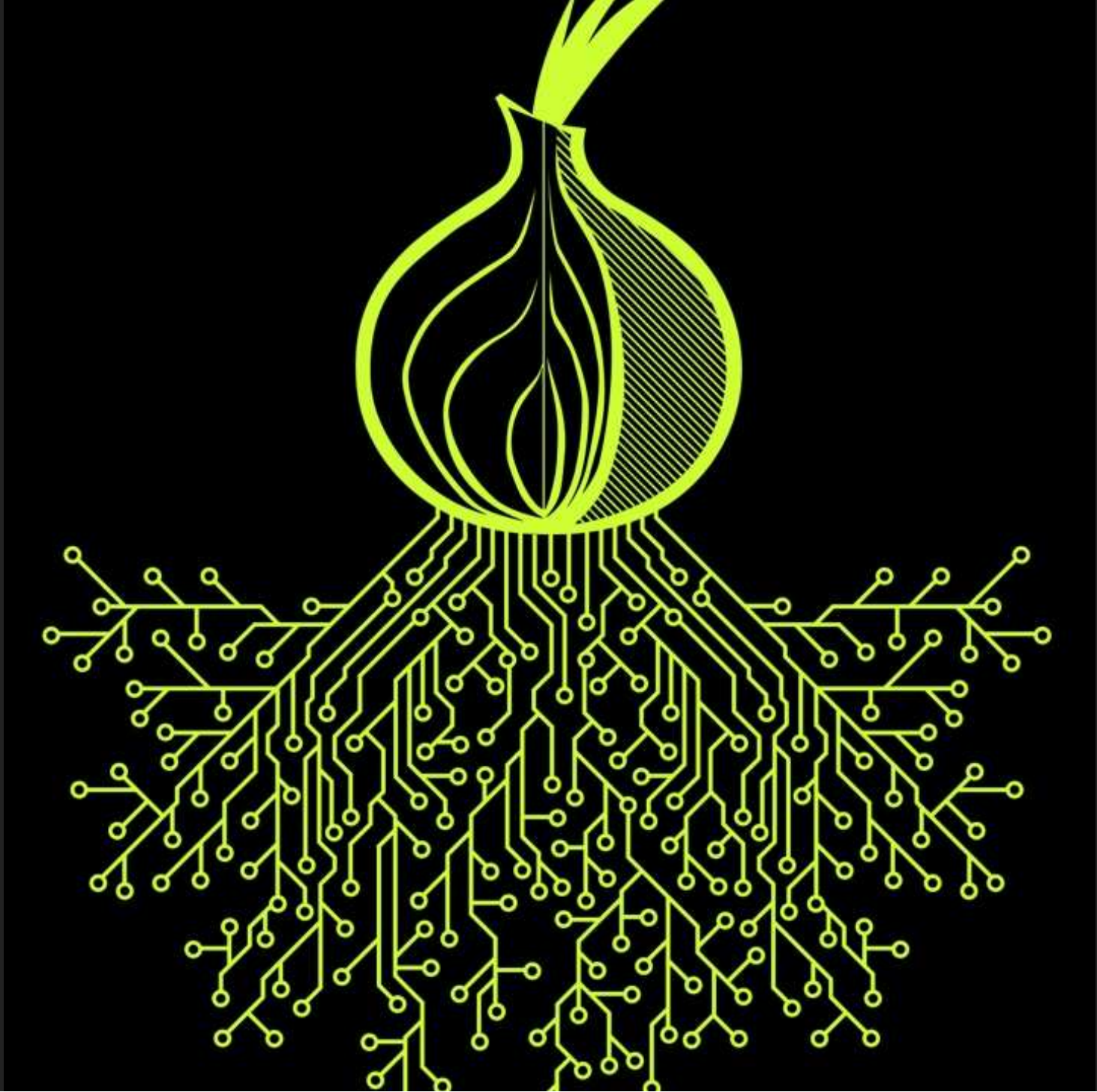
THE TOR PROJECT

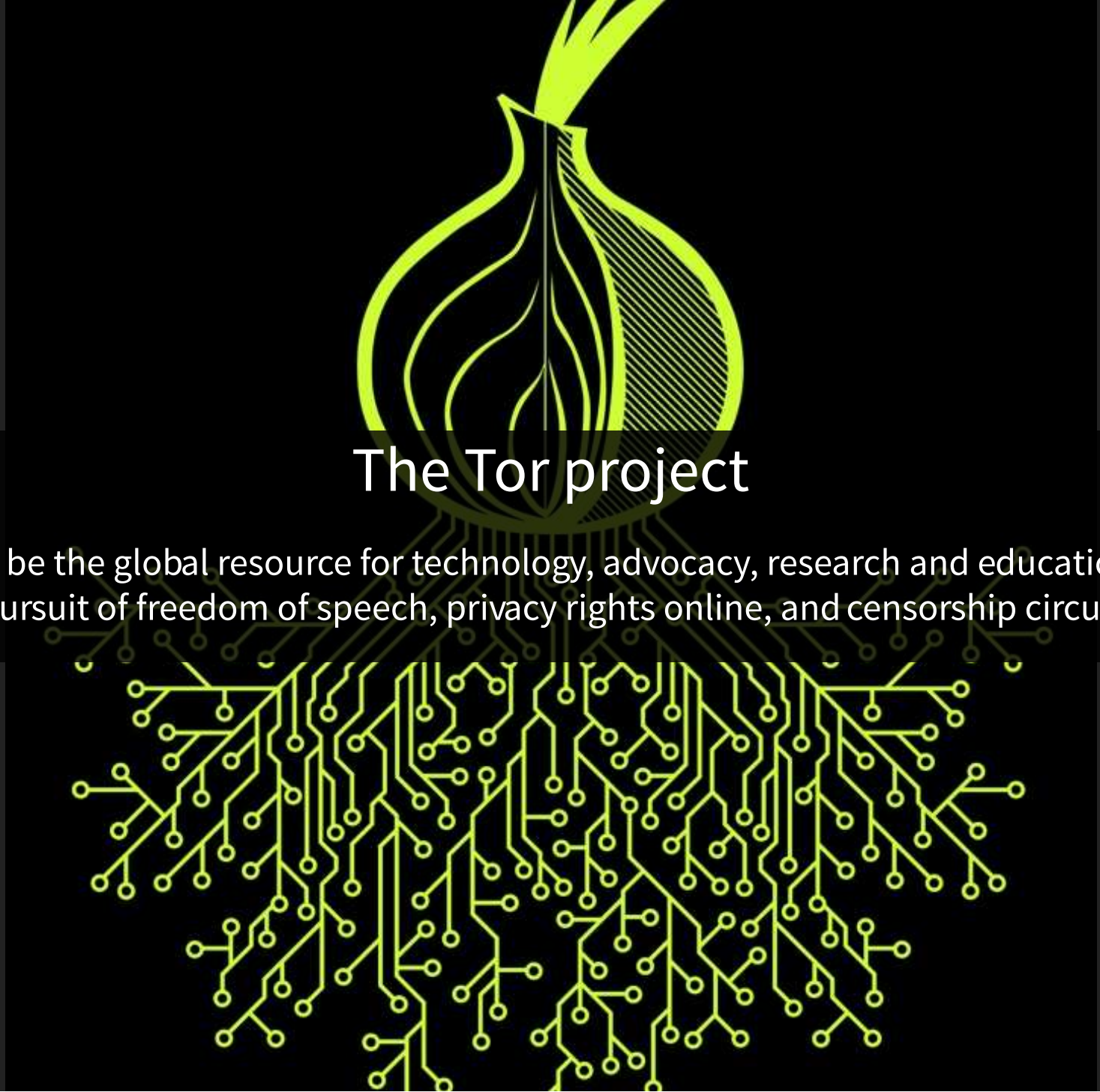
~

OONI

Vasilis Ververis (andz@torproject.org)

GPG Fingerprint: 8FD5 CF5F 39FC 03EB B382 7470 5FBF 70B1 D126 0162
Public Key: https://pgp.mit.edu/pks/lookup?op=get&search=0x5FBF70B1D1260162



