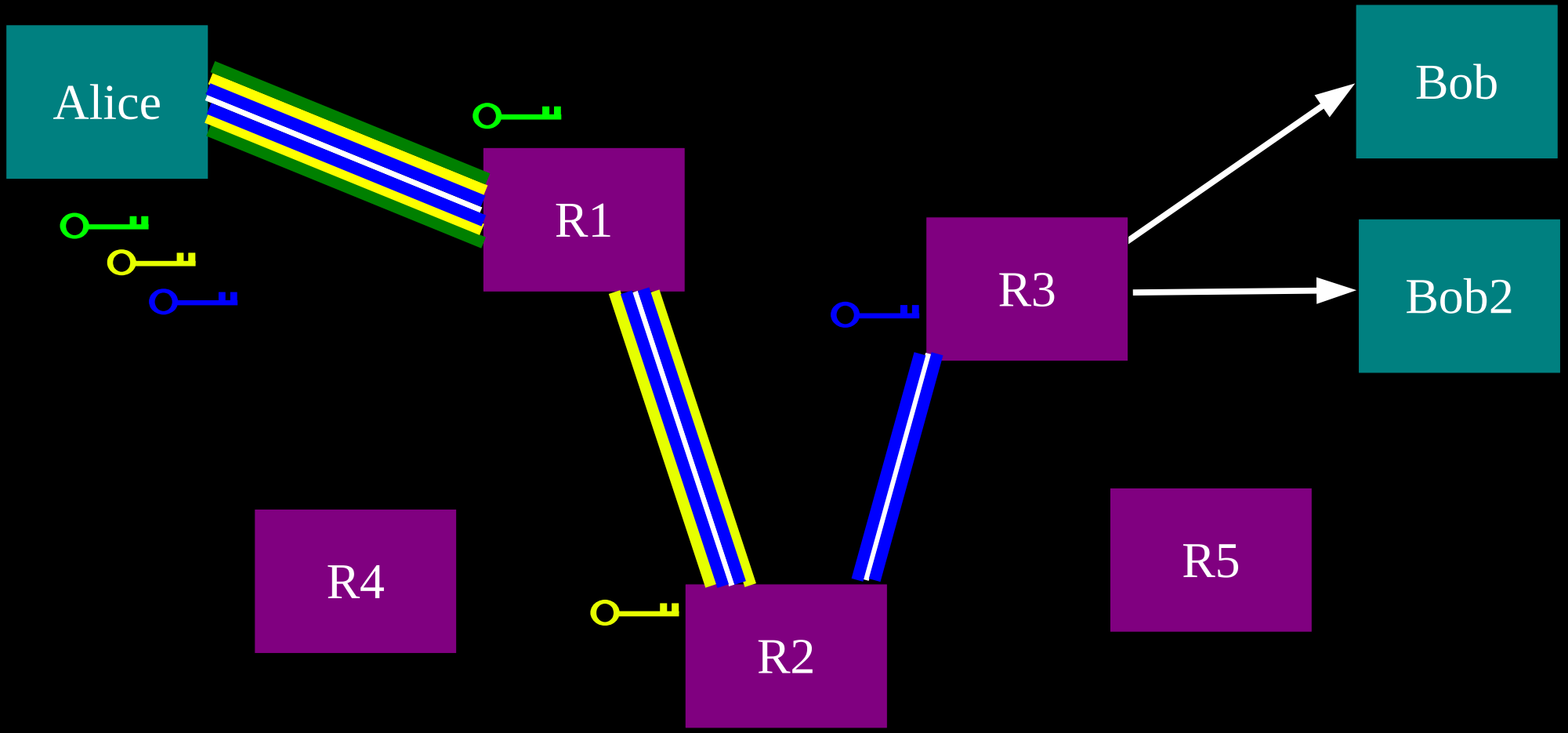
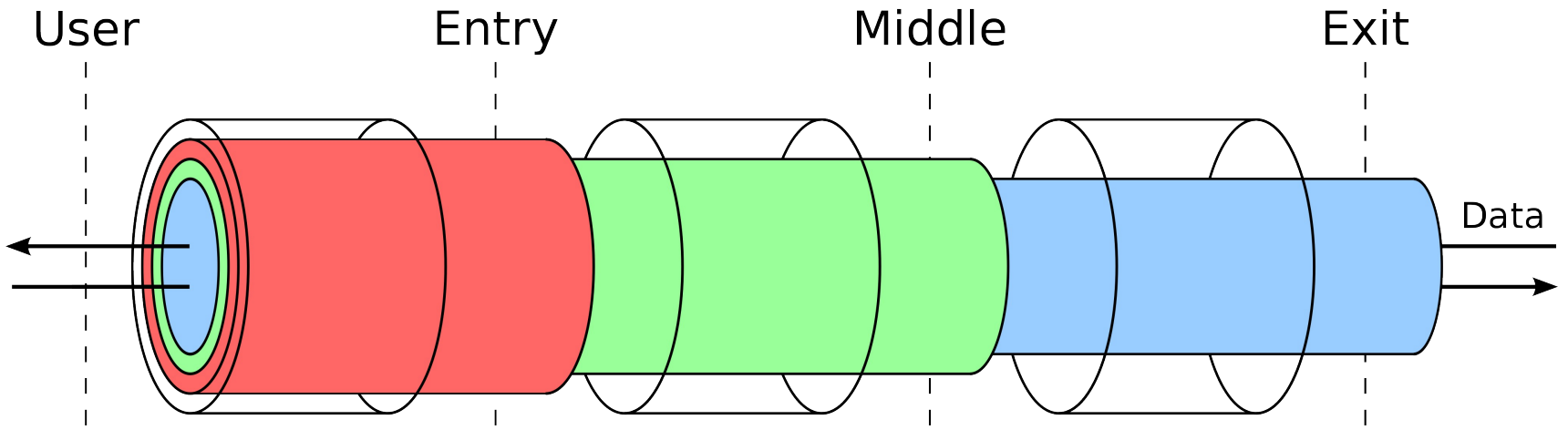
The Tor Project, Inc.

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.

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




User
Entry
Middle
Exit
Data

Other components Tor

- Directory authorities
- Exits (and exit policies)
- Entry guards
  - Predecessor attack, DoS-as-DoA attack
  - raise startup cost to evil relay operator
- Bridges (and pluggable transports)
- Hidden services

Other pieces of Tor

- Load balancing
  - Weight relay section by bandwidth
  - Avoid guards for other than first hop, avoid exits for other than last hop
  - “bandwidth authority” active testing
- Client-side “circuit build timeout” to avoid worst 20% of circuits
- Various scheduling / priority decisions

