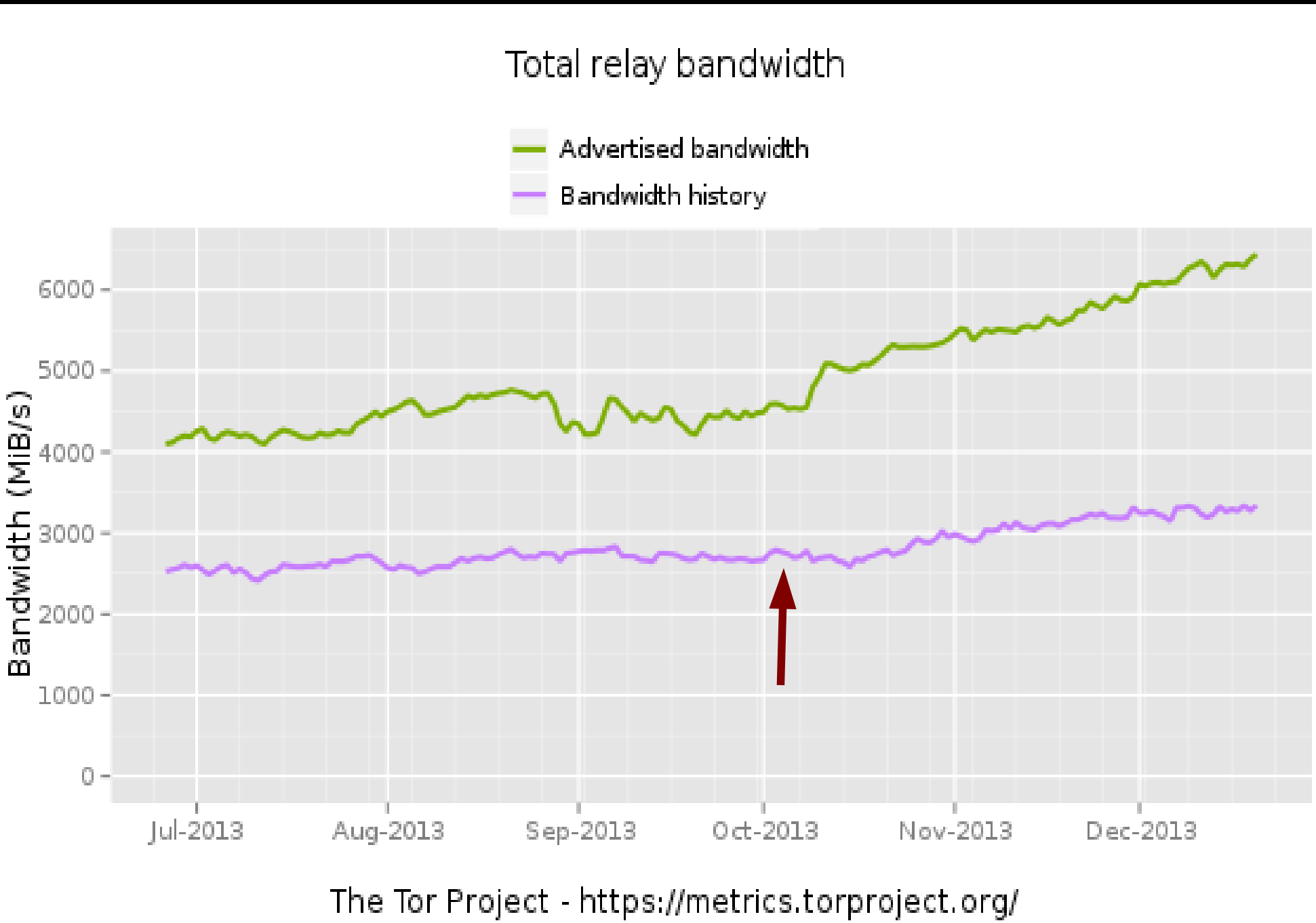
Upcoming

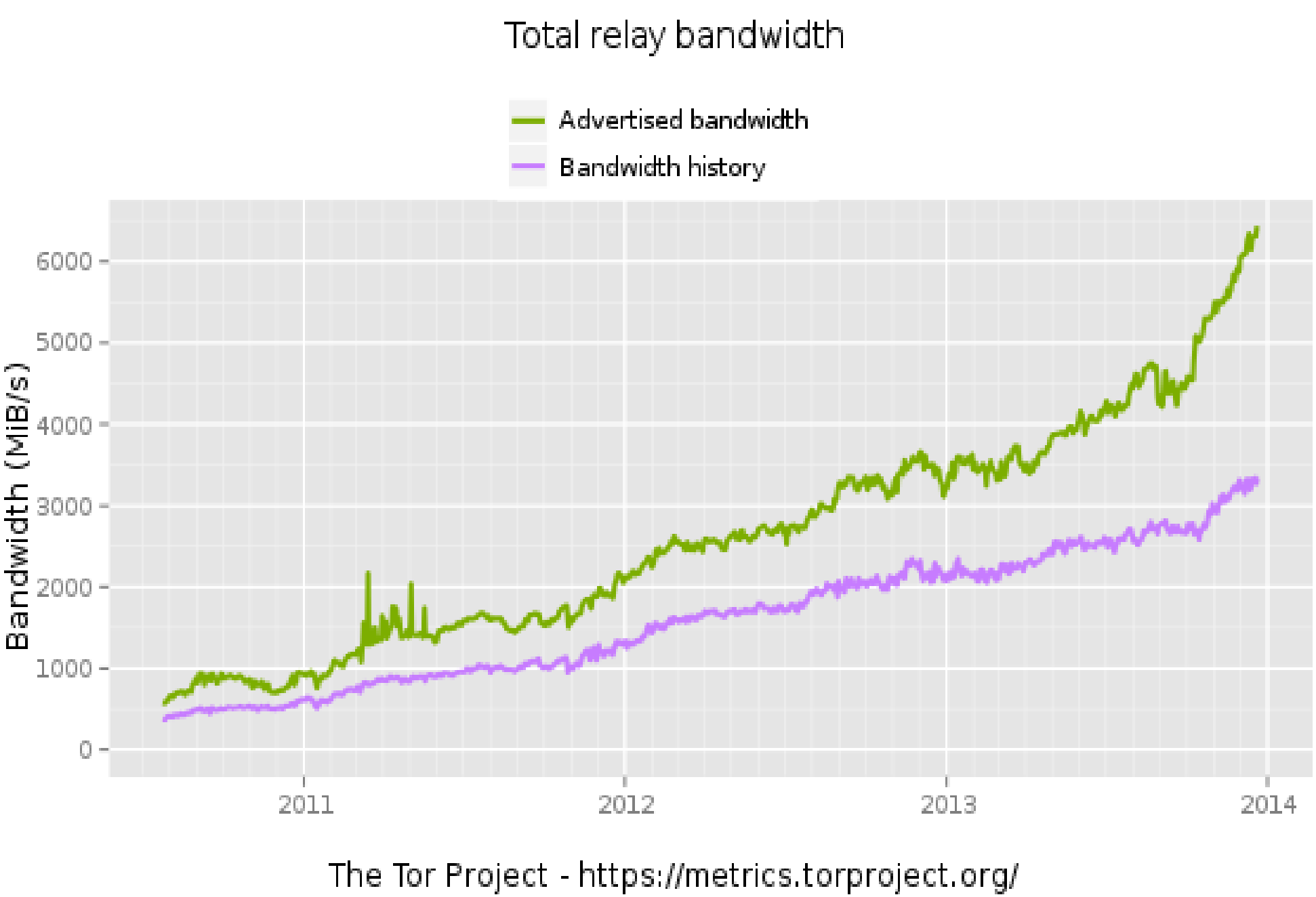
- Lunar @ Conferen
- Roger @ Worksho Enhanci Bloomin
- Tor at Pr Technolo
- Roger @

...Perception

- DoJ's aborted study finding 3% bad content on the Tor network
- How do you compare one Snowden leak to ten true reviews on Yelp?
- BBC's Silk Road articles telling people how to buy drugs safely
- Agent who “showed” massive drop in Tor network load after Silk Road bust


Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
6000
5000
4000
3000
2000
1000
0
Jul-2013
Aug-2013
Sep-2013
Oct-2013
Nov-2013
Dec-2013
The Tor Project - https://metrics.torproject.org/


Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
6000
5000
4000
3000
2000
1000
0
Jul-2013
Aug-2013
Sep-2013
Oct-2013
Nov-2013
Dec-2013
The Tor Project - https://metrics.torproject.org/


Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
6000
5000
4000
3000
2000
1000
0
2011
2012
2013
2014
The Tor Project - https://metrics.torproject.org/

“The Dark Web”
“The Deep Web”
“The <insert pejorative term> Web”

High-profile hidden services

The media has promoted a few hot topics:

- WikiLeaks (~2010)
- Farmer's market (pre-2013)
- Freedom Hosting (2013)
- Silk Road (2013)

There are many more (eg: many GlobaLeaks deployments, etc) which aren't well known by the media (yet).