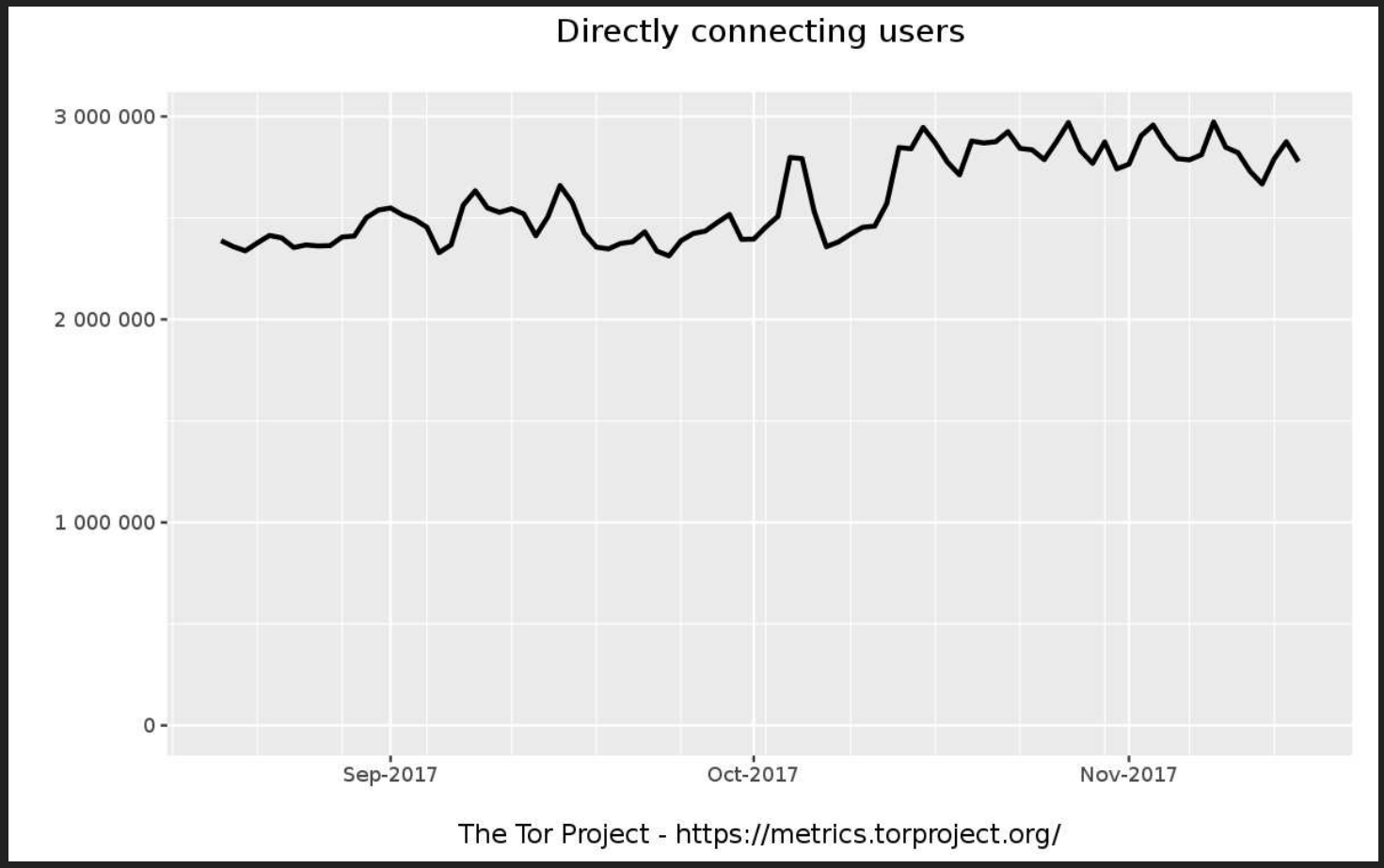


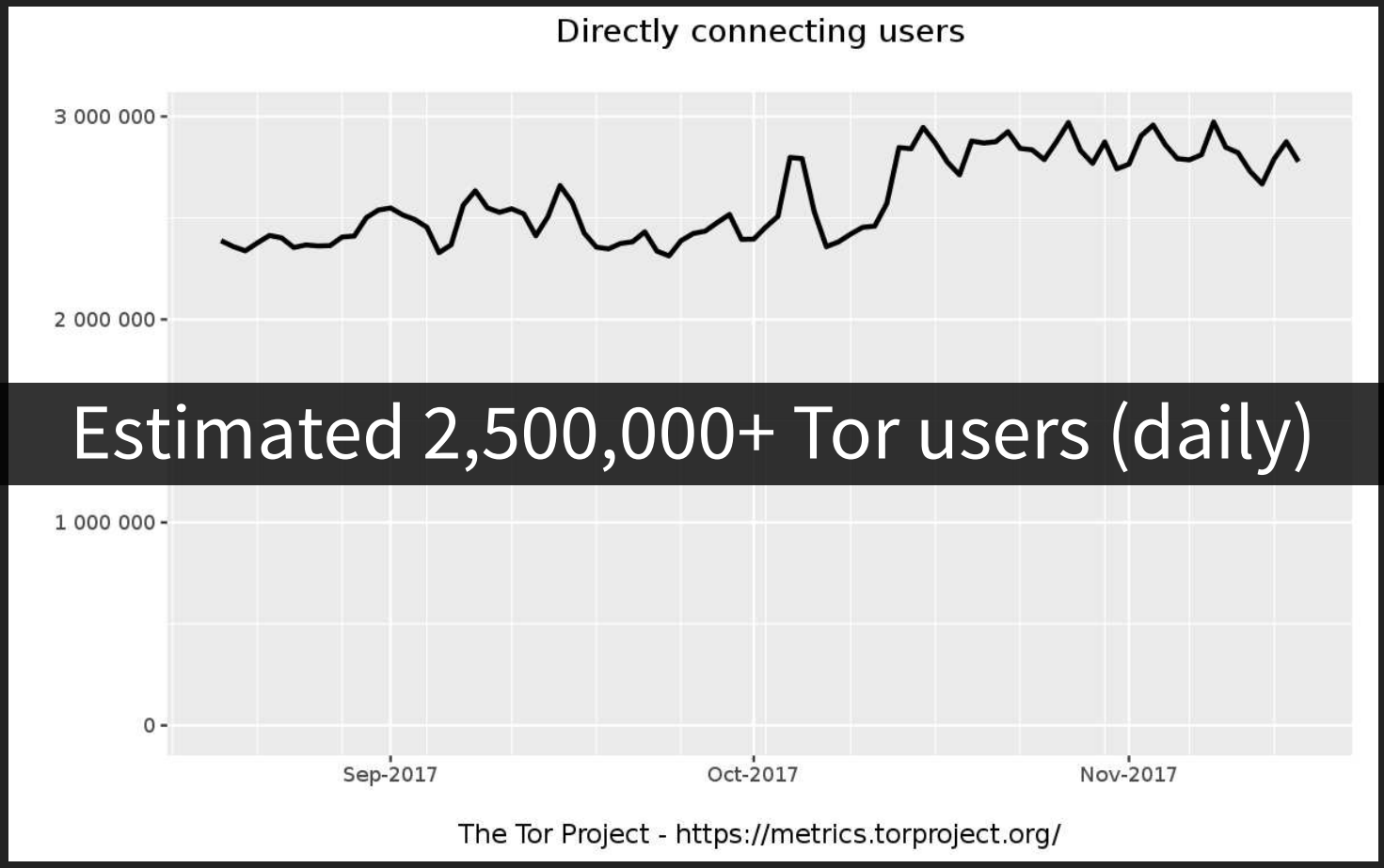
The Tor project

Mission: be the global resource for technology, advocacy, research and education in the ongoing pursuit of freedom of speech, privacy rights online, and censorship circumvention.

What is Tor?

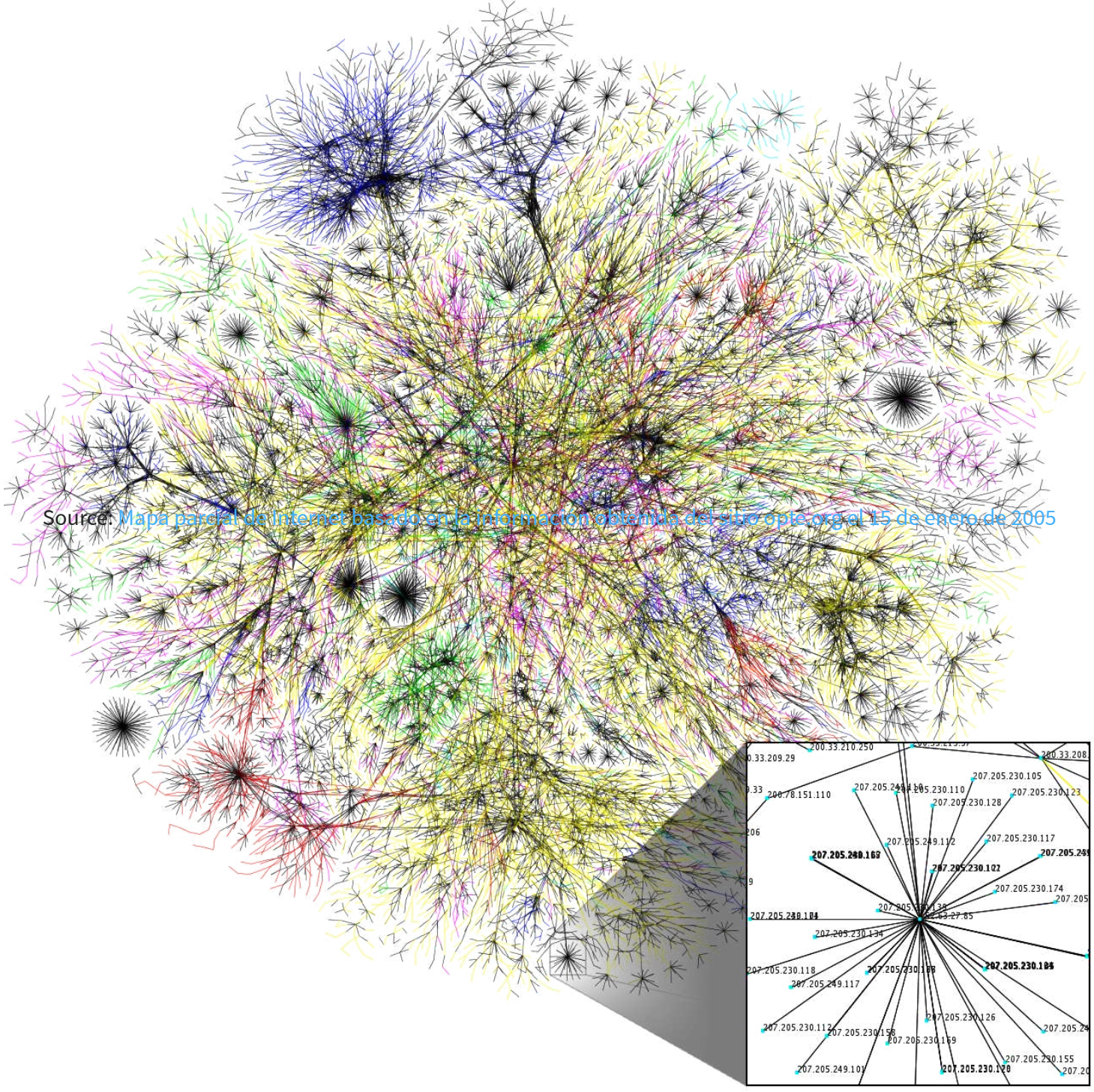
- Online anonymity
  - FL/OSS
  - Open (volunteer based) network
- Community: researchers, developers, users, relay operators, [...]
- U.S. 501(c)(3) non-profit organization


Directly connecting users
3 000 000
2 000 000
1 000 000
0
Sep-2017
Oct-2017
Nov-2017
The Tor Project - https://metrics.torproject.org/