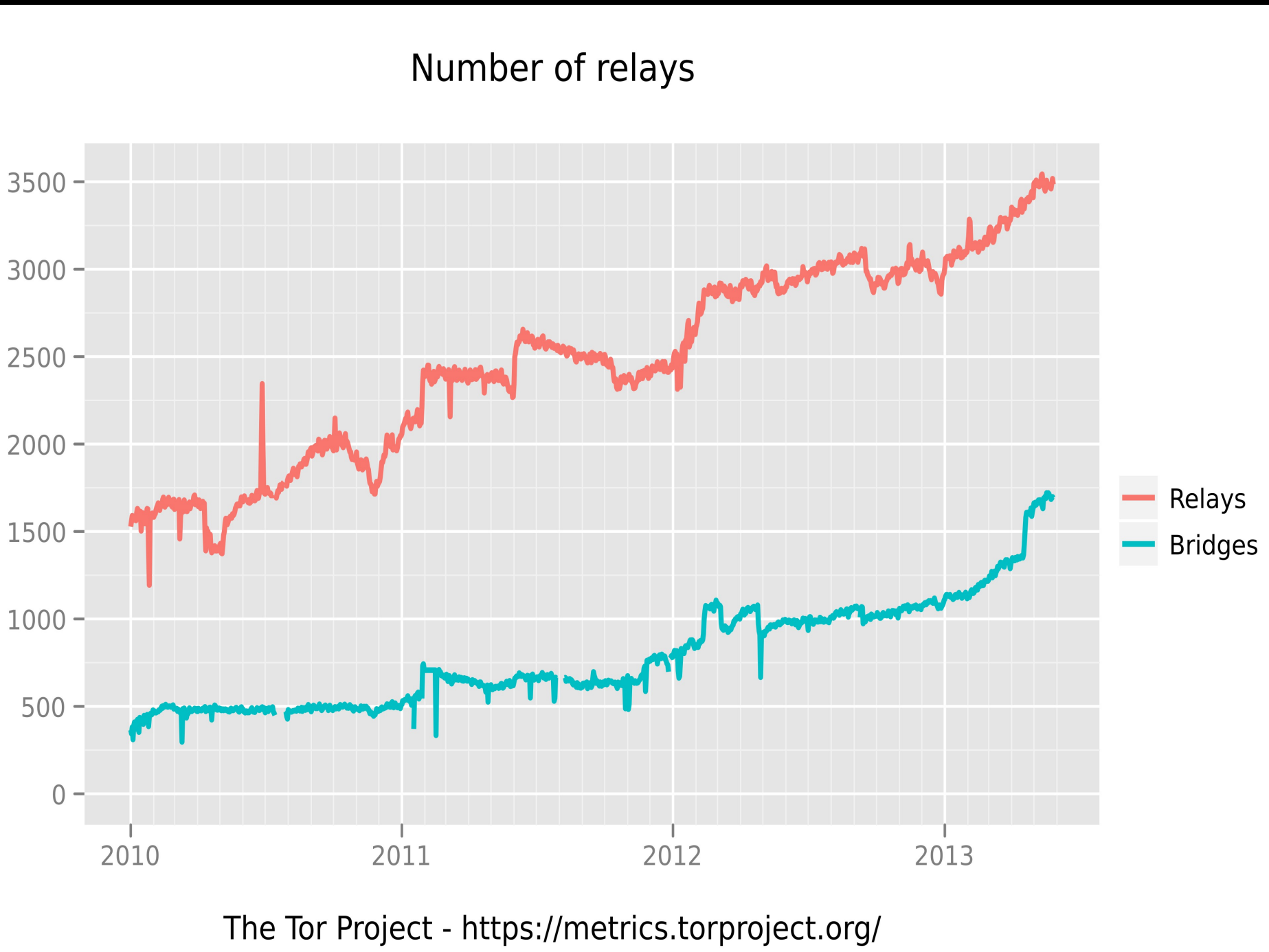
Anybody can sign up to be a relay

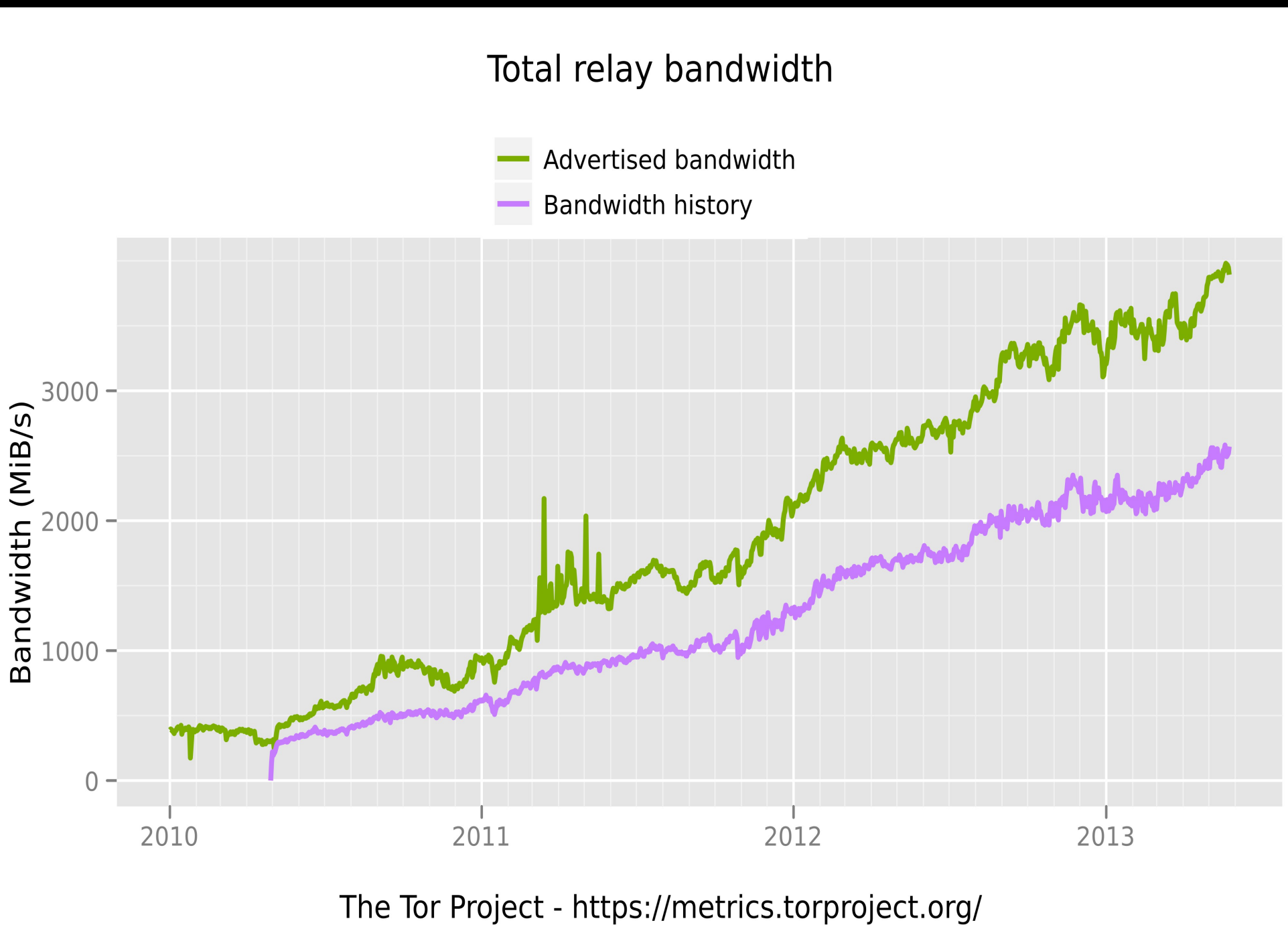
- Torservers.net
- CCC relays in Germany
- DFRI in Sweden
- Noisebridge in the US
- Nos Oignons in France
- …

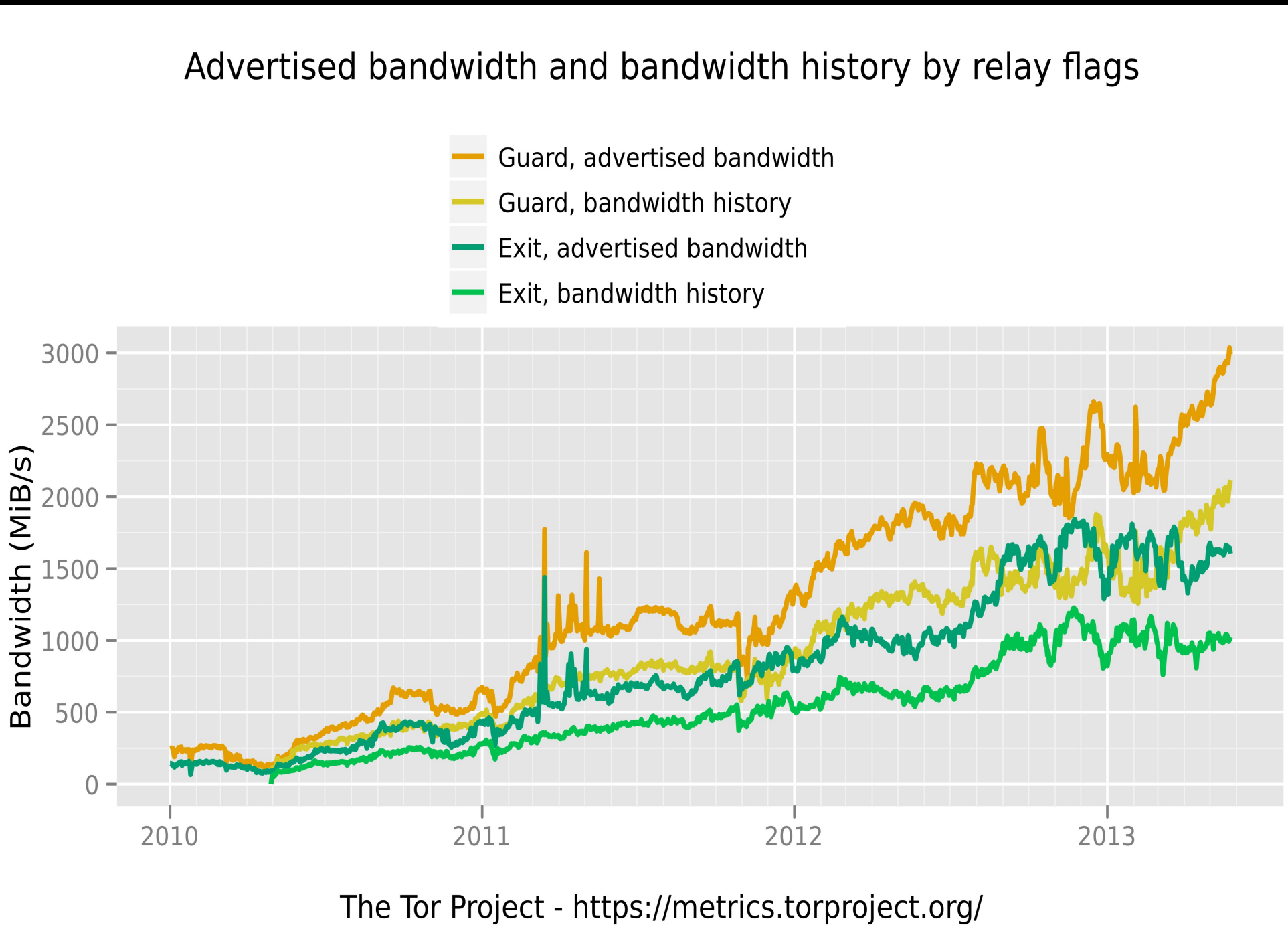
Relay descriptor archives

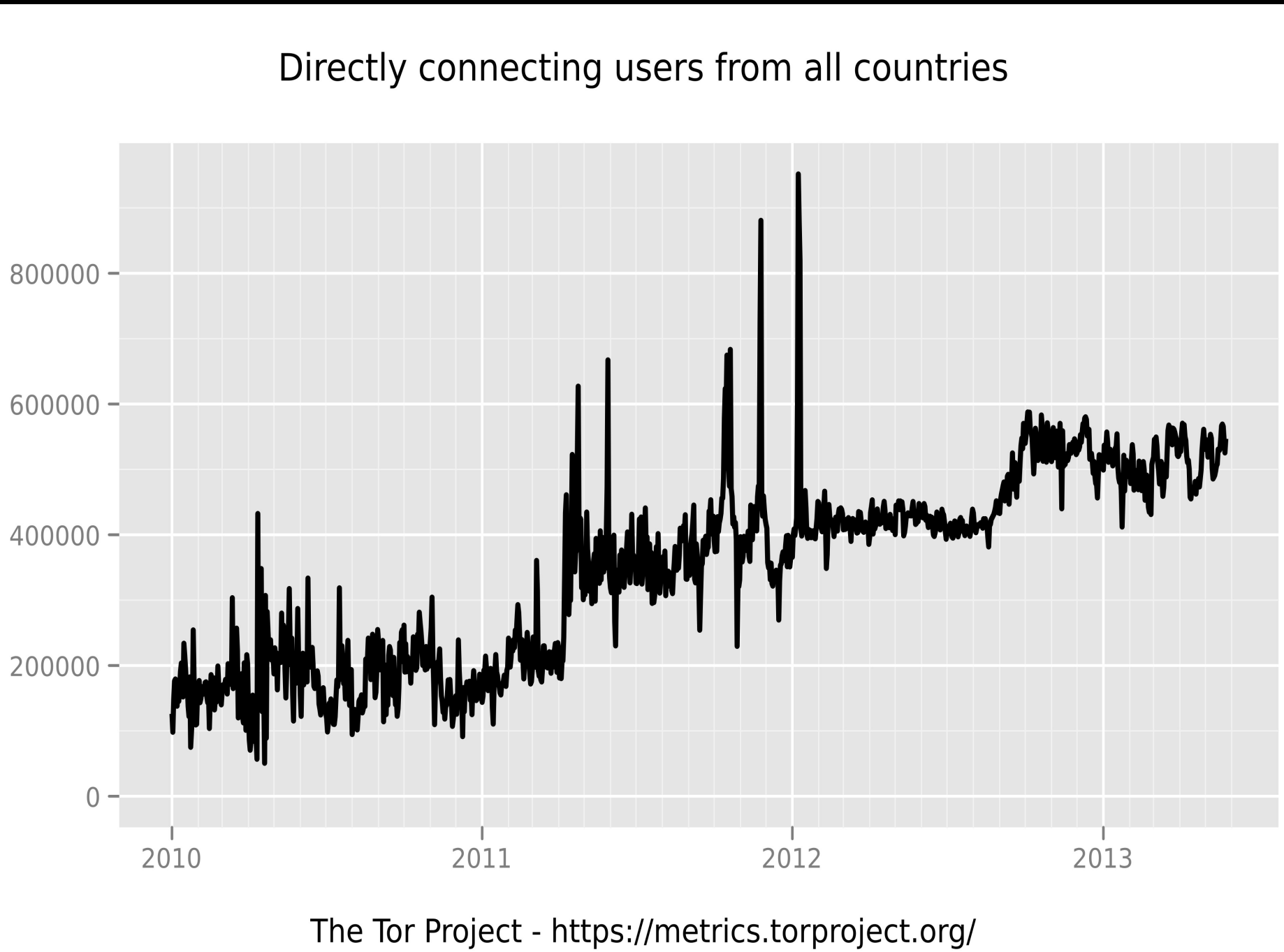
The relay descriptor archives contain all documents that the directory authorities make available about the network of relays. T
include network statuses, server (relay) descriptors, and extra-info descriptors. The data formats are described here.