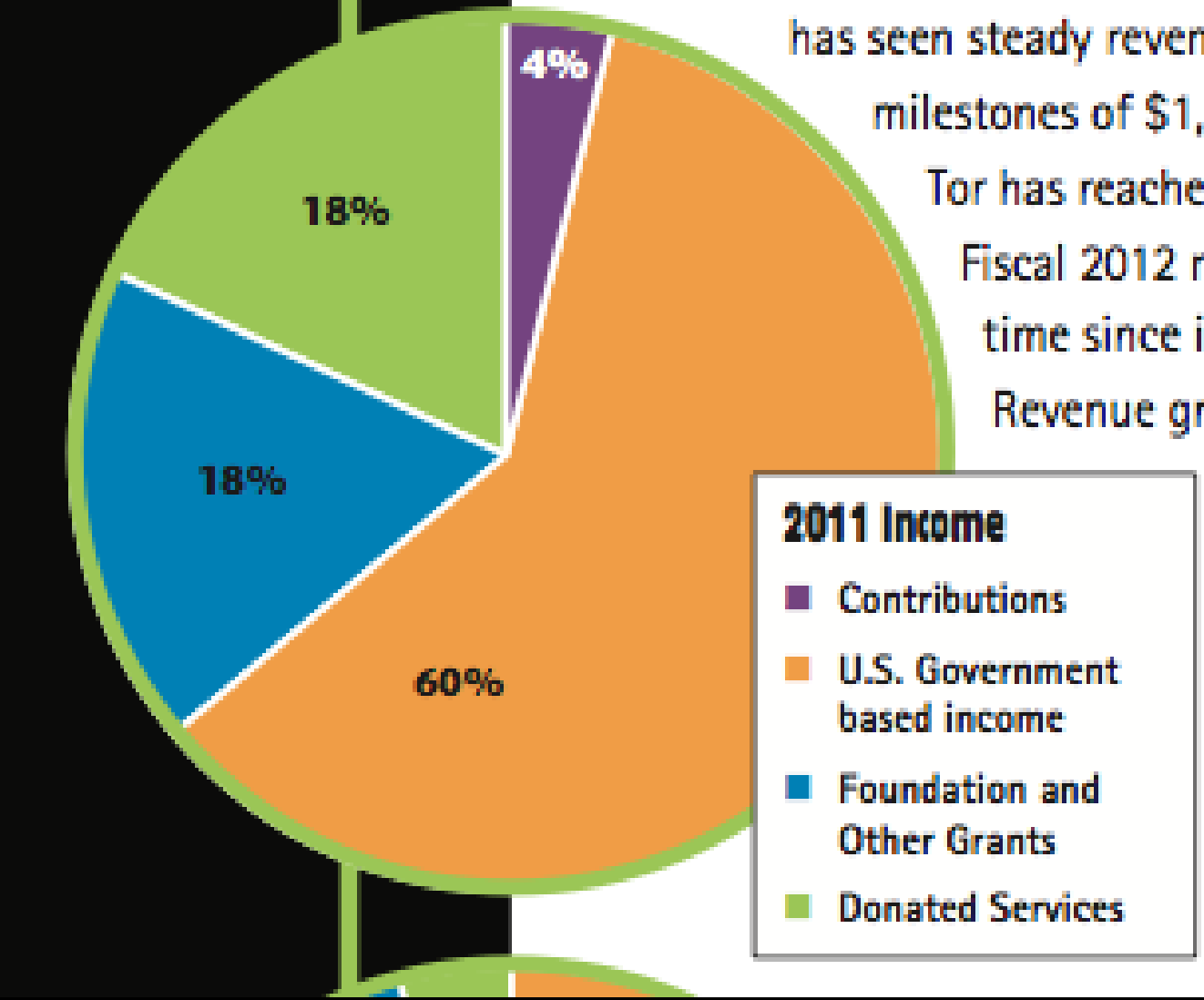
Exploiting old Tor Browser users

- By FBI, NSA, SAIC, VUPEN…?
- Better browser sandboxing is needed!
- The Firefox people are pissed that they're the weak link in all these stories
  - Perhaps they will integrate our patches and adopt some of our serious privacy fixes?
- Chrome has outstanding privacy issues which need to be fixed before we could make it into a TBB.

Financial Review

Tor's fiscal 2012 marked another year of financial improvemer
has seen steady revenue growth since its inception. Si
milestones of $1,253,241 in 2009, $1,574,119 in
Tor has reached new heights in 2012 with ove
Fiscal 2012 results also provided a new finan
time since inception: The Tor Project Inc. ha
Revenue growth was driven by diversity in
U.S. government federal fundi
International, Google, the Swe
Cooperative Agency, and priva

Fiscal responsibility is importa
to maintain financial stability,
sufficient to maintain operatio
Tor is proud to report that, sin