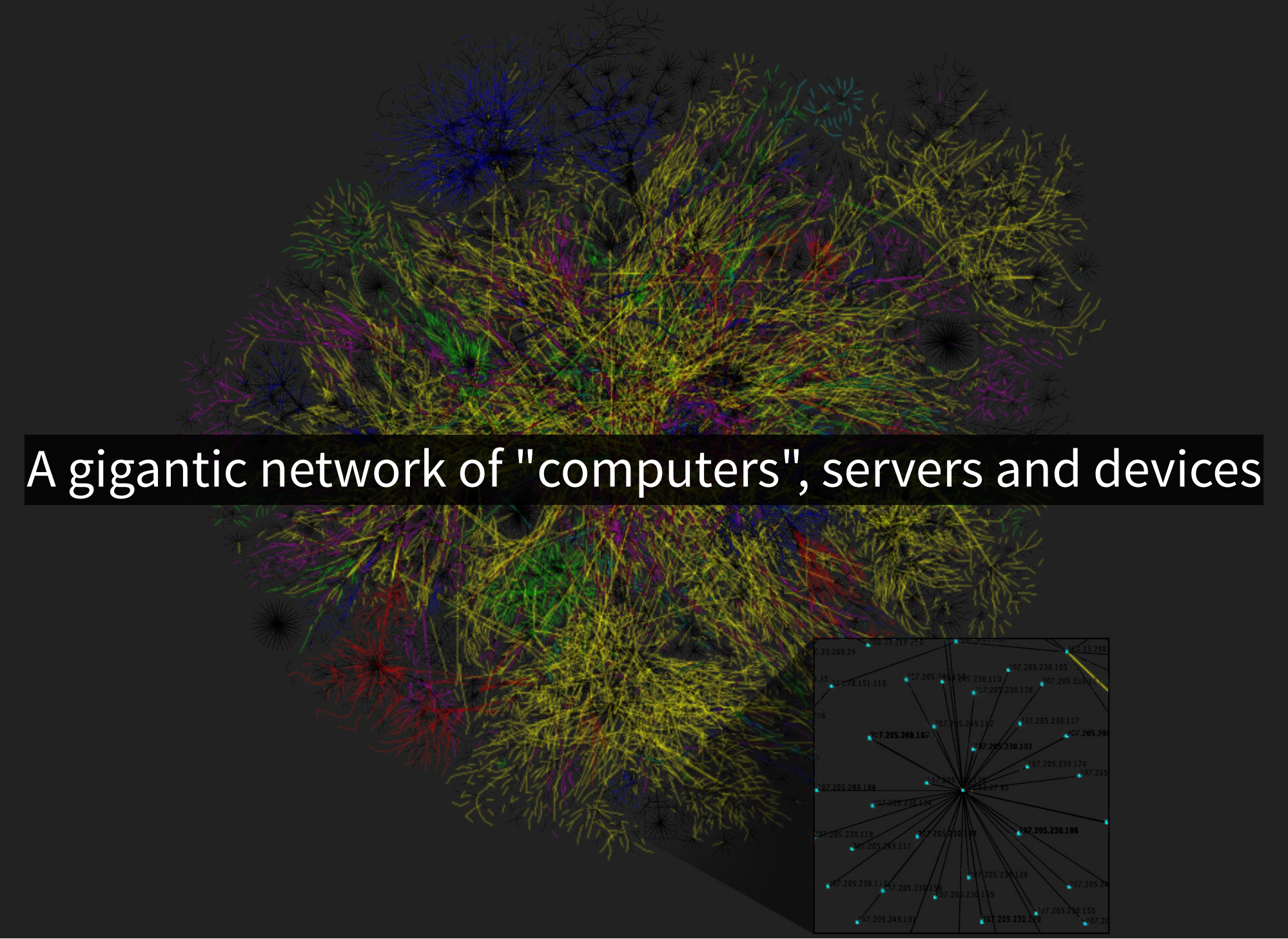


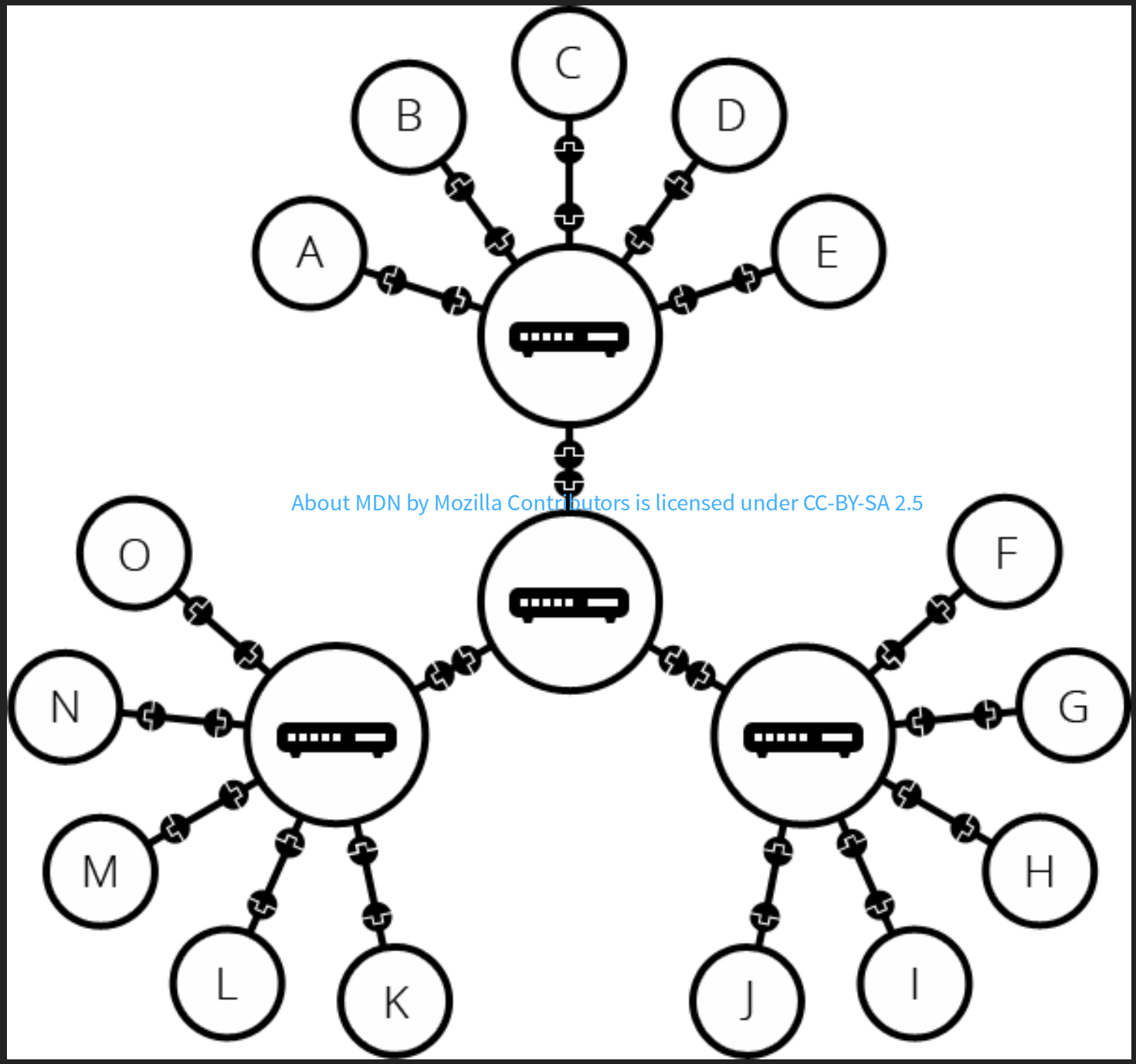
Estimated 2,500,000+ Tor users (daily)

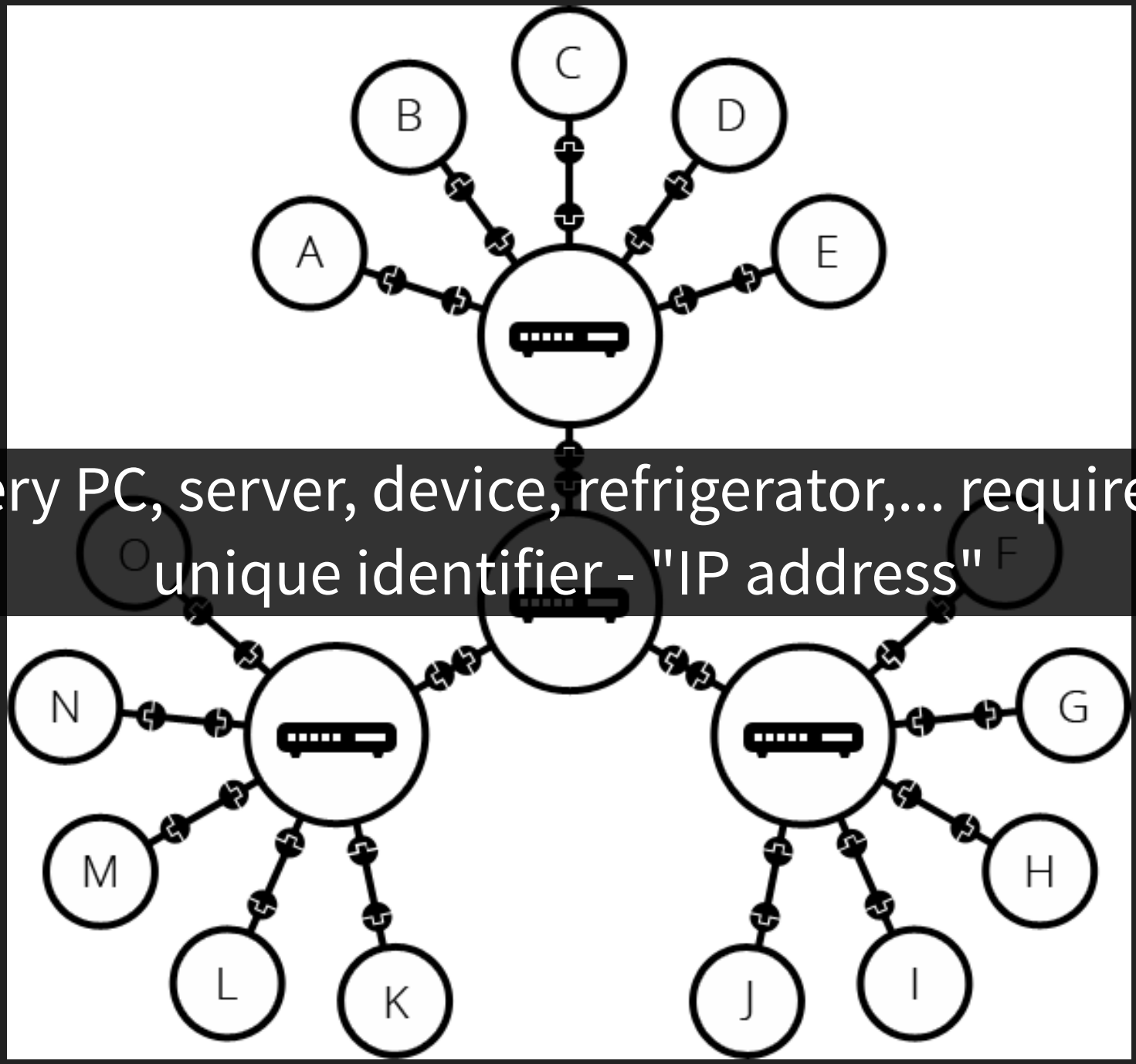
HOW INTERNET WORKS?



Source: Mapa parcial de Internet basado en la información obtenida del sitio opte.org al 15 de enero de 2005