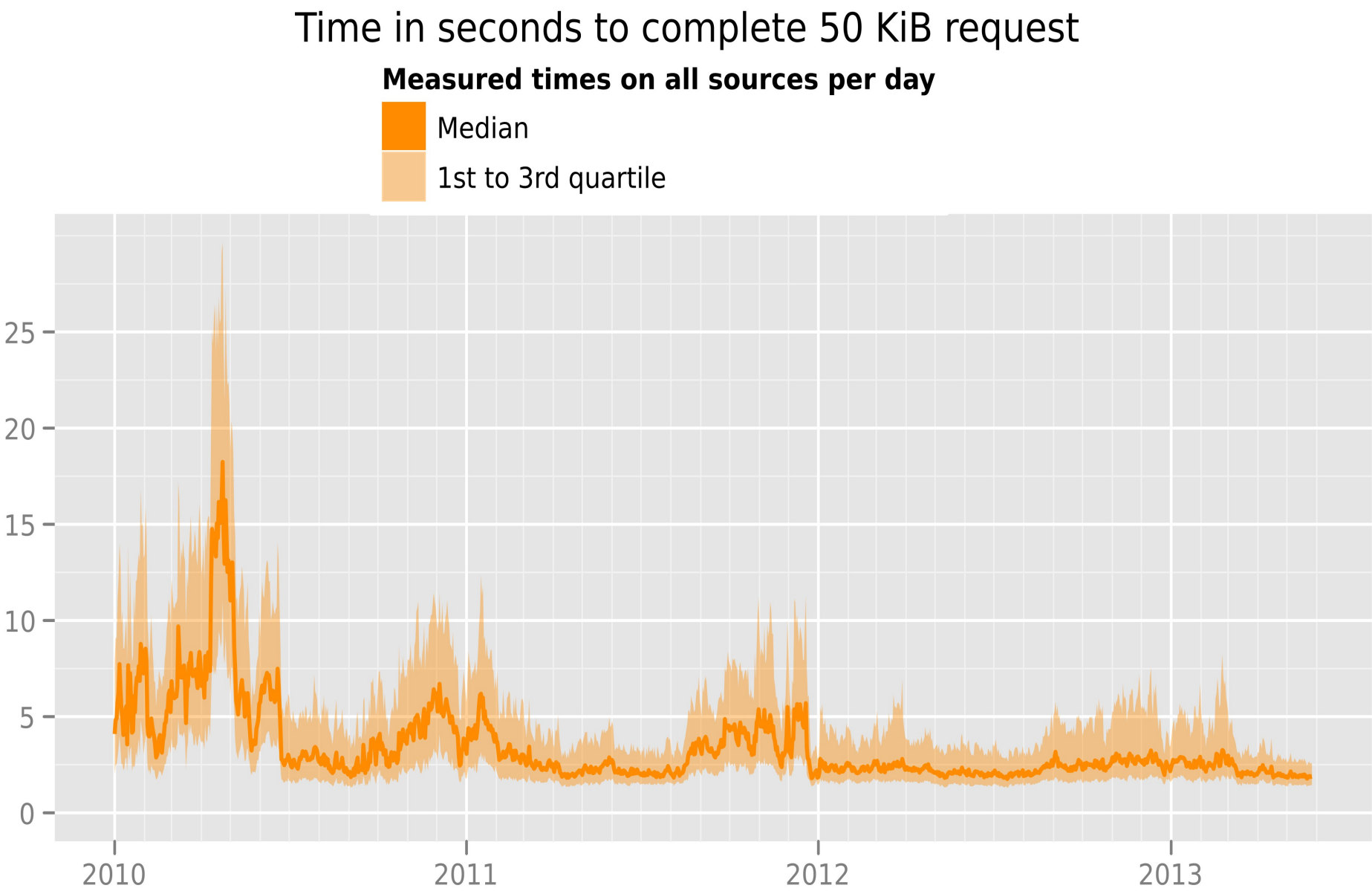
May 2013		server descriptors	extra-infos	v3 votes	v
April 2013		server descriptors	extra-infos	v3 votes	v
March 2013		server descriptors	extra-infos	v3 votes	v
February 2013		server descriptors	extra-infos	v3 votes	v
January 2013		server descriptors	extra-infos	v3 votes	v
December 2012		server descriptors	extra-infos	v3 votes	v
November 2012		server descriptors	extra-infos	v3 votes	v
October 2012		server descriptors	extra-infos	v3 votes	v
September 2012		server descriptors	extra-infos	v3 votes	v
August 2012		server descriptors	extra-infos	v3 votes	v
July 2012		server descriptors	extra-infos	v3 votes	v
June 2012		server descriptors	extra-infos	v3 votes	v
May 2012		server descriptors	extra-infos	v3 votes	v
April 2012		server descriptors	extra-infos	v3 votes	v
March 2012	v2 statuses	server descriptors	extra-infos	v3 votes	v
February 2012	v2 statuses	server descriptors	extra-infos	v3 votes	v
January 2012	v2 statuses	server descriptors	extra-infos	v3 votes	v
December 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v
November 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v
October 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v
September 2011	v2 statuses	server descriptors	extra-infos	v3 votes	v


Number of relays
3500
3000
2500
2000
1500
1000
500
0
2010
2011
2012
2013
Relays
Bridges
The Tor Project - https://metrics.torproject.org/

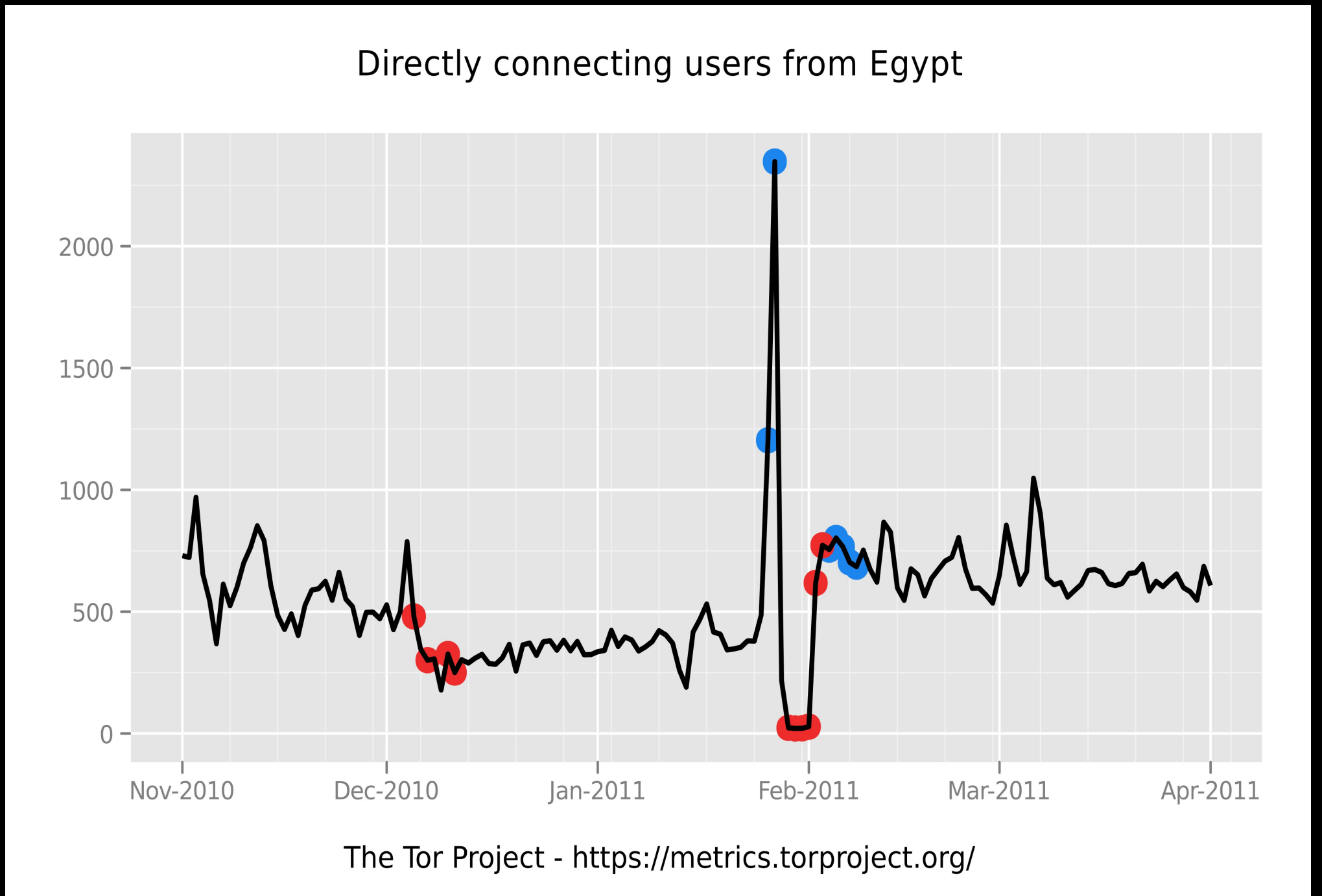

Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (MiB/s)
3000
2000
1000
0
2010
2011
2012
2013
The Tor Project - https://metrics.torproject.org/


Advertised bandwidth and bandwidth history by relay flags
Guard, advertised bandwidth
Guard, bandwidth history
Exit, advertised bandwidth
Exit, bandwidth history
Bandwidth (MiB/s)
3000
2500
2000
1500
1000
500
0
2010
2011
2012
2013
The Tor Project - https://metrics.torproject.org/


Directly connecting users from all countries
800000
600000
400000
200000
0
2010
2011
2012
2013
The Tor Project - https://metrics.torproject.org/



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


Directly connecting users from Egypt
2000
1500
1000
500
0
Nov-2010
Dec-2010
Jan-2011
Feb-2011
Mar-2011
Apr-2011
The Tor Project - https://metrics.torproject.org/

Tor aims for three anonymity properties

- **#1**: A local network attacker can't learn your destination.
- **#2**: No single relay can link you to your destination.
- **#3**: The destination, or somebody watching it, can't learn your location.

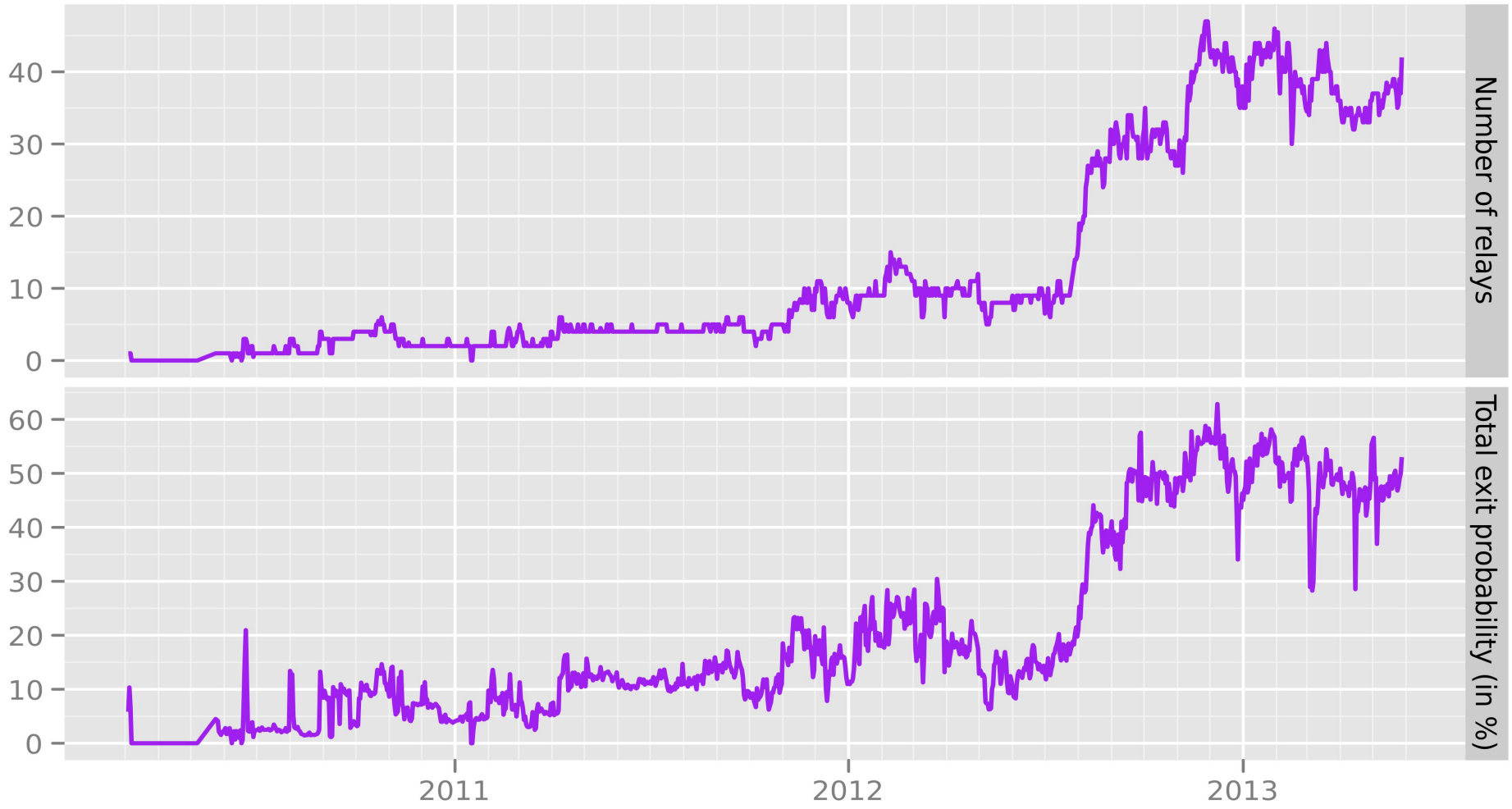
Anonymity: the old hope

- “Anonymity is a function of number of concurrent messages.”
- But, flows are much trickier: they're wildly different sizes, and users expect them to arrive in close-to-real-time.
- More plausible in constrained situation like VoIP?