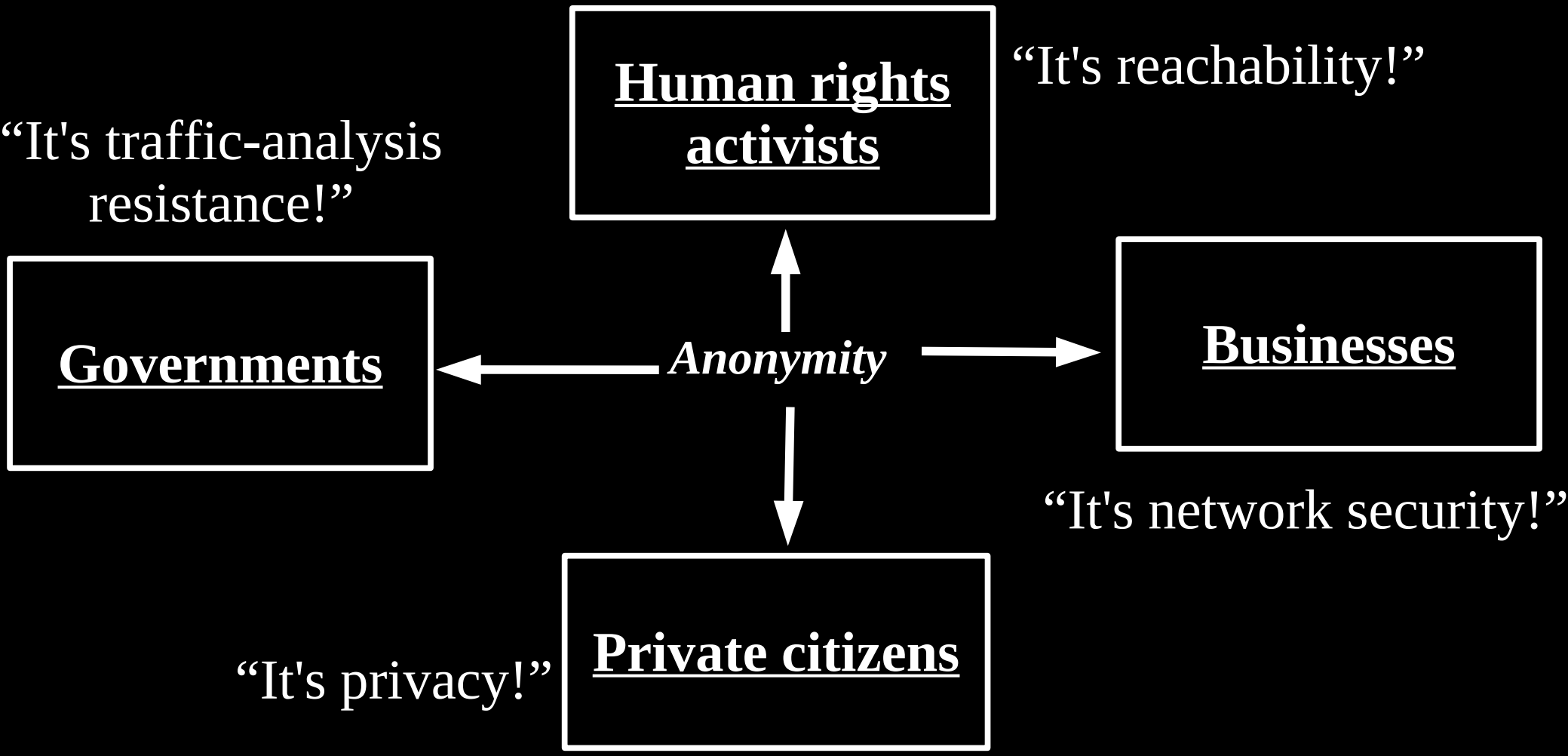
Funding

- Government funding is good because we can do more things
- But it's bad because it influences our priorities
- There is no conspiracy: we don't do things we don't want to do. **No backdoors, ever.**
- Sadly some priorities (like better anonymity) never end up being what funders want most

So what should Tor's role be?

- Can't be solely technical (anymore, if it ever could have been)
- But technical is what we're best at (at least, historically)
- Remember how important diversity of users is

Anonymity serves different interests for different user groups.

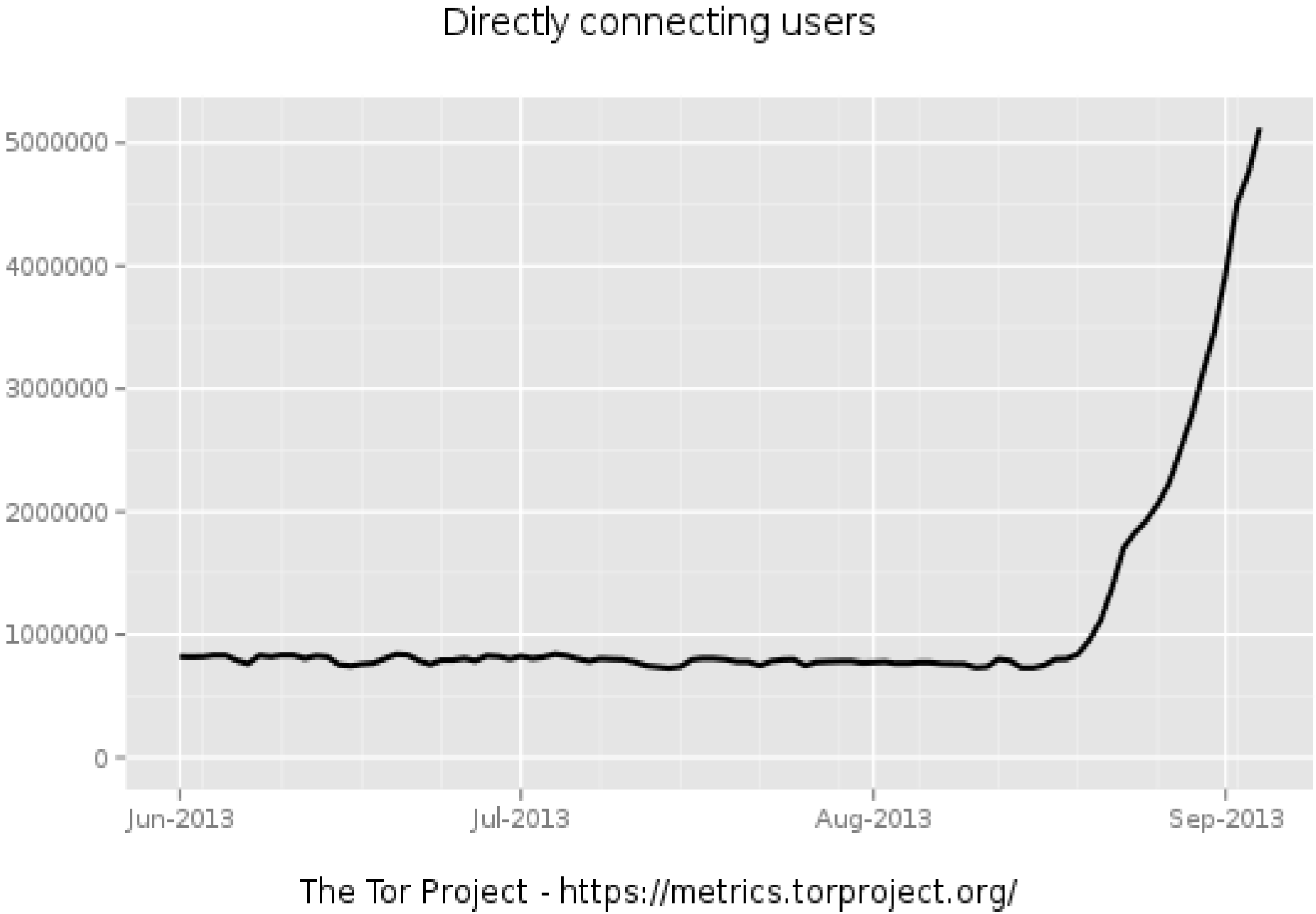


Three ways to destroy your privacy and anonymity (eg: Tor)