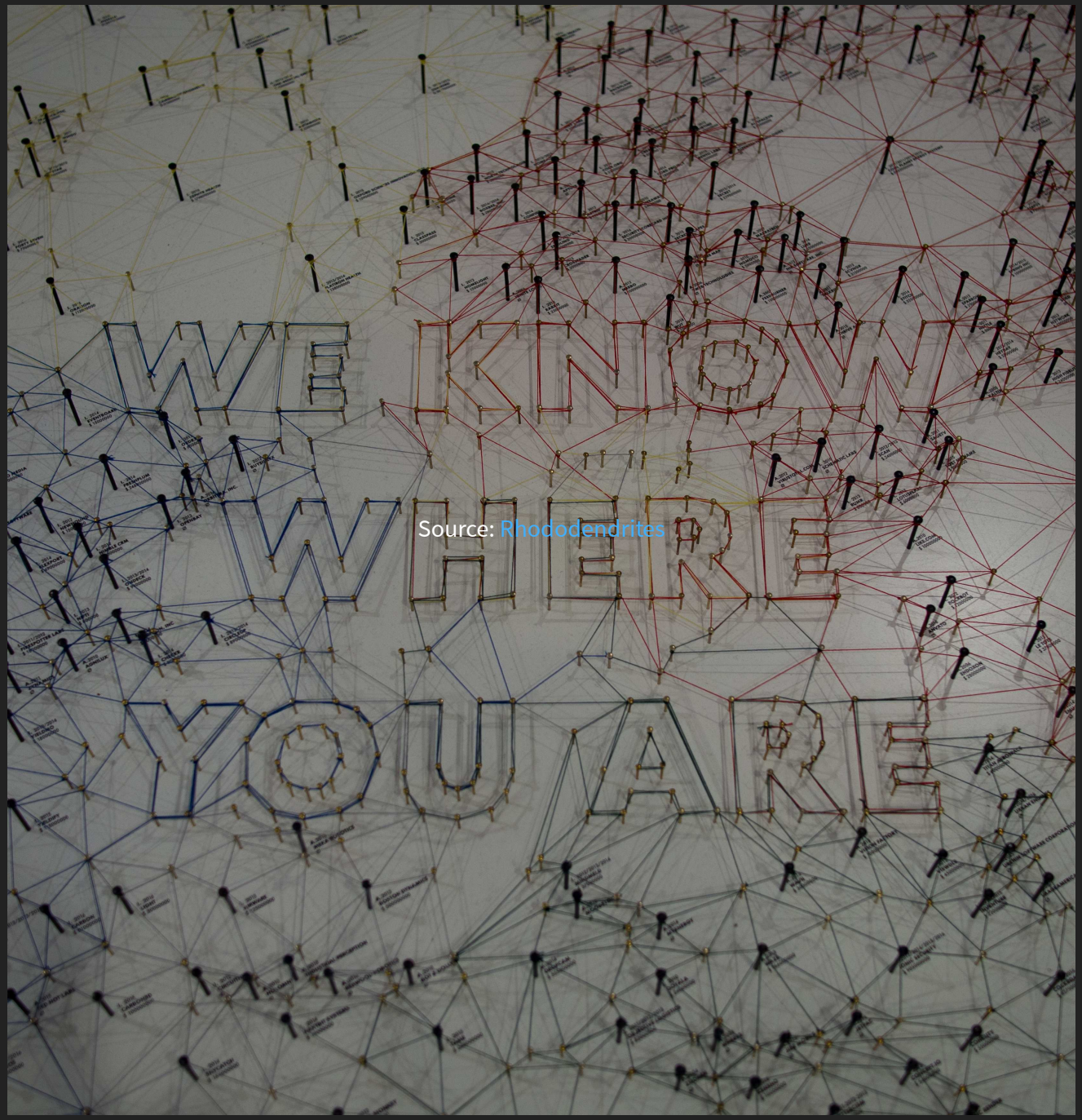

A gigantic network of "computers", servers and devices



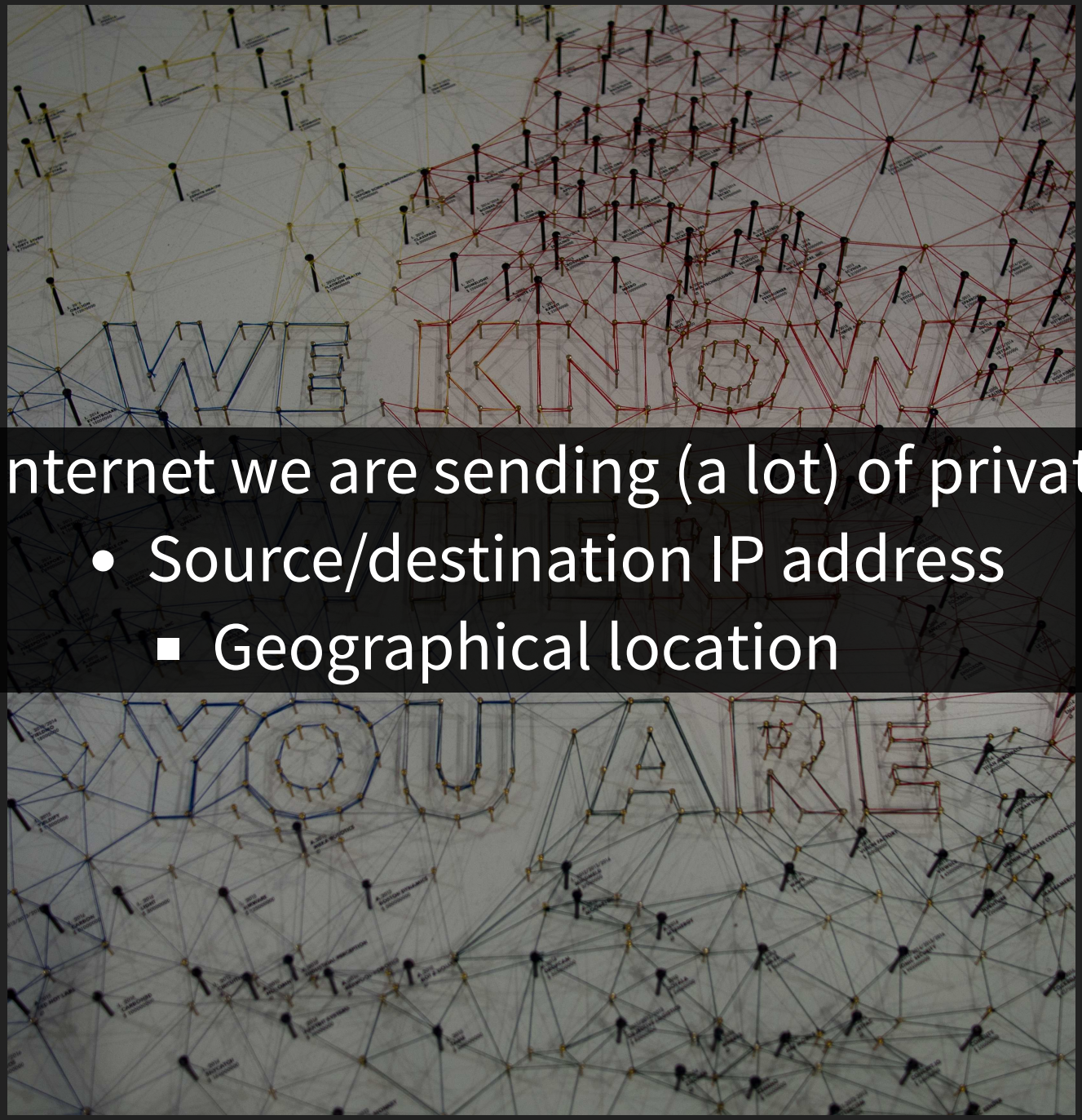


Every PC, server, device, refrigerator,... requires a unique identifier - "IP address"

- Internet is not the WWW (World Wide Web)
- Internet is the infrastructure
- Web is a service of this infrastructure



Source: Rhododendrites



On the Internet we are sending (a lot) of private data:

- Source/destination IP address
  - Geographical location

- WWW (World Wide Web):
  - Web Browser
  - Operating system
  - Addons/Extensions


urce: Eggib

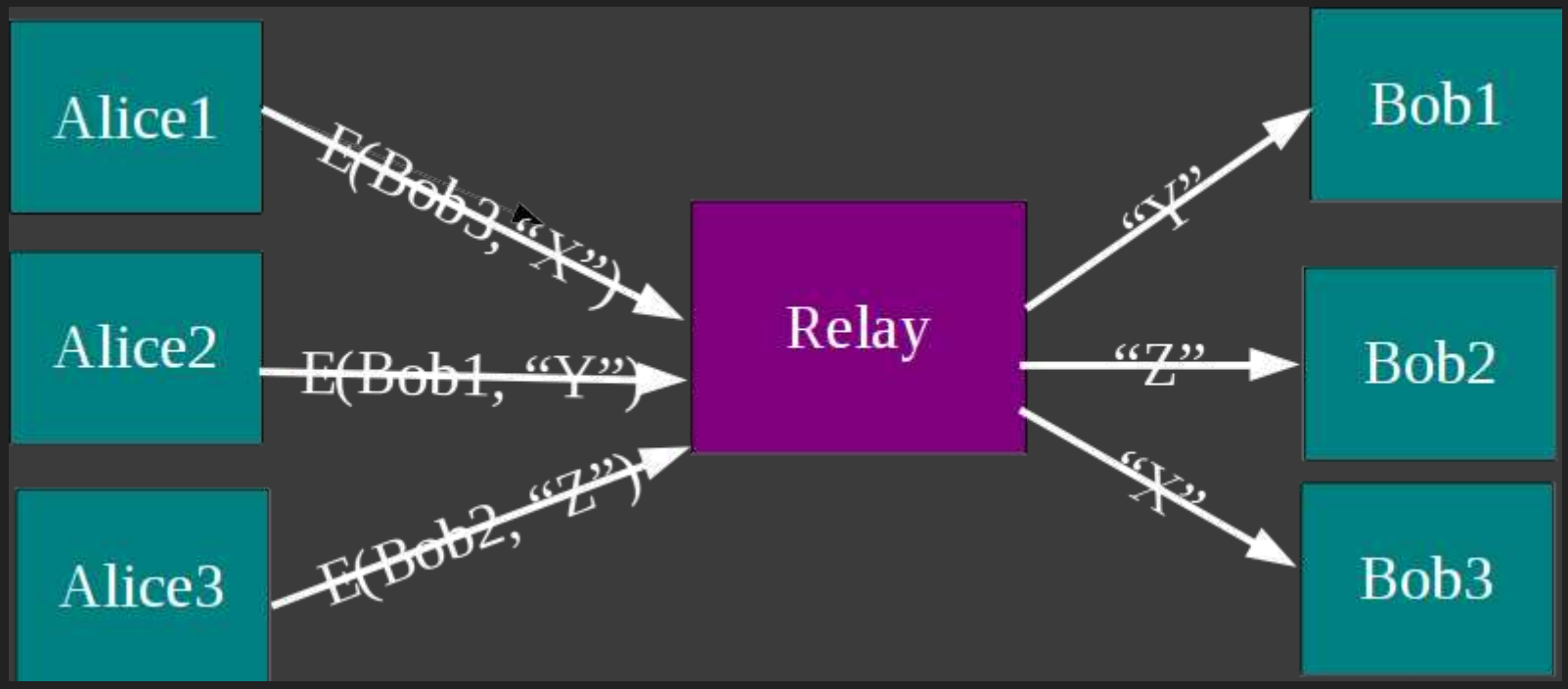
Other services: e-mail, telephone, chat (IRC, IM), file sharing,...

UNDERSTANDING YOUR THREAD MODEL:

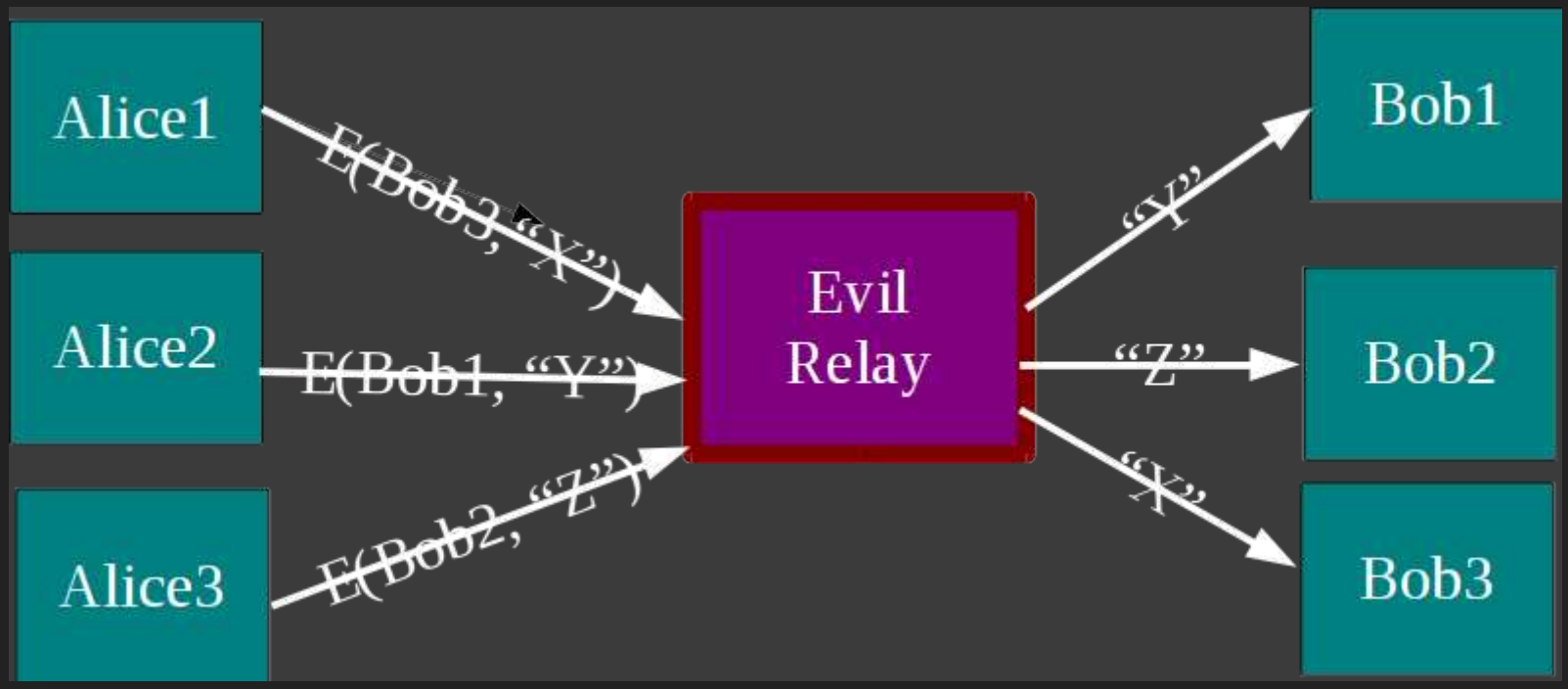
I use encryption (HTTPS, ...) my ISP cannot see my traffic! Maybe it cannot see your traffic (in cleartext), *but* it tracks:

- Websites visited
- Locations logs
- IP address logs
- ..archived for x time: Data retention