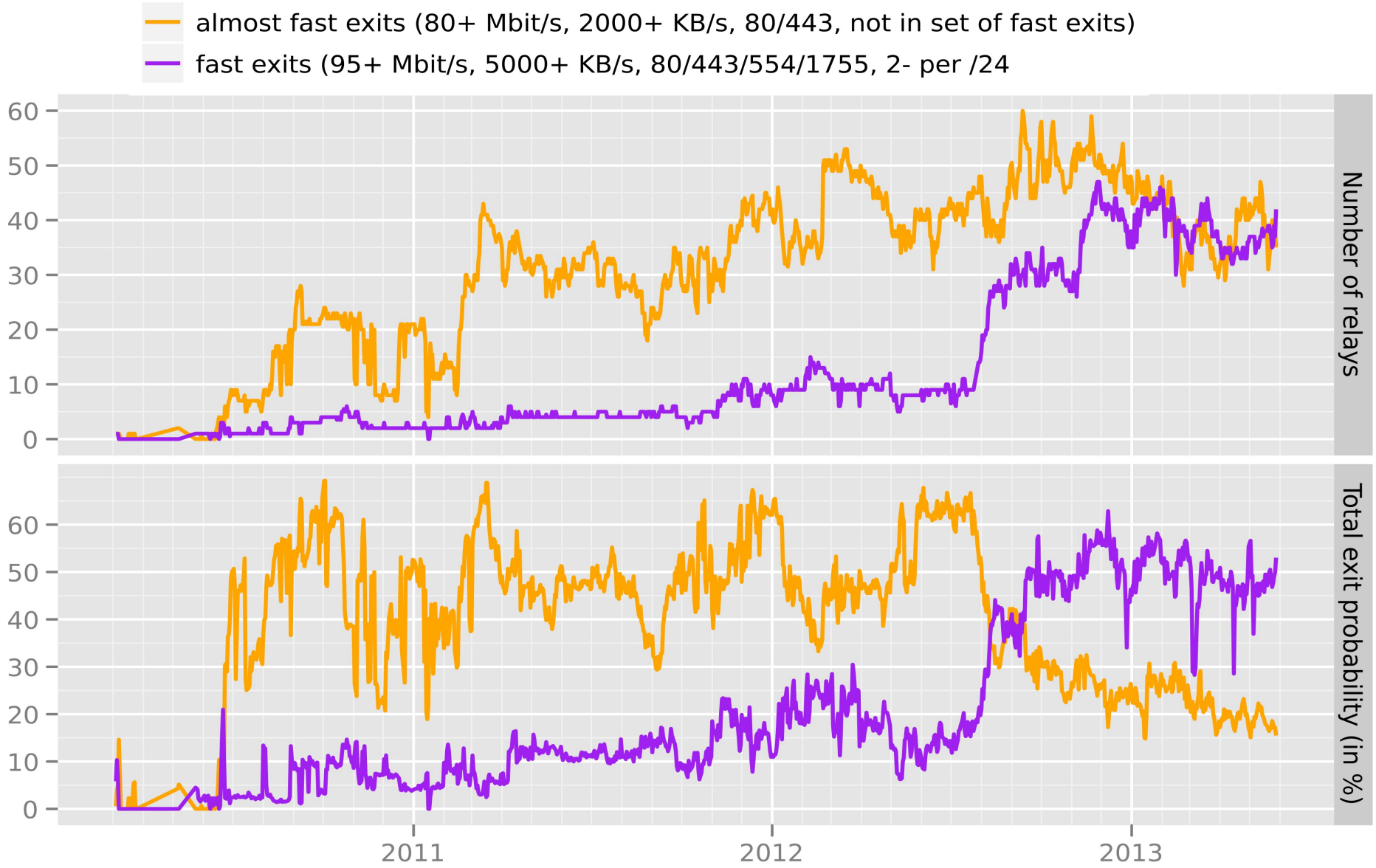
Anonymity: Diversity of relays

- “Given an attacker who can control or observe this set of relays and/or Internet links, we can compute his chances of discovering a given Alice-Bob link.”
  - AS- or IX-level attackers
- ...Syrian Tor user visiting website in Syria?

Fast exits (95+ Mbit/s configured bandwidth rate,
5000+ KB/s advertised bandwidth capacity,
exit to ports 80, 443, 554, and 1755,
at most 2 relays per /24 network)



Relays almost meeting the fast-exit requirements



Tor Tech Reports

Philipp Winter. Design requirements for a Tor censorship analysis tool. Technical Report 2013-02-001, The T

Karsten Loesing. Counting daily bridge users. Technical Report 2012-10-001, The Tor Project, October 2012

[...]

Karsten Loesing. Case study: Learning whether a Tor bridge is blocked by looking at its aggregate usage sta 2011-09-002, The Tor Project, September 2011. [bib | .pdf]

George Danezis. An anomaly-based censorship-detection system for Tor. Technical Report 2011-09-001, Th .pdf]

Roger Dingledine. Better guard rotation parameters. Technical Report 2011-08-001, The Tor Project, August

Roger Dingledine. Strategies for getting more bridges. Technical Report 2011-05-001, The Tor Project, May

Karsten Loesing. Overview of statistical data in the Tor network. Technical Report 2011-03-001, The Tor Proj

Roger Dingledine. Measuring the safety of the Tor network. Technical Report 2011-02-001, The Tor Project,

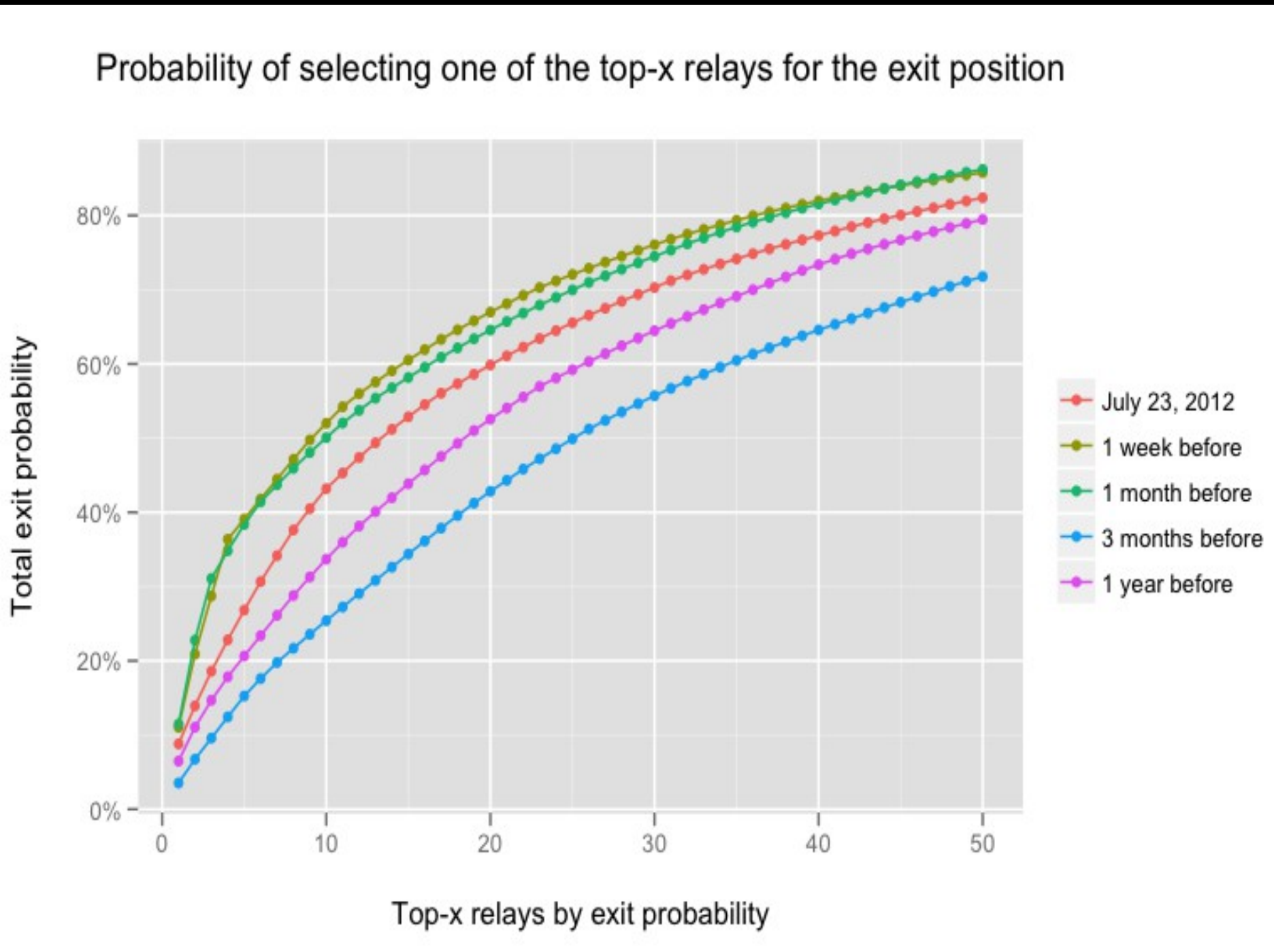
Sebastian Hahn and Karsten Loesing. Privacy-preserving ways to estimate the number of Tor users. Technic November 2010. [bib | .pdf]

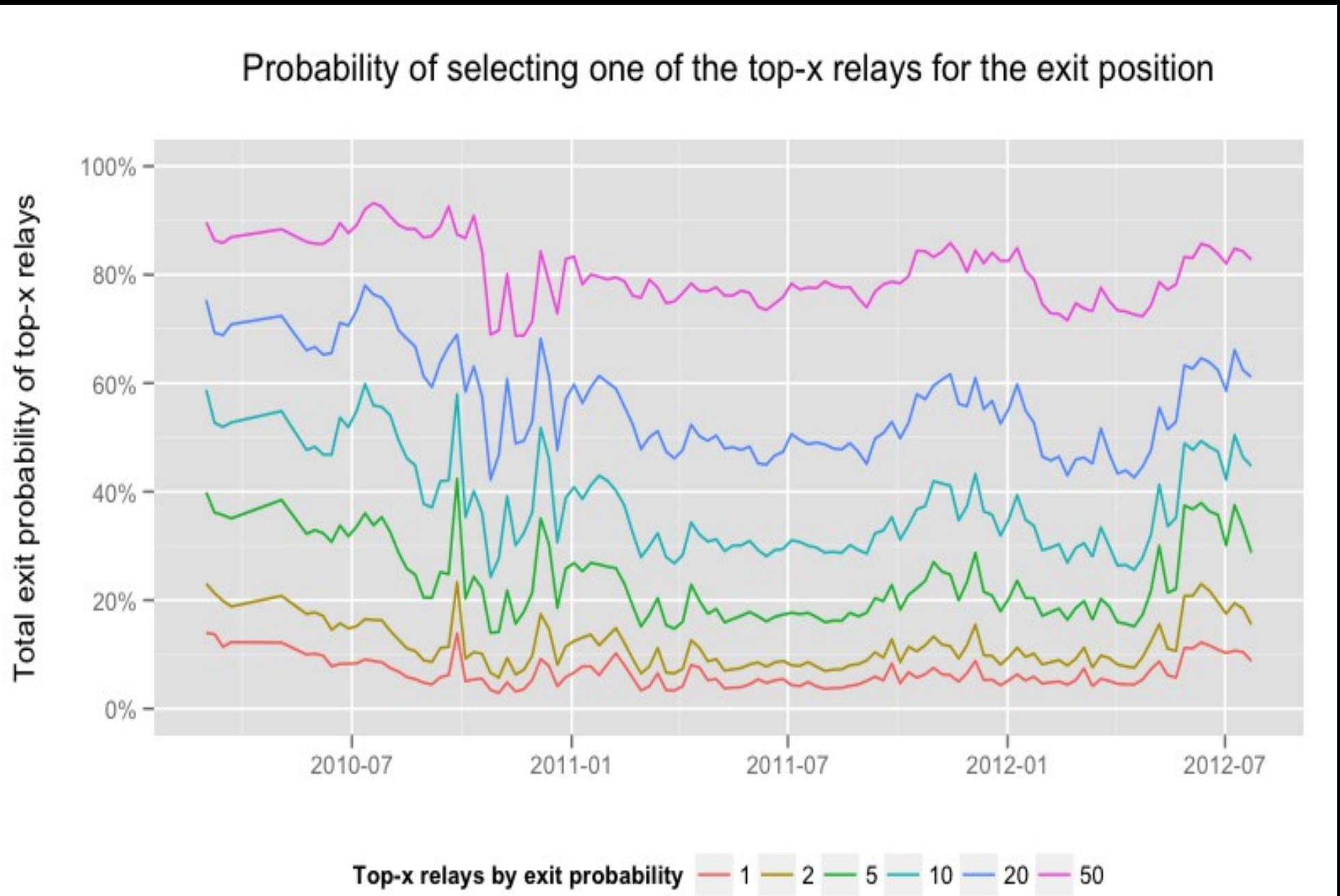
Roger Dingledine. Adaptive throttling of Tor clients by entry guards. Technical Report 2010-09-001, The Tor