- 1) Legal / policy attacks
- 2) Make ISPs hate hosting exit relays
- 3) Make services hate Tor connections
  - Yelp, Wikipedia, Google, Skype, …

Five ways to destroy your privacy and anonymity (eg: Tor)

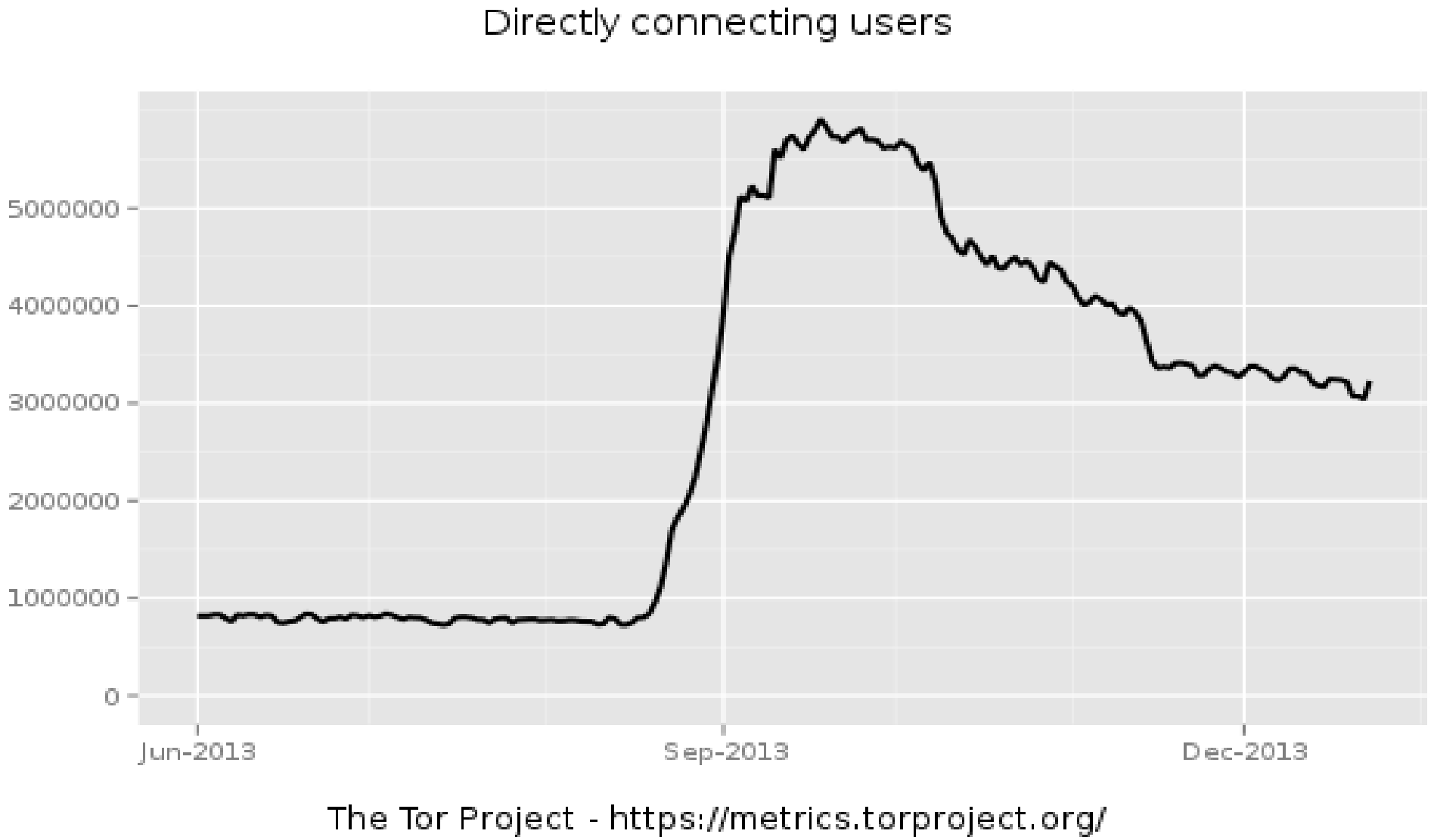
- 1) Legal / policy attacks
- 2) Make ISPs hate hosting exit relays
- 3) Make services hate Tor connections
  - Yelp, Wikipedia, Google, Skype, …
- 4) Hype that it is broken when it isn't
- 5) ...Build a botnet to melt the network


Directly connecting users
5000000
4000000
3000000
2000000
1000000
0
Jun-2013
Jul-2013
Aug-2013
Sep-2013
The Tor Project - https://metrics.torproject.org/

Botnet

- Some jerk in the Ukraine signed up 5 million bots as Tor clients (not relays)
- Our scalability work paid off!
- Good thing it wasn't malicious.
- Ultimately it didn't work: everybody noticed, and Microsoft has been cleaning up the bots
  - Which says something for Windows users!