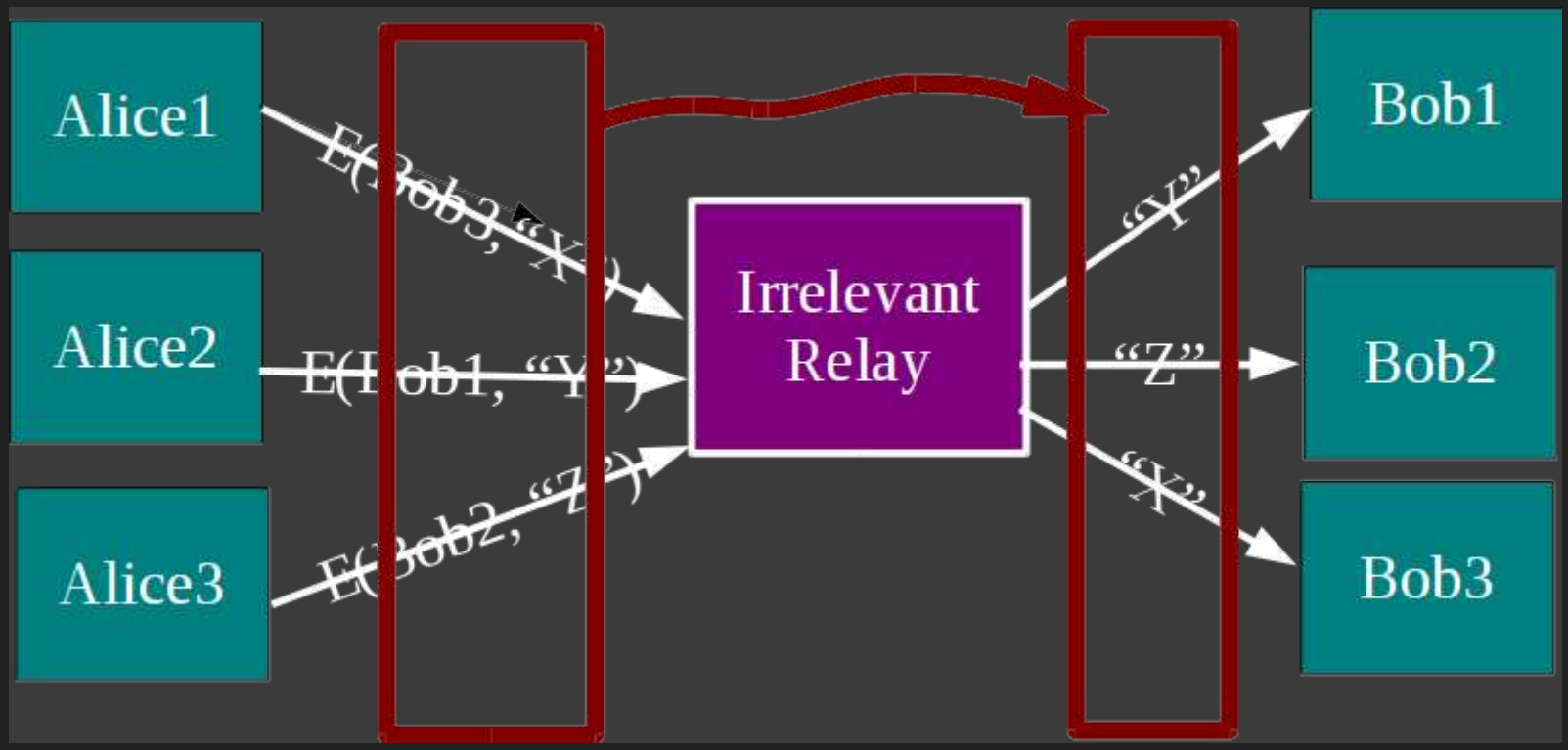
VPN / Proxy Providers



VPN / Proxy Providers: (often) single point of failure

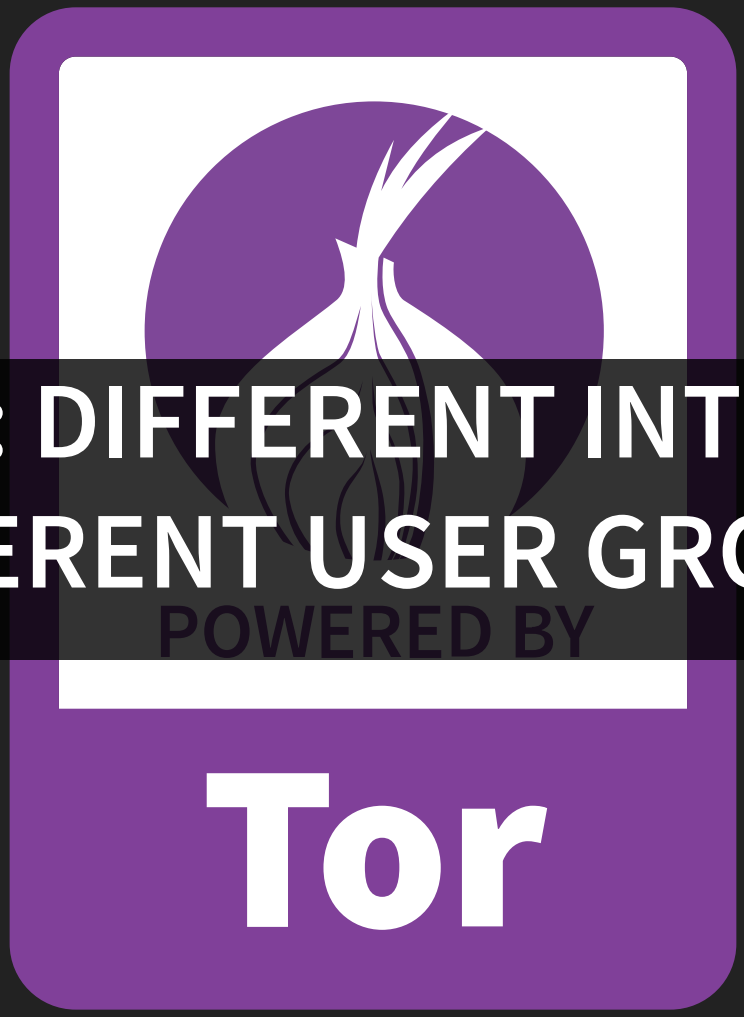


VPN / Proxy Providers: (often) single point of bypass

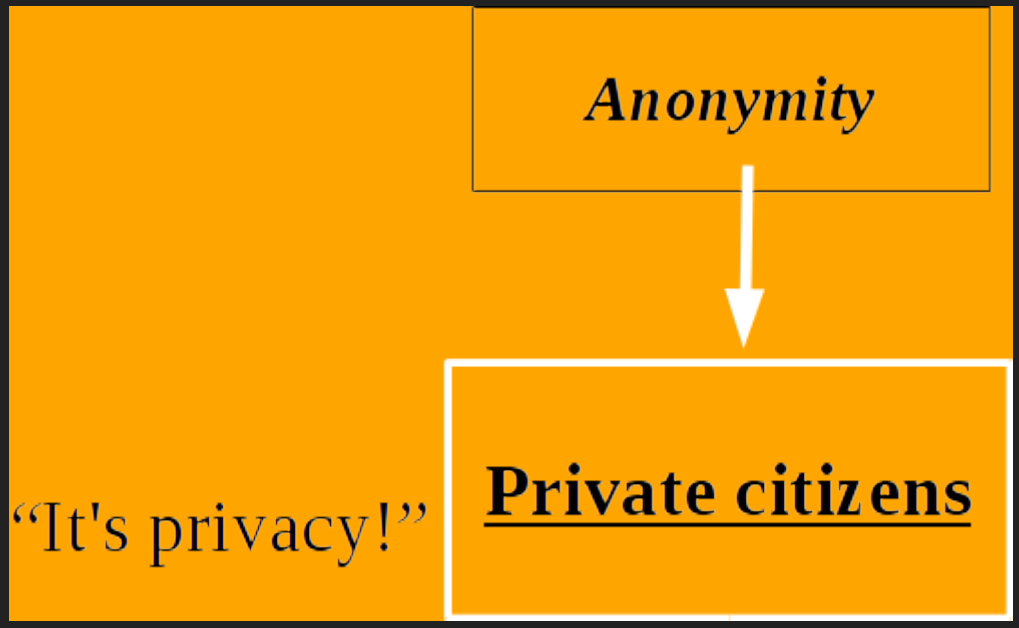



POWERED BY
Tor

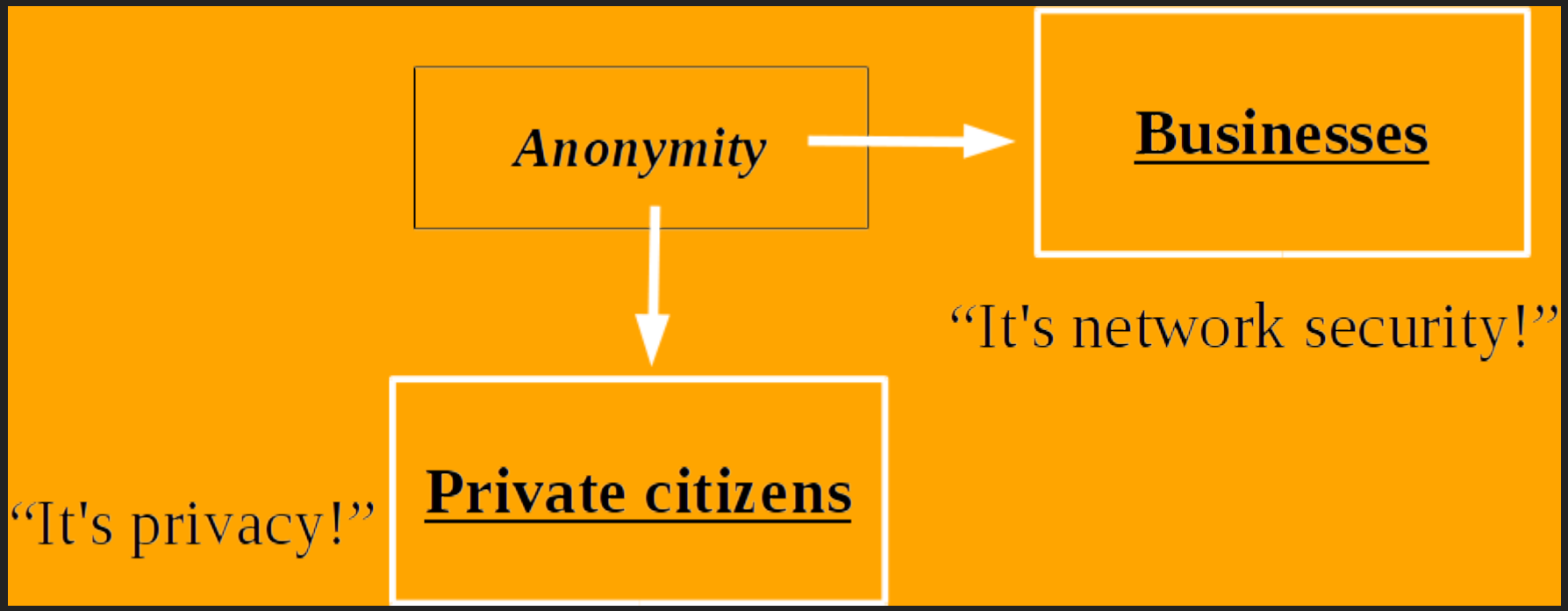
ANONYMITY: DIFFERENT INTERESTS FOR DIFFERENT USER GROUPS



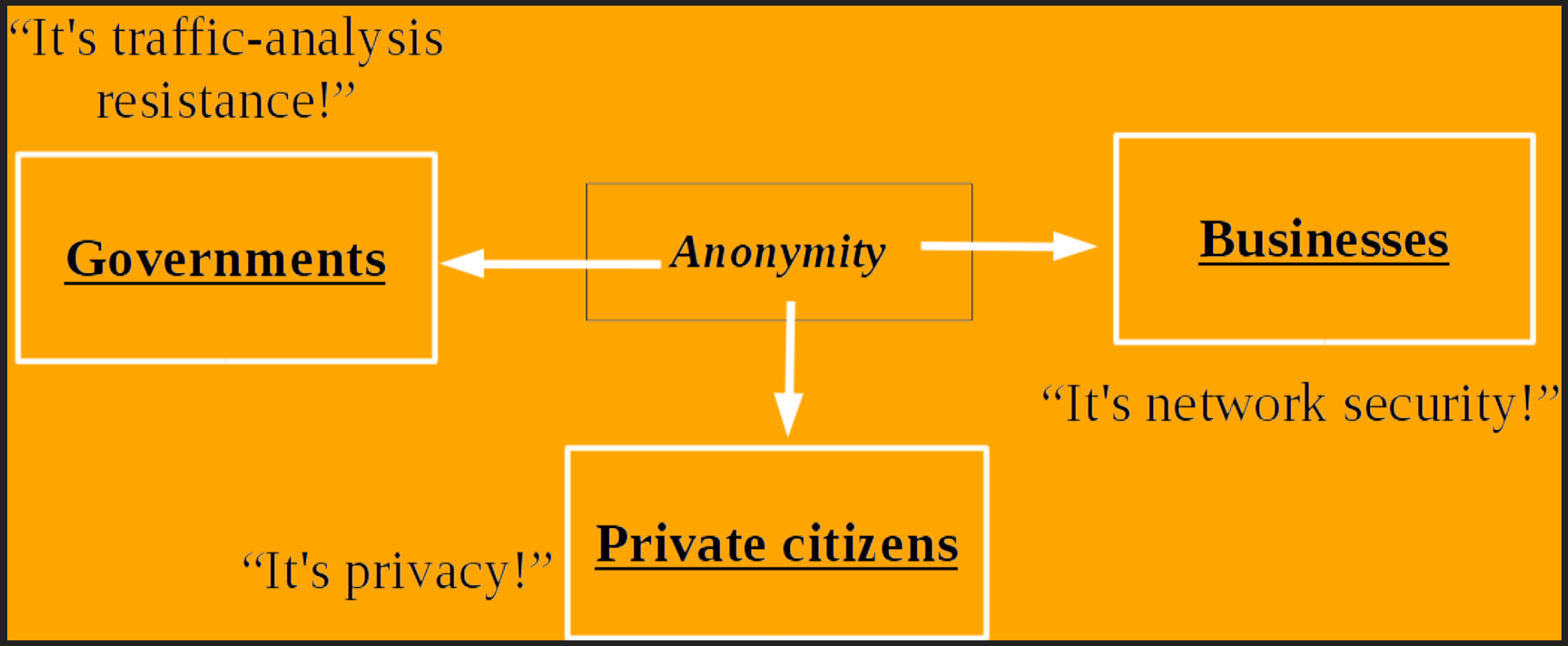
ANONYMITY: DIFFERENT INTERESTS FOR DIFFERENT USER GROUPS