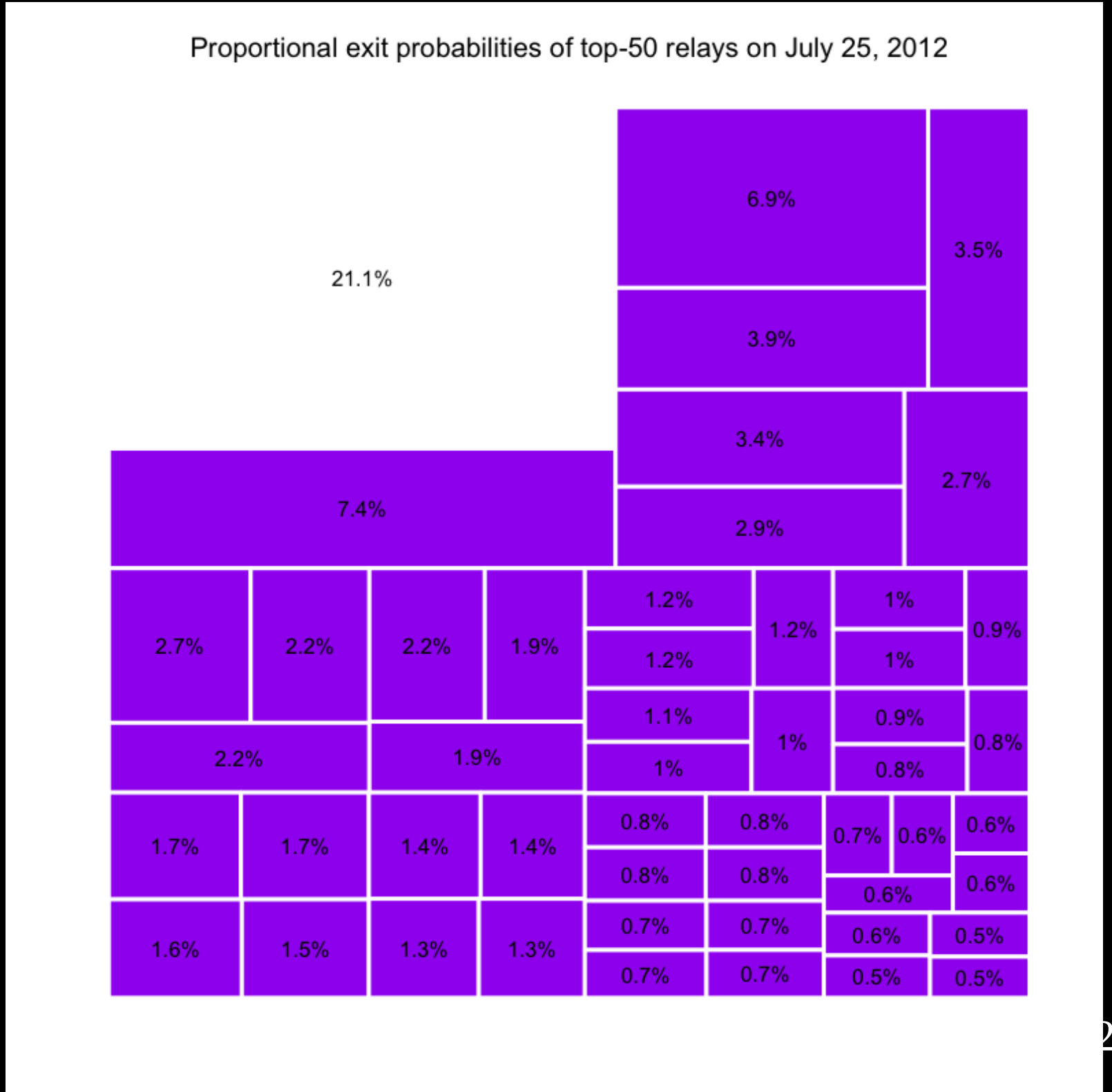
Roger Dingledine and Steven J. Murdoch. Performance improvements on Tor or, why Tor is slow and what w Report 2009-11-001, The Tor Project, November 2009. [bib | .pdf]

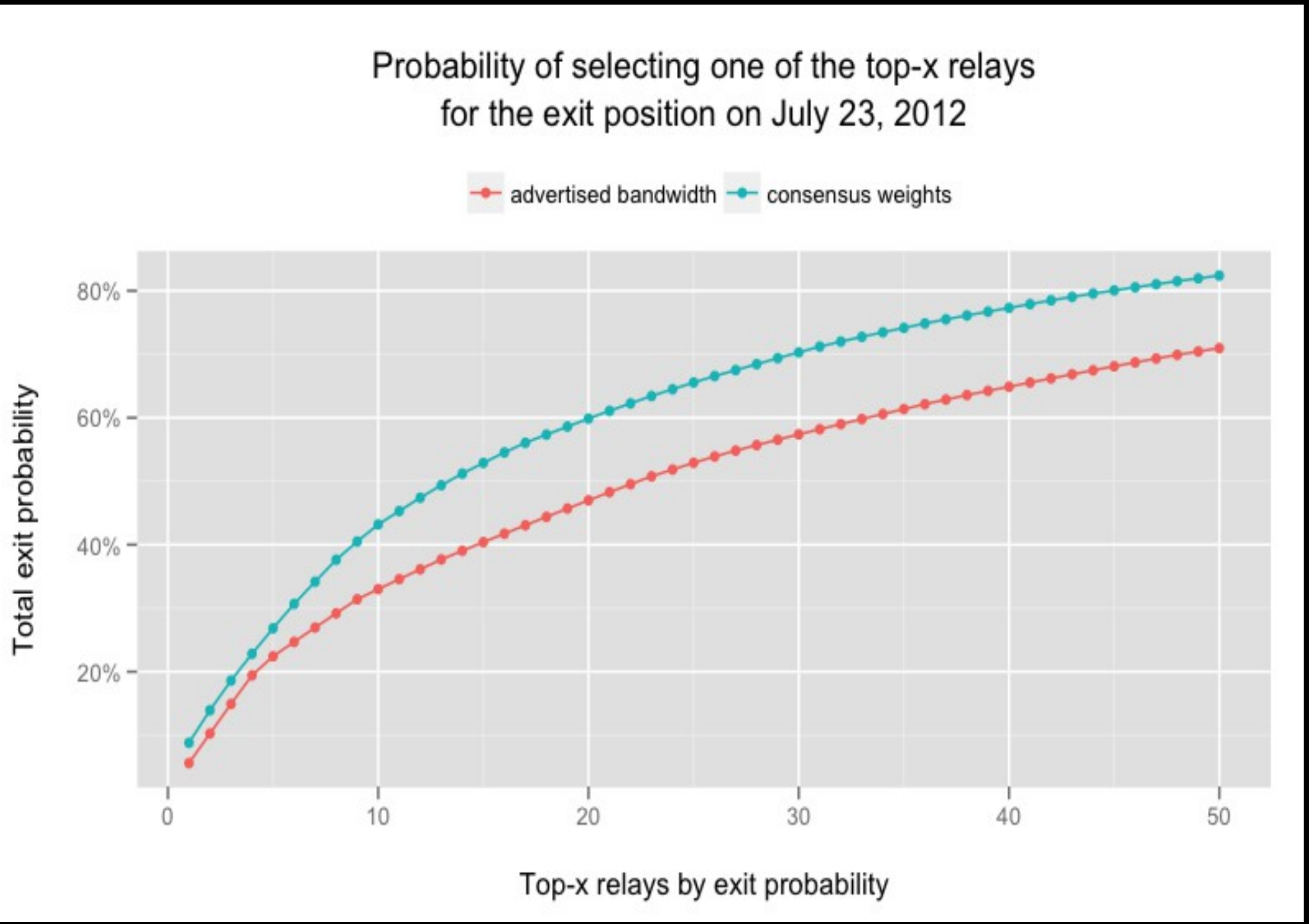
Karsten Loesing. Comparison of GeoIP databases for Tor. Technical Report 2009-10-001, The Tor Project, C

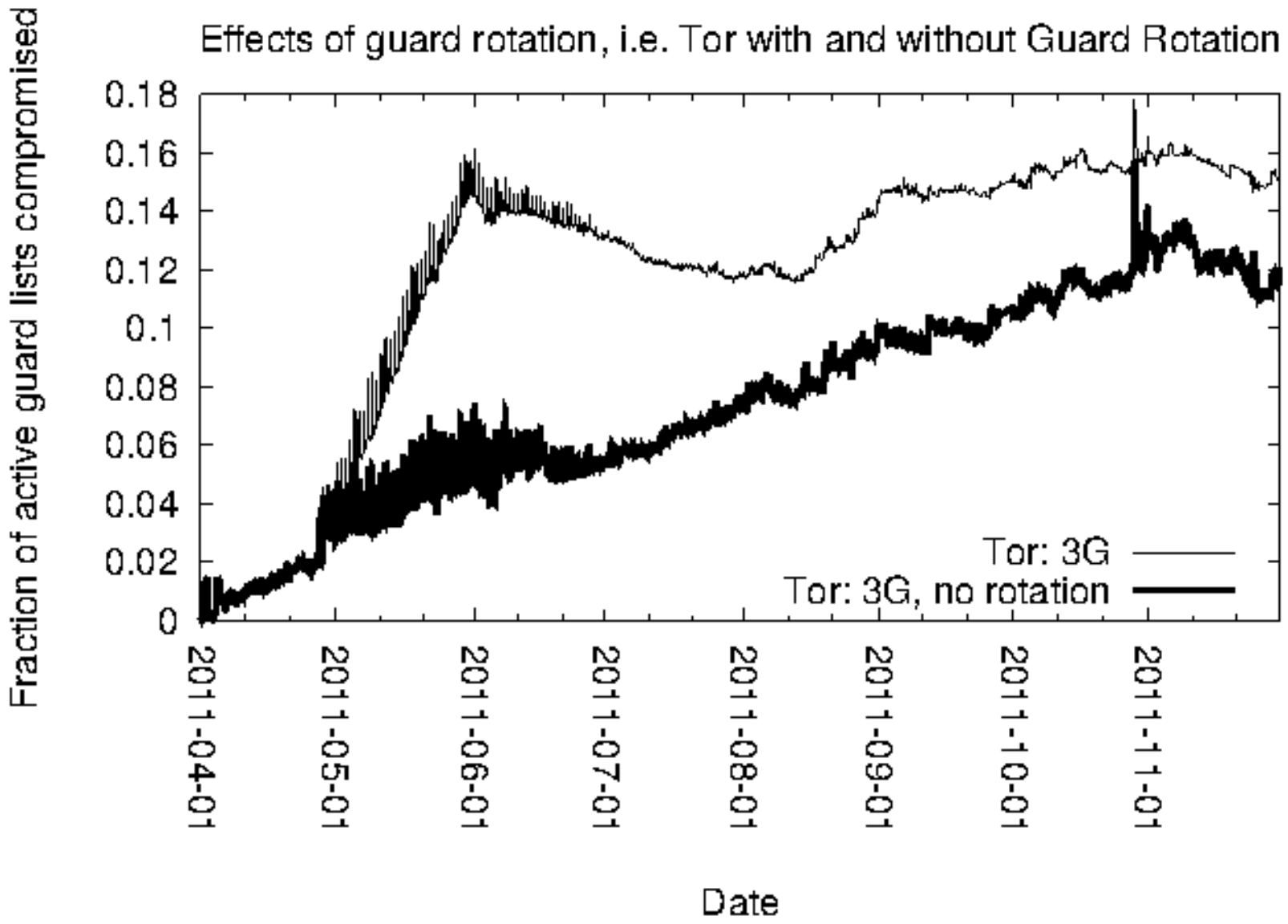
Karsten Loesing. Performance of requests over the Tor network. Technical Report 2009-09-001, The Tor Pro