Number of daily Tor users



Stinks (U)

[redacted]

CT SIGDEV

[redacted]

JUN 2012

Derived From: [redacted]
Dated: [redacted]
[redacted] On: [redacted]

NSA/GCHQ programs that affect Tor

- Quick Ant (QFD), Quantum Insert, Foxacid
- Quantum for cookie tests (good thing we moved away from Torbutton's “toggle”)
- Remember, they can do these things even more easily to non-Tor users
- At least they can't target specific Tor users (until they identify themselves)
- “Don't worry, we never attack Americans” (!)

omg nsa runs relays

- Actually it appears they mostly don't
  - And the few they did were on EC2!

omg nsa runs relays

- Actually it appears they mostly don't
  - And the few they did were on EC2!
- But don't be happy: it's just as bad if the relay's upstream logs
  - And that happens for honest relays?
- And this is even worse for a single hop VPN or barebacking with the internet.


Blog
Community
Twitter
Affiliate
Jobs
Contact
HIDE MY ASS!
Pro VPN
Web Proxy
IP:Port Proxies
Anonymous Email
Privacy Software
File Upload
Anonymous Referrer
Protect Your Online Privacy Now:
Web Proxy
free!
Use our free proxy to surf anonymously online, hide your IP address, secure your internet connection, hide your internet history, and protect your online identity. Learn more »
http://google.com
Hide My Ass!
SSL security
OFF
Advanced options
Pro VPN
up to 43% OFF
Go PRO! for more beneficial features, including ...
52'000+ IP's in 59 countries
Improved security and encryption
Anonymously encrypt all traffic
Works with all applications
Easy to use software
Learn More and See Pricing

Parallel construction

- Scenario 1, NSA tips off FBI who finds that the Silk Road guy has crappy opsec
- Scenario 2, Silk Road guy has crappy opsec
- We know that both are true in various cases.