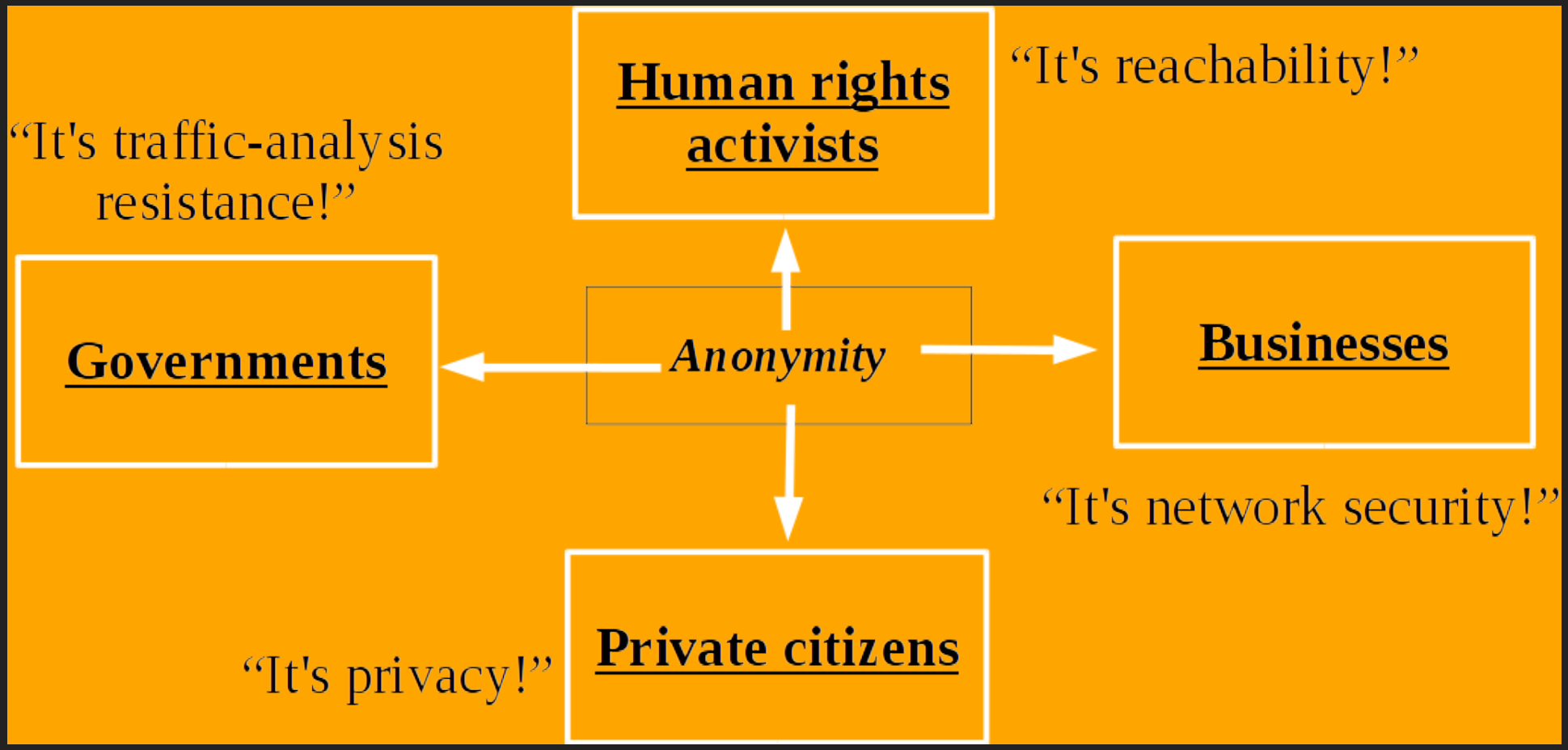
ANONYMITY: DIFFERENT INTERESTS FOR DIFFERENT USER GROUPS

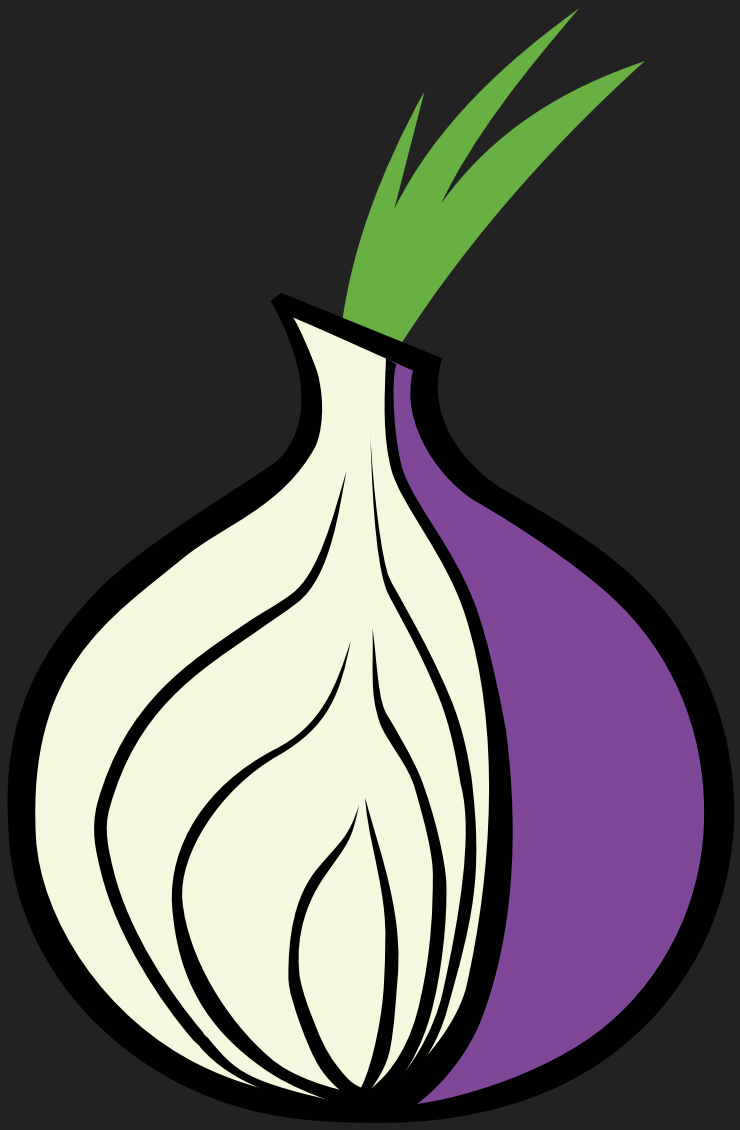


ANONYMITY: DIFFERENT INTERESTS FOR DIFFERENT USER GROUPS

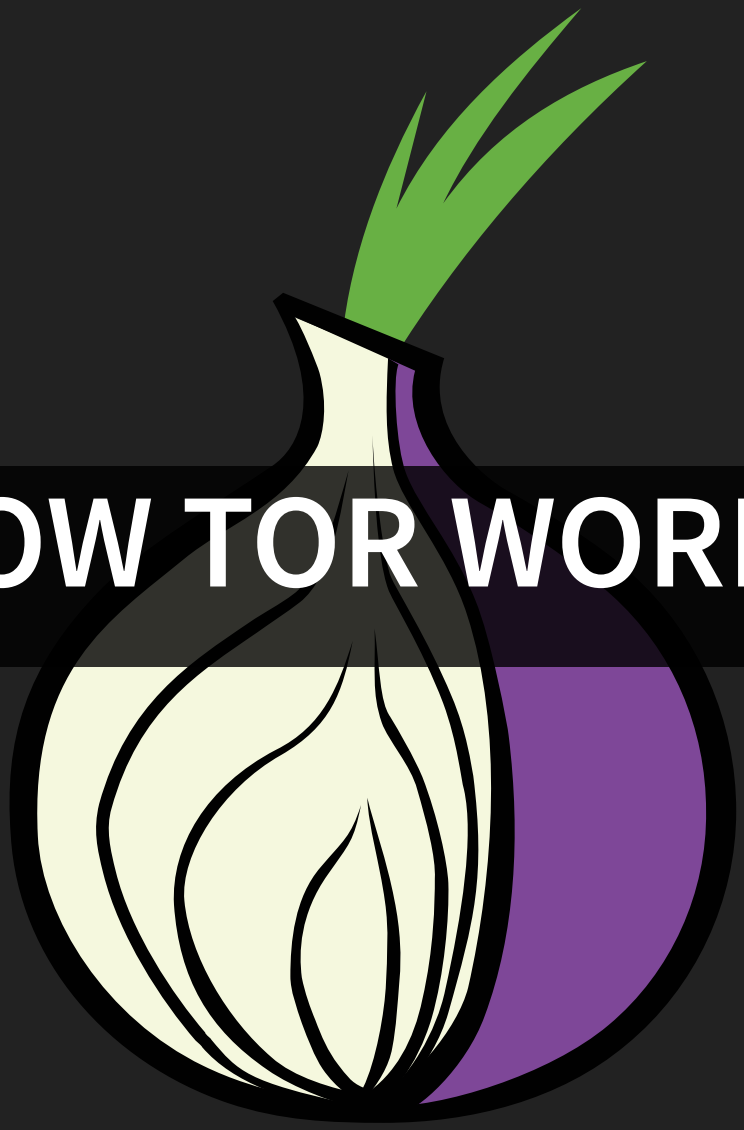


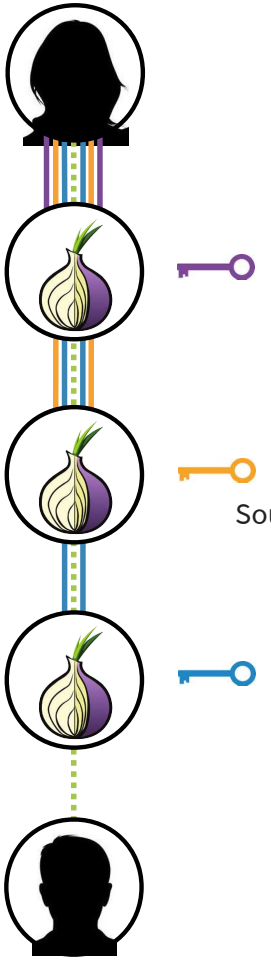
ANONYMITY: DIFFERENT INTERESTS FOR DIFFERENT USER GROUPS





HOW TOR WORKS





A Alice criptografa o seu pedido online para o Bob três vezes, e envia-o para o primeiro servidor

O primeiro servidor remove a primeira camada de criptografia, mas não vê consegue saber que o pedido é dirigido ao Bob.