Probability of selecting one of the top-x relays for the exit position
Total exit probability
80%
60%
40%
20%
0%
0
10
20
30
40
50
Top-x relays by exit probability
July 23, 2012
1 week before
1 month before
3 months before
1 year before

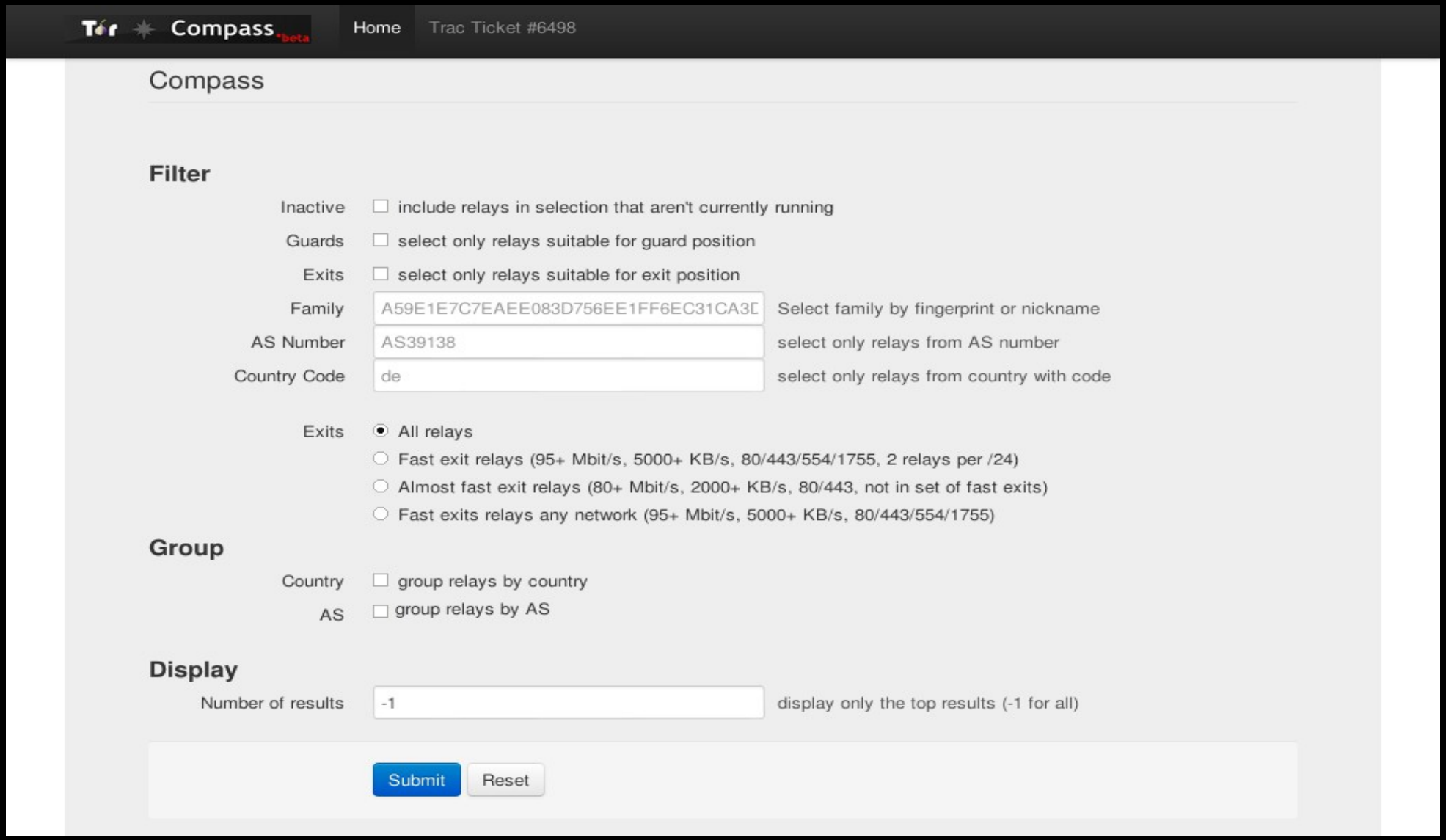

Probability of selecting one of the top-x relays for the exit position
Total exit probability of top-x relays
100%
80%
60%
40%
20%
0%
2010-07
2011-01
2011-07
2012-01
2012-07
Top-x relays by exit probability
1
2
5
10
20
50


Proportional exit probabilities of top-50 relays on July 25, 2012
21.1%
6.9%
3.5%
3.9%
3.4%
2.7%
7.4%
2.9%
2.7%
2.2%
2.2%
1.9%
1.2%
1.2%
1.2%
1%
1%
0.9%
2.2%
1.9%
1.1%
1%
1%
0.9%
0.8%
0.8%
1.7%
1.7%
1.4%
1.4%
0.8%
0.8%
0.8%
0.8%
0.7%
0.6%
0.6%
0.6%
1.6%
1.5%
1.3%
1.3%
0.7%
0.7%
0.7%
0.7%
0.6%
0.5%
0.5%
0.5%


Probability of selecting one of the top-x relays
for the exit position on July 23, 2012
advertised bandwidth
consensus weights
80%
60%
40%
20%
Total exit probability
0
10
20
30
40
50
Top-x relays by exit probability


Effects of guard rotation, i.e. Tor with and without Guard Rotation
Fraction of active guard lists compromised
0.18
0.16
0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
2011-04-01
2011-05-01
2011-06-01
2011-07-01
2011-08-01
2011-09-01
2011-10-01
2011-11-01
Date
Tor: 3G
Tor: 3G, no rotation

compass.torproject.org



compass.torproject.org

Tor Compass beta | Home | Trac Ticket #6498

#	Consensus Weights	Advertised Bandwidth	Guard Probability	Middle Probability	Exit Probability	Nickname	Fingerprint	Exit	Guard	Country	Autonomous System
1	3.2680%	1.0554%	1.6295%	1.6295%	6.5450%	TorLand1	4E377F91	Exit	Guard	??	AS13213 UK-2 Ltd Autonomous System
2	2.9021%	0.9346%	1.4470%	1.4471%	5.8122%	chaoscomputerclub20	CFA48FC3	Exit	Guard	de	AS39138 rrbone UG
3	2.4947%	0.8704%	1.2439%	1.2439%	4.9961%	chaoscomputerclub19	A59E1E7C	Exit	Guard	de	AS39138 rrbone UG
4	1.6714%	1.1596%	0.0000%	3.8116%	1.2026%	manning1	073F2793	Exit	-	us	AS29761 OC3 Networks & Web Solutions, LLC
5	1.4552%	0.9069%	0.7256%	0.7256%	2.9144%	TorLand2	332895D0	Exit	Guard	??	AS13213 UK-2 Ltd Autonomous System
6	1.3638%	1.1625%	0.0000%	3.1100%	0.9812%	dorrisdeebrown	C1E2CF4B	Exit	-	us	AS8100 IPTelligent LLC
7	1.1891%	0.3974%	0.5929%	0.5929%	2.3815%	chaoscomputerclub4	659DF653	Exit	Guard	de	AS20773 Host Europe GmbH
8	1.1143%	0.3121%	0.0000%	2.5411%	0.8017%	Unnamed	2624AE04	Exit	-	se	AS47155 ViaEuropa Sweden
9	1.0478%	0.4420%	0.5224%	0.5224%	2.0984%	kramse	3C5DF71E	Exit	Guard	dk	AS197564 Solido Networks ApS
10	1.0228%	0.5791%	0.5100%	0.5100%	2.0484%	assk	8543536F	Exit	Guard	se	AS51815 Teknikbyran i Sverige AB
11	0.9480%	0.3556%	0.0000%	2.1618%	0.6821%	Unnamed	AE5A97FA	Exit	-	se	AS47155 ViaEuropa

compass.torproject.org

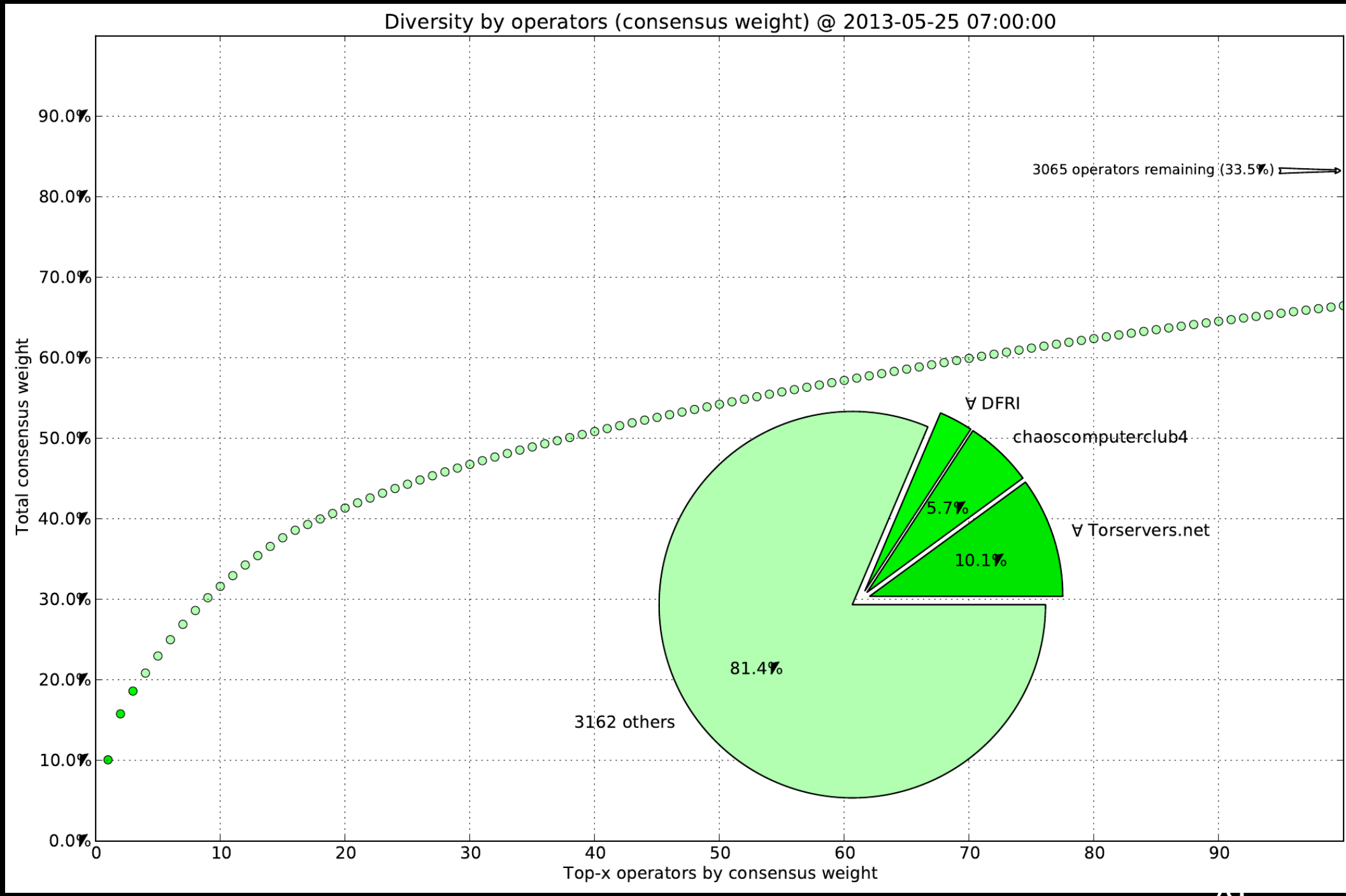
Tor Compass *beta | Home | Trac Ticket #6498