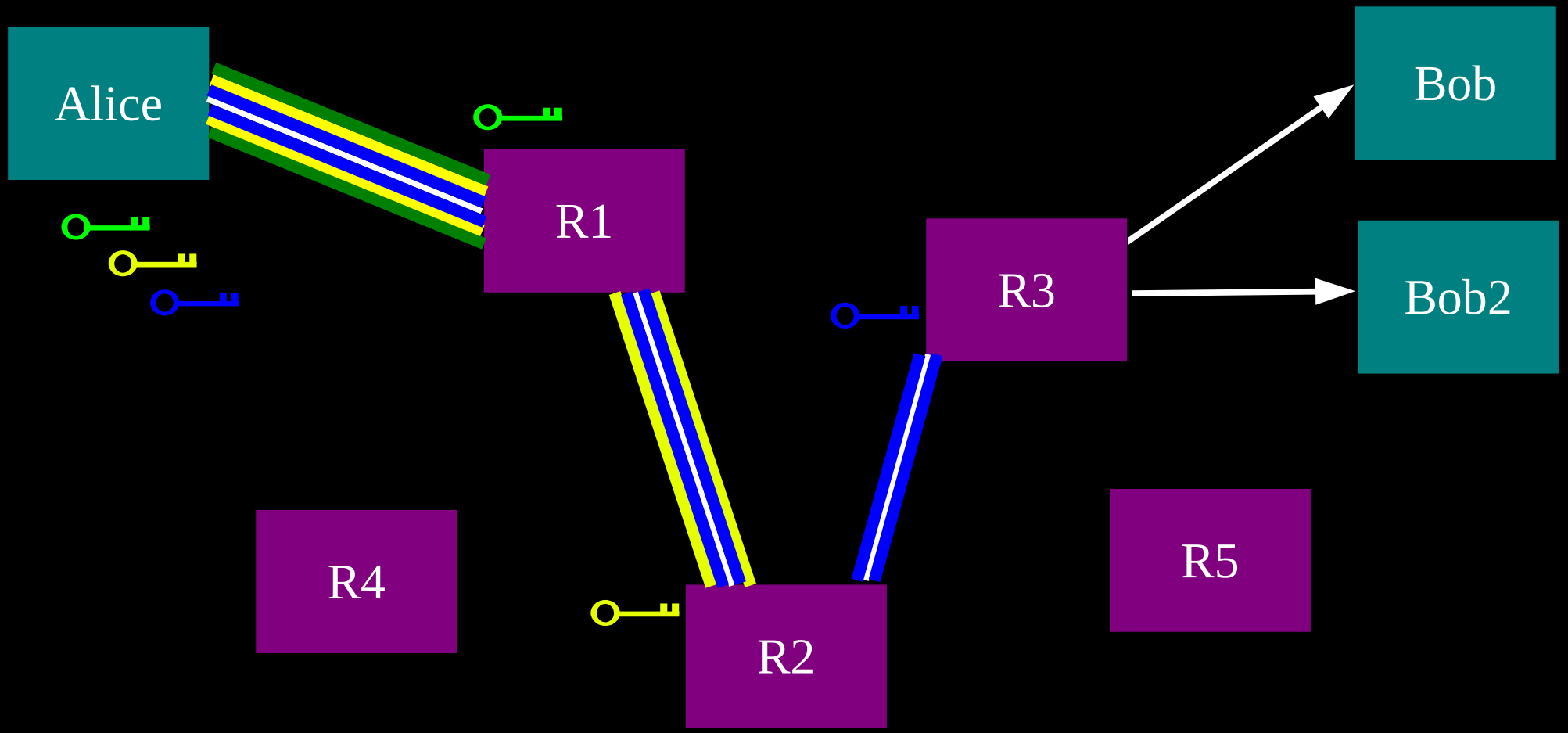
Hidden services need some changes

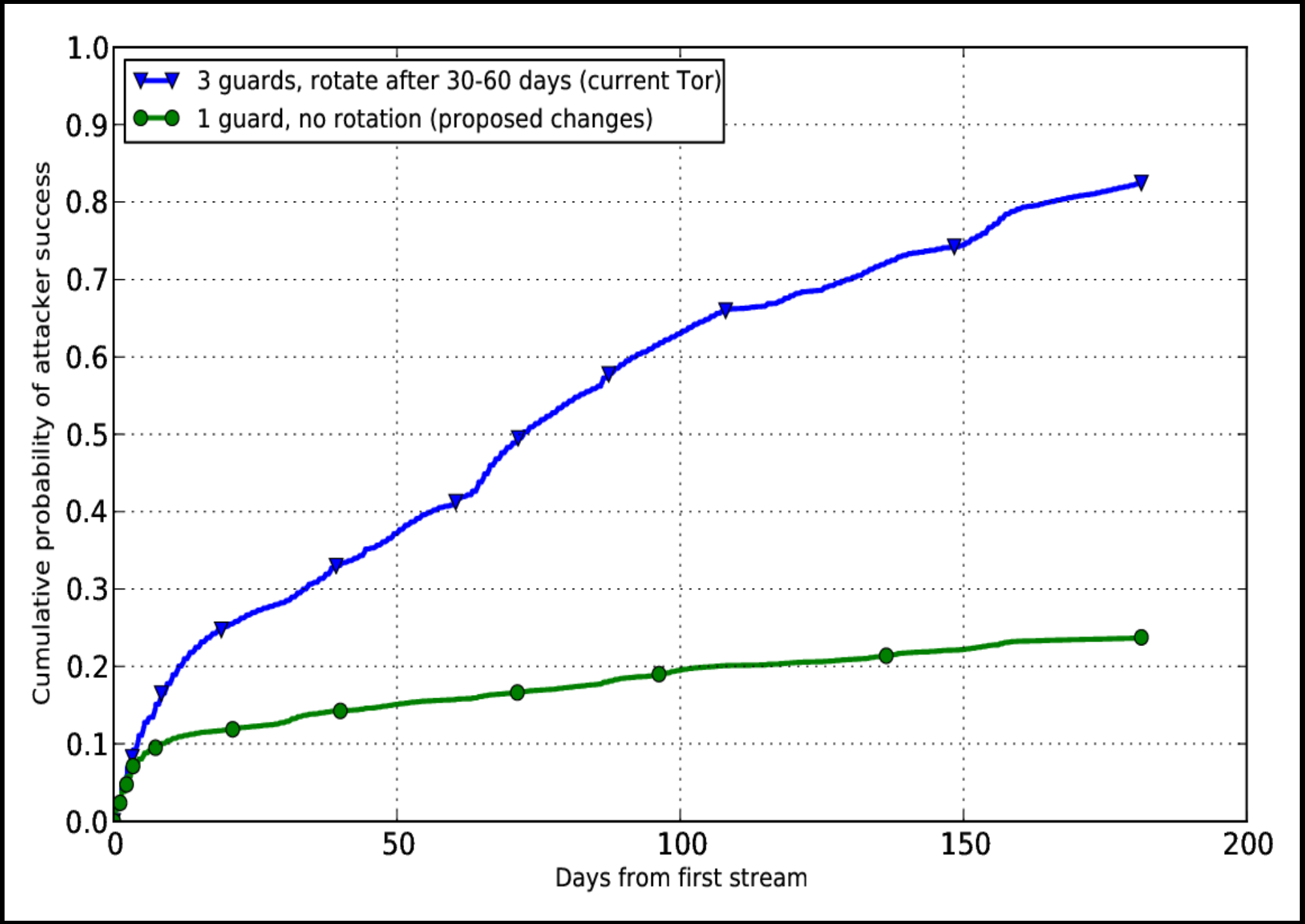
- Make it hard for HSDir to enumerate .onion addresses
- Make it hard for attacker to predict HSDir locations into the future
- And stronger keys / handshake
- But most important: better performance, better usability will lead to “better” uses

“Users Get Routed” (CCS 2013)

- Tor clients choose three “entry guards”, but rotate to new ones after 2ish months
- Need to use better rotation parameters: fewer guards, rotate less often
- Threat also comes from a network adversary observing honest relays
- Hidden services are especially vulnerable

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




3 guards, rotate after 30-60 days (current Tor)
1 guard, no rotation (proposed changes)
Cumulative probability of attacker success
Days from first stream
0.0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1.0
0
50
100
150
200

So what's next?