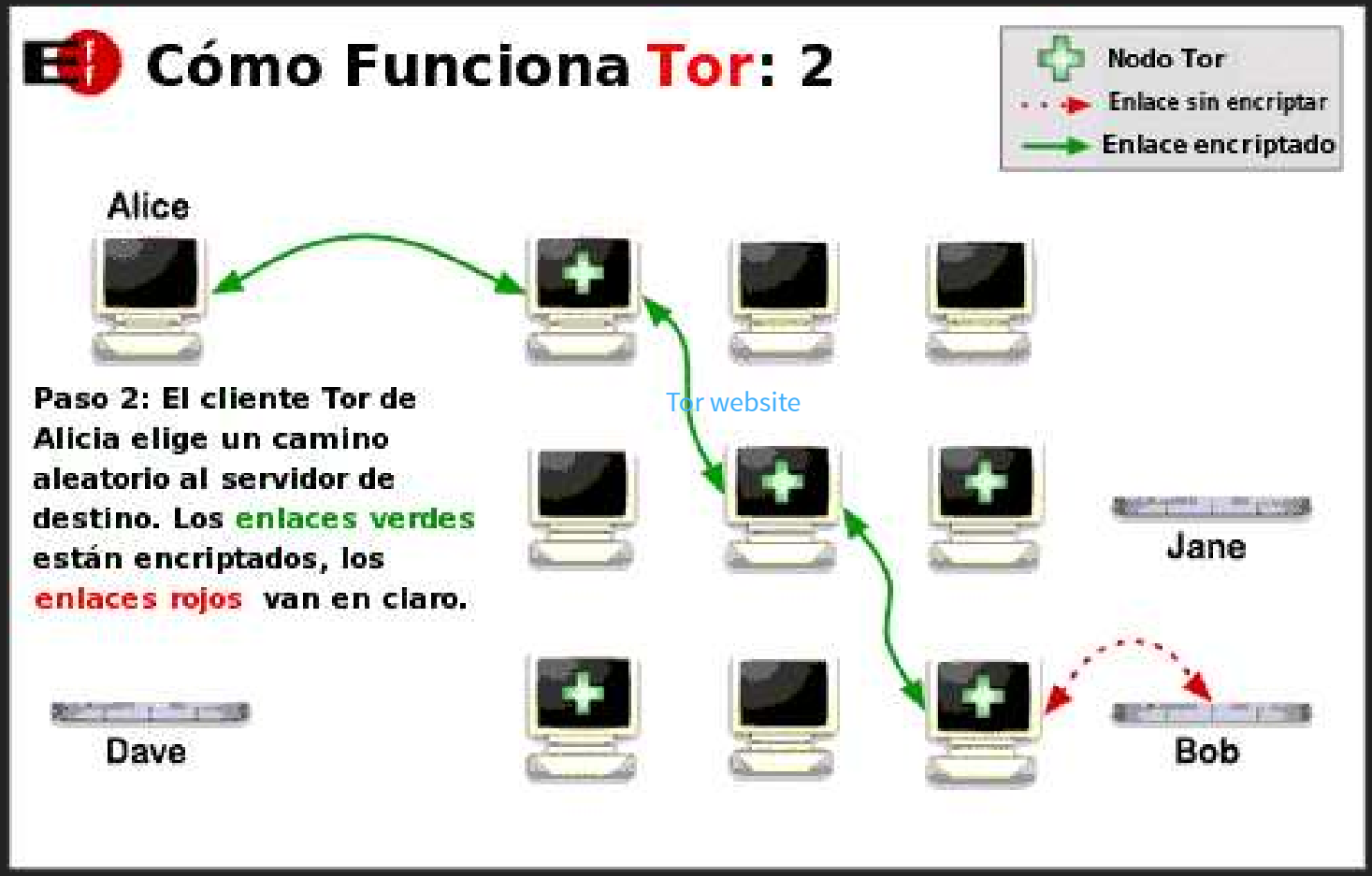
O segundo servidor remove outra camada de criptografia e reencaminha o pedido.

Source: Tor brochure

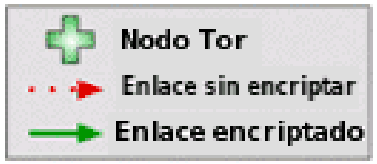
O terceiro servidor remove a última camada de criptografia e entrega o pedido ao Bob, mas não consegue saber que o pedido veio da Alice.

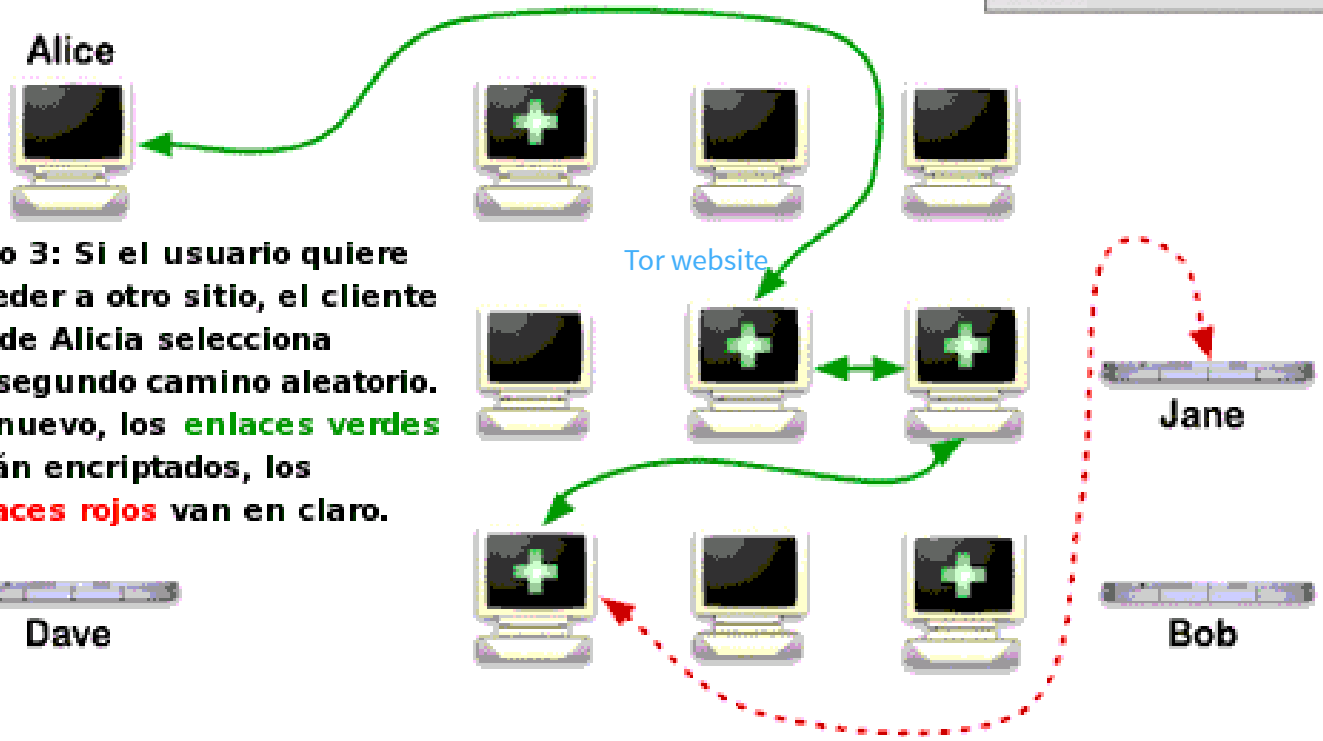
O Bob não sabe que o pedido online foi feito pela Alice, a menos que ela mesma o diga.


Cómo Funciona Tor: 1
Nodo Tor
Enlace sin encriptar
Enlace encriptado
Alice
Paso 1: El cliente Tor de Alicia obtiene una lista de nodos Tor desde un servidor de directorio
Tor website
Jane
Dave
Bob

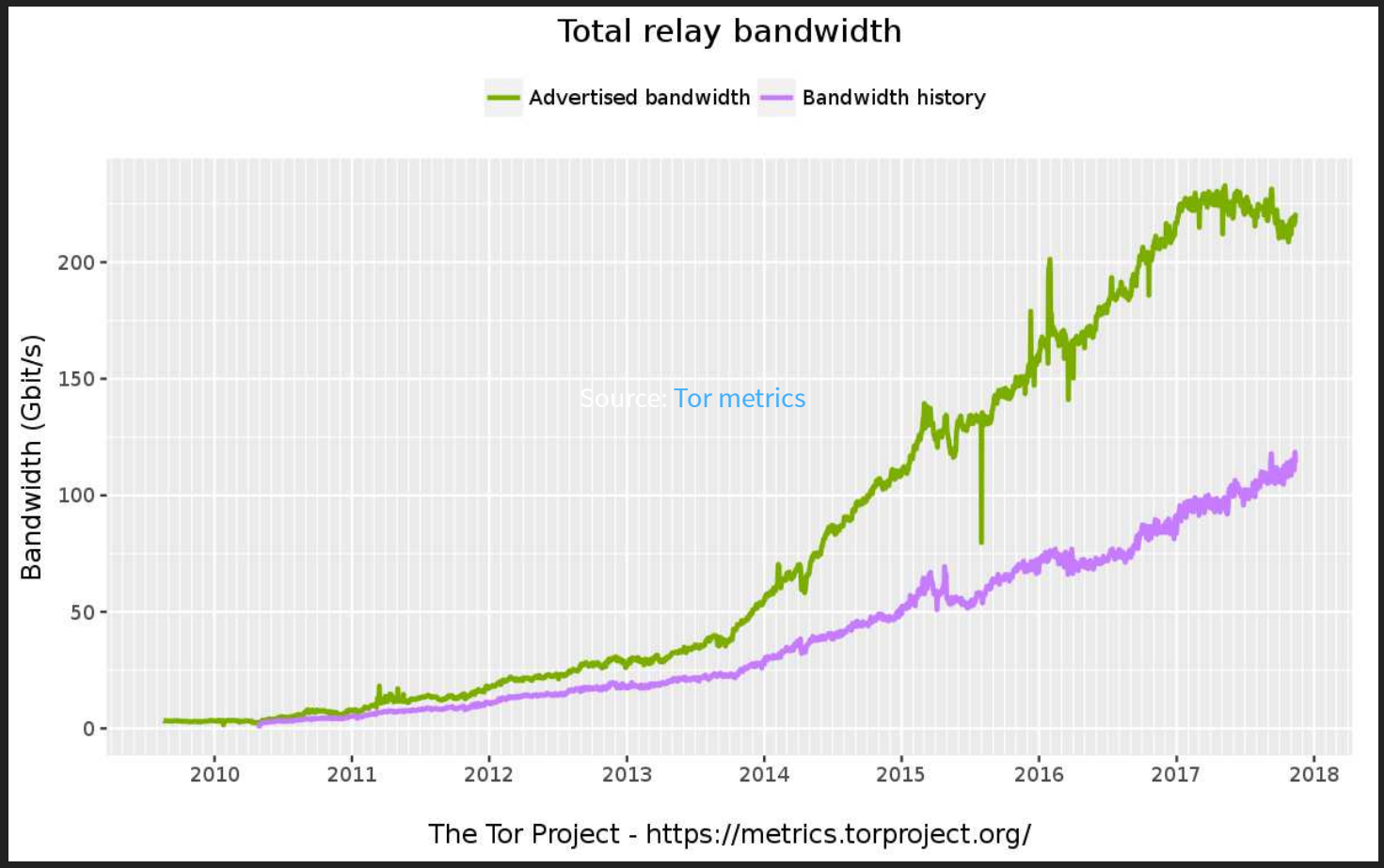

Cómo Funciona Tor: 2
Nodo Tor
Enlace sin encriptar
Enlace encriptado
Alice
Paso 2: El cliente Tor de Alicia elige un camino aleatorio al servidor de destino. Los enlaces verdes están encriptados, los enlaces rojos van en claro.
Tor website
Jane
Dave
Bob

Cómo Funciona Tor: 3





Paso 3: Si el usuario quiere acceder a otro sitio, el cliente Tor de Alicia selecciona un segundo camino aleatorio. De nuevo, los enlaces verdes están encriptados, los enlaces rojos van en claro.