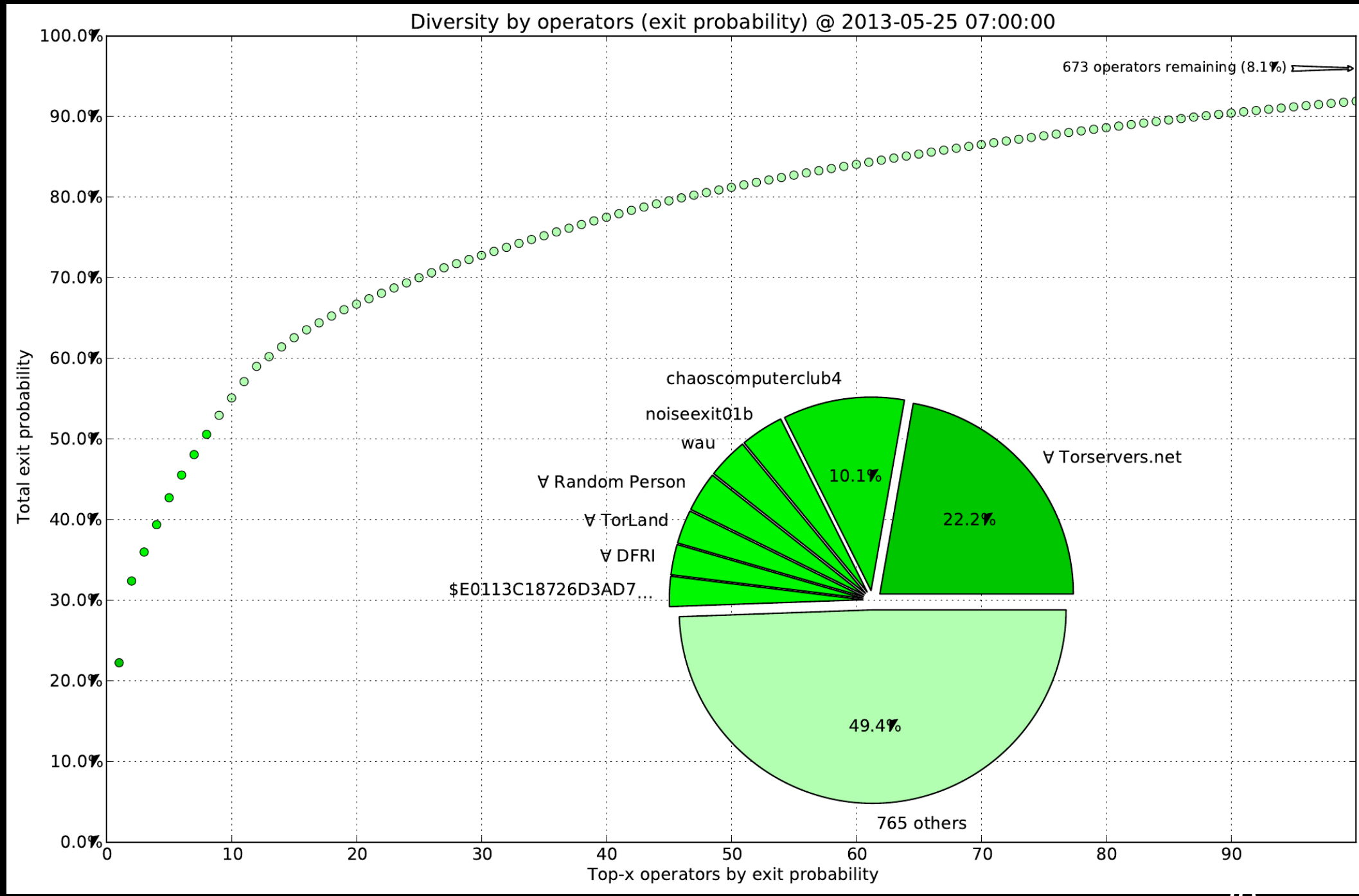
#	Consensus Weights	Advertised Bandwidth	Guard Probability	Middle Probability	Exit Probability	Nickname	Fingerprint	Exit	Guard	Country	Autonomous System
11	16.9410%	9.3179%	7.3388%	12.4071%	31.0763%	*	(93 relays)	(93)	(50)	de	(36)
11	16.4037%	15.9140%	4.2991%	22.0444%	22.8665%	*	(196 relays)	(196)	(58)	us	(94)
11	6.9328%	3.5566%	2.4072%	7.2074%	11.1835%	*	(18 relays)	(18)	(6)	??	(10)
11	5.9957%	3.9851%	1.4297%	8.5637%	7.9934%	*	(35 relays)	(35)	(17)	se	(14)
11	4.3453%	3.6399%	1.1942%	5.6417%	6.1998%	*	(62 relays)	(62)	(18)	nl	(21)
11	2.0473%	1.6717%	0.4237%	3.1546%	2.5635%	*	(69 relays)	(69)	(13)	fr	(15)
11	1.5967%	1.0994%	0.7739%	0.8758%	3.1405%	*	(23 relays)	(23)	(11)	ca	(13)
11	1.5656%	3.3506%	0.7397%	0.9267%	3.0302%	*	(15 relays)	(15)	(10)	ro	(5)
11	1.3084%	0.7519%	0.6420%	0.6896%	2.5936%	*	(14 relays)	(14)	(6)	dk	(8)
11	0.7217%	1.2861%	0.1452%	1.1270%	0.8928%	*	(134 relays)	(134)	(13)	ru	(49)
11	0.7048%	0.6389%	0.3347%	0.4111%	1.3686%	*	(12 relays)	(12)	(5)	ch	(5)
11	0.6985%	0.3215%	0.3387%	0.3826%	1.3742%	*	(28 relays)	(28)	(5)	gb	(16)
11	0.6395%	0.7764%	0.2571%	0.5397%	1.1218%	*	(26 relays)	(26)	(6)	ua	(17)
11	0.6238%	0.6516%	0.1891%	0.7468%	0.9354%	*	(21 relays)	(21)	(2)	lu	(2)
11	0.4634%	0.4638%	0.2308%	0.2320%	0.9274%	*	(14 relays)	(14)	(12)	cz	(8)
11	0.4285%	0.2444%	0.2136%	0.2141%	0.8580%	*	(3 relays)	(3)	(2)	gr	(2)
11	0.3941%	0.2973%	0.1961%	0.1979%	0.7883%	*	(2 relays)	(2)	(1)	a2	(2)
11	0.3166%	0.5118%	0.0431%	0.5680%	0.3388%	*	(8 relays)	(8)	(1)	eu	(5)
11	0.2070%	0.2899%	0.1022%	0.1070%	0.4119%	*	(10 relays)	(10)	(3)	pl	(7)
11	0.0730%	0.1709%	0.0010%	0.1630%	0.0551%	*	(9 relays)	(9)	(1)	at	(5)
11	0.0510%	0.1195%	0.0000%	0.1162%	0.0367%	*	(4 relays)	(4)	(0)	lv	(4)
11	0.0235%	0.0295%	0.0117%	0.0117%	0.0471%	*	(1 relays)	(1)	(1)	md	(1)