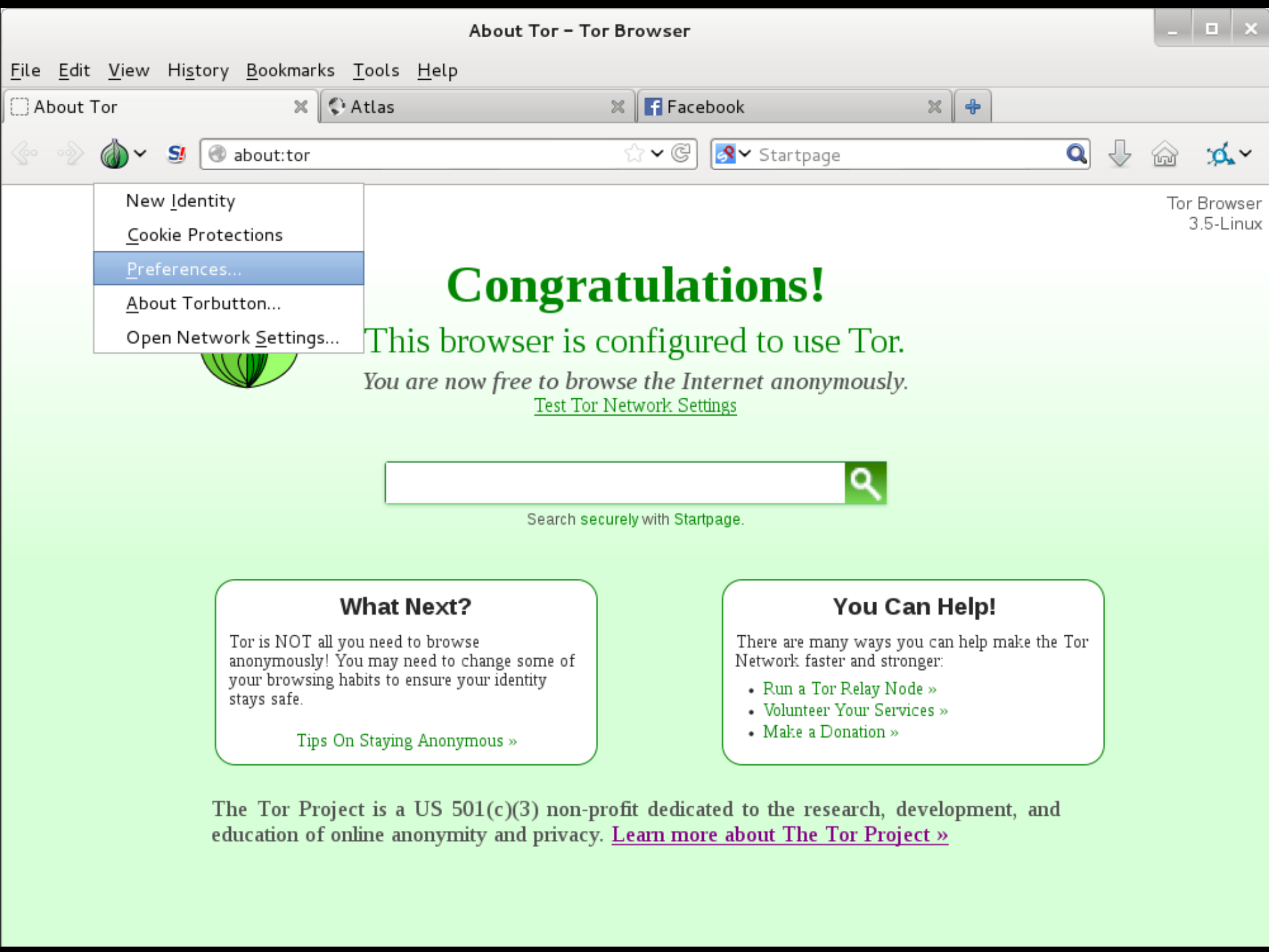
- “Tor: endorsed by Egyptian activists, Wikileaks, NSA, GCHQ, Chelsea Manning, Snowden, ...”
- Different communities like Tor for different reasons.

So what's next?

- Tails (“adds severe CNE misery”)
- WiNoN, Whonix
- Torbirdy
- Usable, secure systems are the worst enemy of those wishing to target our users
- Migrating from 1024-bit RSA to ECC and Curve25519 with Ntor
- TLS improvements

Tor Browser Bundle 3.x

- Deterministic Builds
- “Tor launcher” extension, no Vidalia
- Asks if you want bridges first
- Local homepage, so much faster startup
- Security slider (for e.g. JavaScript)
- Privacy fixes, e.g. font enumeration


About Tor – Tor Browser
File Edit View History Bookmarks Tools Help
About Tor
Atlas
Facebook
about:tor
Startpage
New Identity
Cookie Protections
Preferences...
About Torbutton...
Open Network Settings...
Tor Browser
3.5-Linux
Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Startpage.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

“Core” Tor tasks

- Core Tor (specs, design, hidden services)
- Tor Browser Bundle, deterministic builds
- Metrics and measurements
- Bridges and pluggable transports
- Research
- Outreach and education

Finally, we accept Bitcoin too

- Please help us get more independent from our government funding!
- (Alas, we do it via Bitpay so we don't get screwed in our yearly audit.)
- https://www.torproject.org/donate

Workshop at the Noisy Square:
“How to Help Tor”
21:30 – 23:00+ (right now)