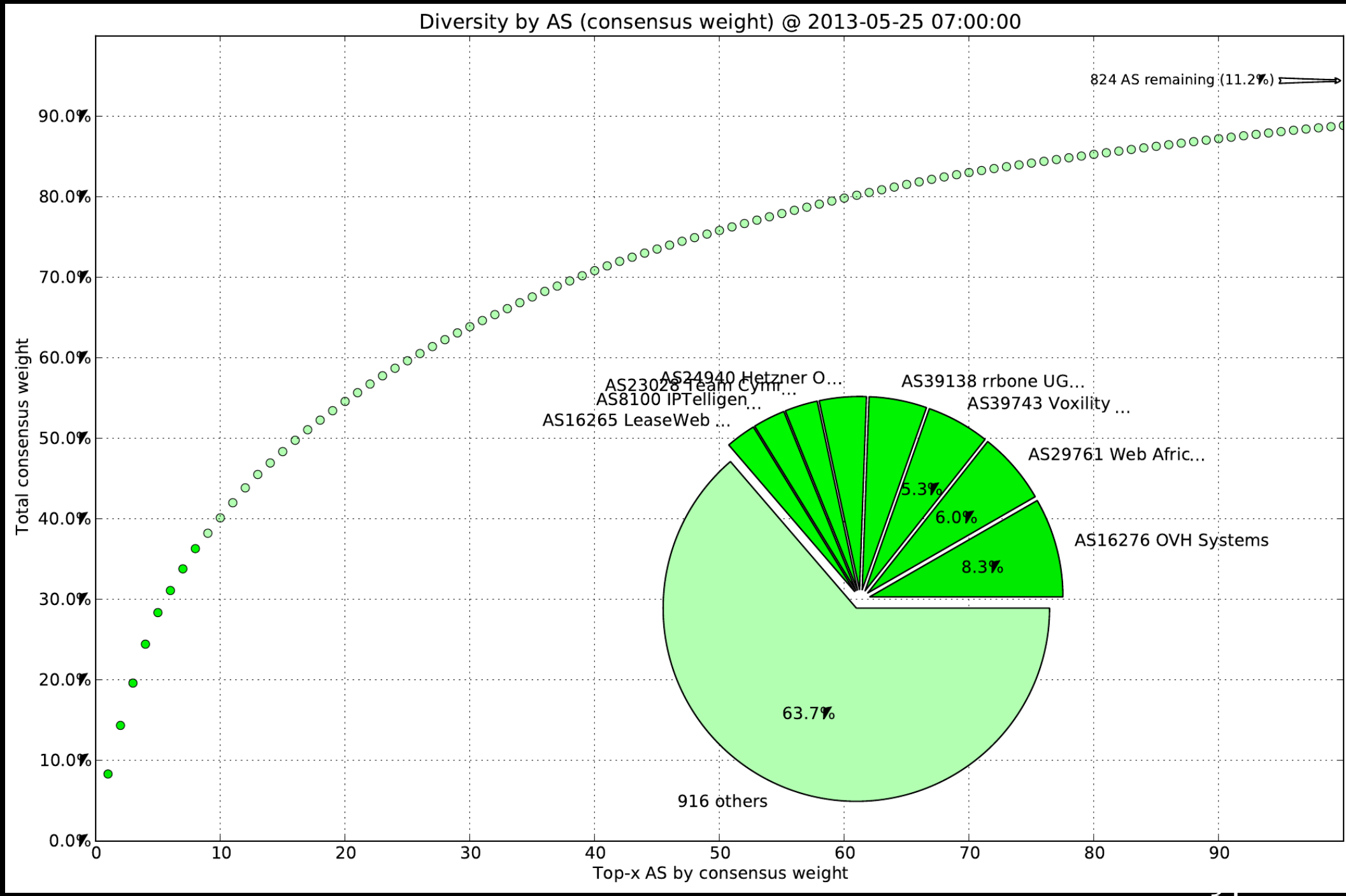
compass.torproject.org

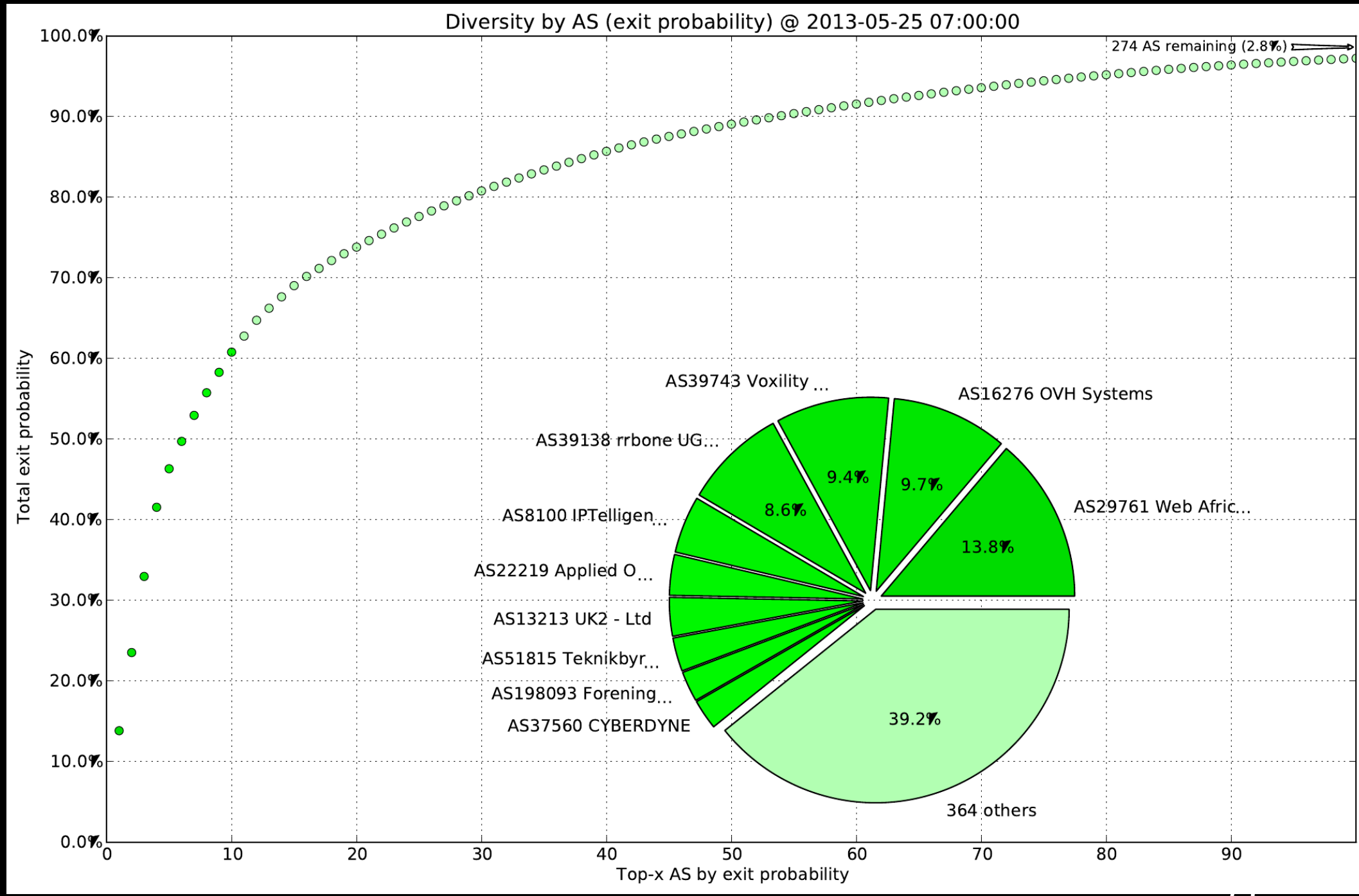
Tor Compass *beta | Home | Trac Ticket #6498

#	Consensus Weights	Advertised Bandwidth	Guard Probability	Middle Probability	Exit Probability	Nickname	Fingerprint	Exit	Guard	Country	Autonomous System
14	9.4299%	3.5801%	4.7018%	4.7020%	18.8854%	*	(4 relays)	(4)	(4)	de	AS39138 rrbone UG
15	6.4778%	2.9081%	2.3550%	6.3564%	10.7218%	*	(3 relays)	(3)	(2)	??	AS13213 UK-2 Ltd Autonomous System
17	5.0251%	4.8345%	0.8015%	8.5954%	5.6782%	*	(7 relays)	(7)	(4)	us	AS29761 OC3 Networks & Web Solutions, LLC
14	3.6971%	1.8147%	1.8434%	1.8435%	7.4043%	*	(6 relays)	(6)	(6)	de	AS20773 Host Europe GmbH
14	3.5358%	2.7354%	1.1278%	4.0330%	5.4464%	*	(5 relays)	(5)	(3)	nl	AS43350 NFOrce Entertainment BV
13	2.9845%	3.5895%	0.0000%	6.8059%	2.1473%	*	(3 relays)	(3)	(0)	us	AS8100 IPTelligent LLC
13	2.8958%	1.7706%	0.7035%	4.0899%	3.8940%	*	(33 relays)	(33)	(11)	fr	AS16276 OVH Systems
14	2.8739%	2.1561%	1.4329%	1.4330%	5.7556%	*	(8 relays)	(8)	(8)	us	AS22219 Applied Operations, LLC
13	2.6111%	1.0402%	0.0000%	5.9544%	1.8786%	*	(3 relays)	(3)	(0)	se	AS47155 ViaEuropa Sweden
15	1.8436%	1.1358%	0.9192%	0.9193%	3.6922%	*	(2 relays)	(2)	(2)	se	AS51815 Teknikbyran i Sverige AB
13	1.6806%	3.5000%	0.7199%	1.2600%	3.0618%	*	(13 relays)	(13)	(8)	ro	AS39743 Voxility SRL
14	1.0478%	0.4420%	0.5224%	0.5224%	2.0984%	*	(1 relays)	(1)	(1)	dk	AS197564 Solido Networks ApS

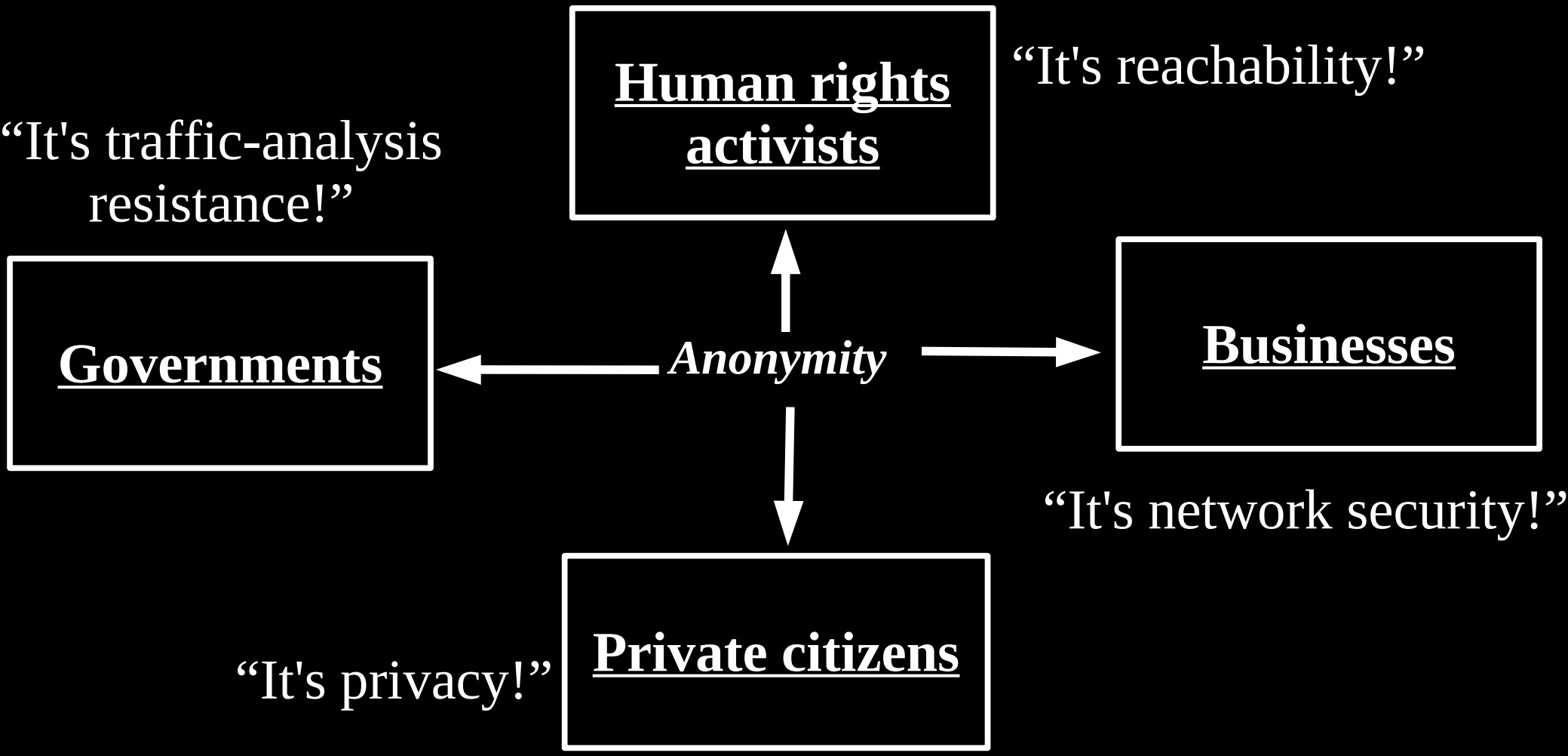

Diversity by operators (consensus weight) @ 2013-05-25 07:00:00
Total consensus weight
Top-x operators by consensus weight
0.0%
10.0%
20.0%
30.0%
40.0%
50.0%
60.0%
70.0%
80.0%
90.0%
0
10
20
30
40
50
60
70
80
90
3065 operators remaining (33.5%)
∀ DFRI
chaoscomputerclub4
∀ Torservers.net
5.7%
10.1%
81.4%
3162 others


Diversity by operators (exit probability) @ 2013-05-25 07:00:00
673 operators remaining (8.1%)
Total exit probability
Top-x operators by exit probability
100.0%
90.0%
80.0%
70.0%
60.0%
50.0%
40.0%
30.0%
20.0%
10.0%
0.0%
0
10
20
30
40
50
60
70
80
90
chaoscomputerclub4
noiseexit01b
wau
∀ Random Person
∀ TorLand
∀ DFRI
$E0113C18726D3AD7...
10.1%
∀ Torservers.net
22.2%
49.4%
765 others


Diversity by AS (consensus weight) @ 2013-05-25 07:00:00
824 AS remaining (11.2%)
Total consensus weight
Top-x AS by consensus weight
0.0%
10.0%
20.0%
30.0%
40.0%
50.0%
60.0%
70.0%
80.0%
90.0%
0
10
20
30
40
50
60
70
80
90
AS24940 Hetzner O...
AS23028 Team Cymr ...
AS8100 IPTelligen...
AS16265 LeaseWeb ...
AS39138 rrbone UG...
AS39743 Voxility ...
AS29761 Web Afric...
AS16276 OVH Systems
5.3%
6.0%
8.3%
63.7%
916 others


Diversity by AS (exit probability) @ 2013-05-25 07:00:00
274 AS remaining (2.8%)
Total exit probability
Top-x AS by exit probability
100.0%
90.0%
80.0%
70.0%
60.0%
50.0%
40.0%
30.0%
20.0%
10.0%
0.0%
0
10
20
30
40
50
60
70
80
90
AS39743 Voxility ...
AS16276 OVH Systems
AS39138 rrbone UG...
AS8100 IPTelligen...
AS22219 Applied O...
AS13213 UK2 - Ltd
AS51815 Teknikbyr...
AS198093 Forening...
AS37560 CYBERDYNE
AS29761 Web Afric...
9.4%
9.7%
8.6%
13.8%
39.2%
364 others

Anonymity serves different interests for different user groups.



Anonymity: Diversity of *users*?

- Can't have an anonymity network for just cancer survivors
- 50000 daily Tor users in Iran means almost all of them are normal citizens
- But, the smaller the area, the smaller the anonymity set

Anonymity: End-to-end correlation?

- Website fingerprinting is a real issue, and may be amenable to partial solutions like padding
- Can we resurrect the anonymity set?
- “Crank up the false positives with enough users”

Coming soon(*)

- Stream isolation
- Multi-path circuits
- Congestion-aware routing
- Mixed-latency designs?
- Load balancing based on link properties
- Incentives to be a relay
- Trust-based path selection
- Scalable directory servires (PIRTor, etc)

What happens to anonymity...

- ...if we assign the Guard flag differently?
- ...if we load balance by active measurement rather than consensus bw?
- ...if we cap the weights for new relays?
- ...if we discard all relays under bw X?
- ...if we discard X% highest-latency paths?
- ...if Alice chooses her paths to optimize some other network parameter like jitter?