Total relay bandwidth
Advertised bandwidth
Bandwidth history
Bandwidth (Gbit/s)
200
150
100
50
0
2010
2011
2012
2013
2014
2015
2016
2017
2018
Source: Tor metrics
The Tor Project - https://metrics.torproject.org/

Tor's safety comes from diversity

- Diversity of relays
- Diversity of users

Transparency for Tor is key

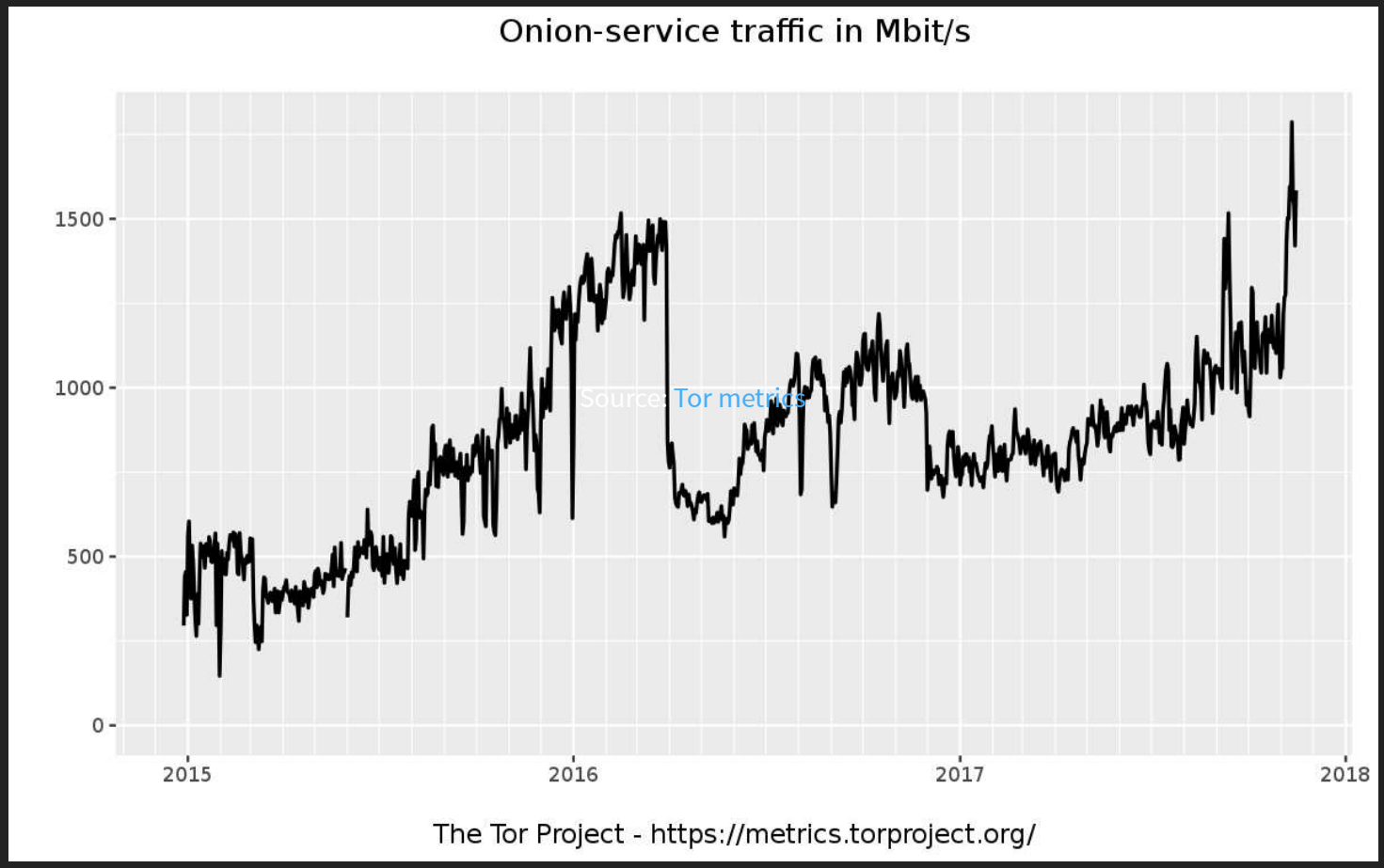
- FL/OSS
- Public design documents and specifications

But what about the bad people?

- (remember) the millions of daily users
- Still a two-edged sword?
- Good people need Tor much more than bad people need it

Onion services

- Self authenticated
- End-to-end encrypted
- Built-in NAT punching
- Limit surface area
- No need to “exit” from Tor


Onion-service traffic in Mbit/s
1500
1000
500
0
2015
2016
2017
2018
Source: Tor metrics
The Tor Project - https://metrics.torproject.org/

- About 3% of Tor's traffic has to do with onion services at all
- Onion services are still in the "neat toy" stage
- Terbium labs (and others) found ~7000 useful onion sites


World Wide Web
Deep Web
Dark Web

Facebook - Log In or Si...

Facebook, Inc. (US) | https://www.facebookcorewwwi.onion/?_rdr

1 Million People use Facebook over Tor

FACEBOOK OVER TOR · FRIDAY, APRIL 22, 2016

People who choose to communicate over Tor do so for a variety of reasons related to privacy, security and safety. As we've written previously it's important to us to provide methods for people to use our services securely – particularly if they lack reliable methods to do so.

This is why in the last two years we built the Facebook onion site and onion-mobile site, helped standardise the ".onion" domain name, and implemented Tor connectivity for our Android mobile app by enabling connections through Orbot.

...

... and many others

Package repository

`http://vwakviie2ienjx6t.onion/`

debian

```
apt-get install apt-tor-transport
```

Ubuntu Desktop

en 6:19 PM Yan

File Edit View History Bookmarks Tools Help

SecureDrop

kzjgrjodst3ie7v2.onion

Startpage

SECUREDROP

Submit documents for the first time

If this is your first time submitting documents to journalists, start here.

SUBMIT DOCUMENTS

Already submitted something?

If you have already submitted documents in the past, login here to check for responses. You will need to know your code name.

CHECK FOR A RESPONSE

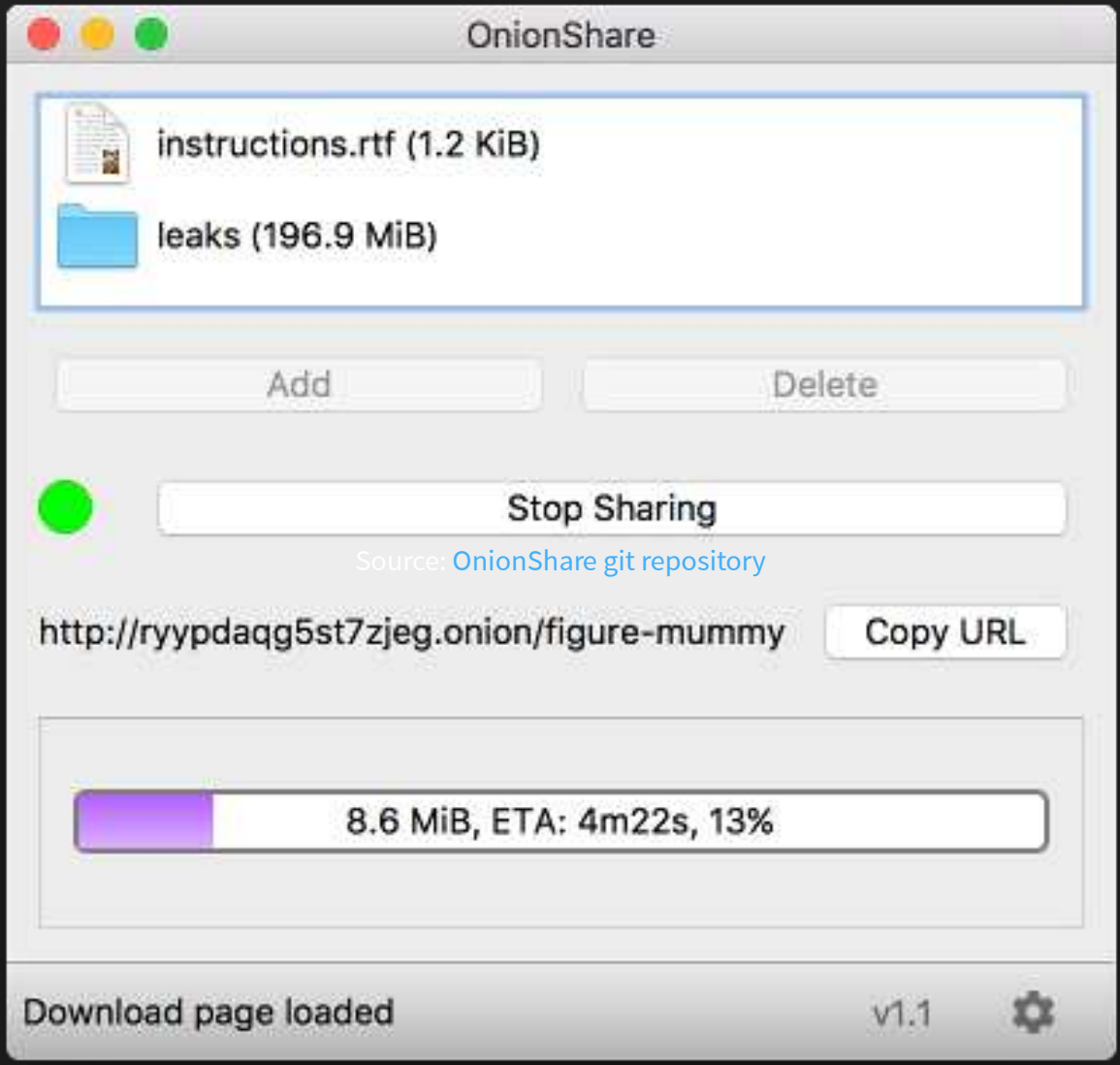
Like all software, SecureDrop may contain security bugs. Use at your own risk.

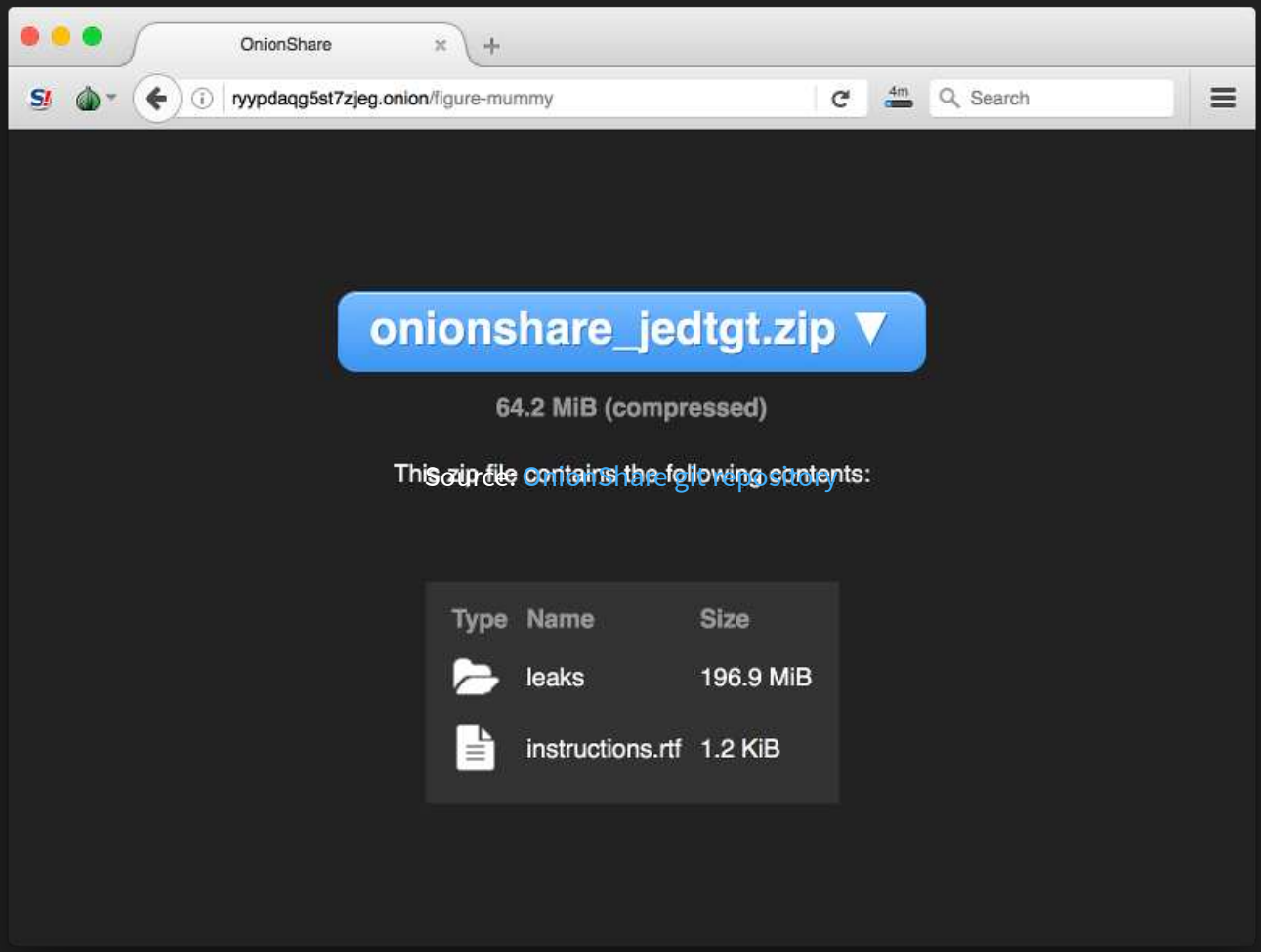
Powered by *SecureDrop 0.2development.*

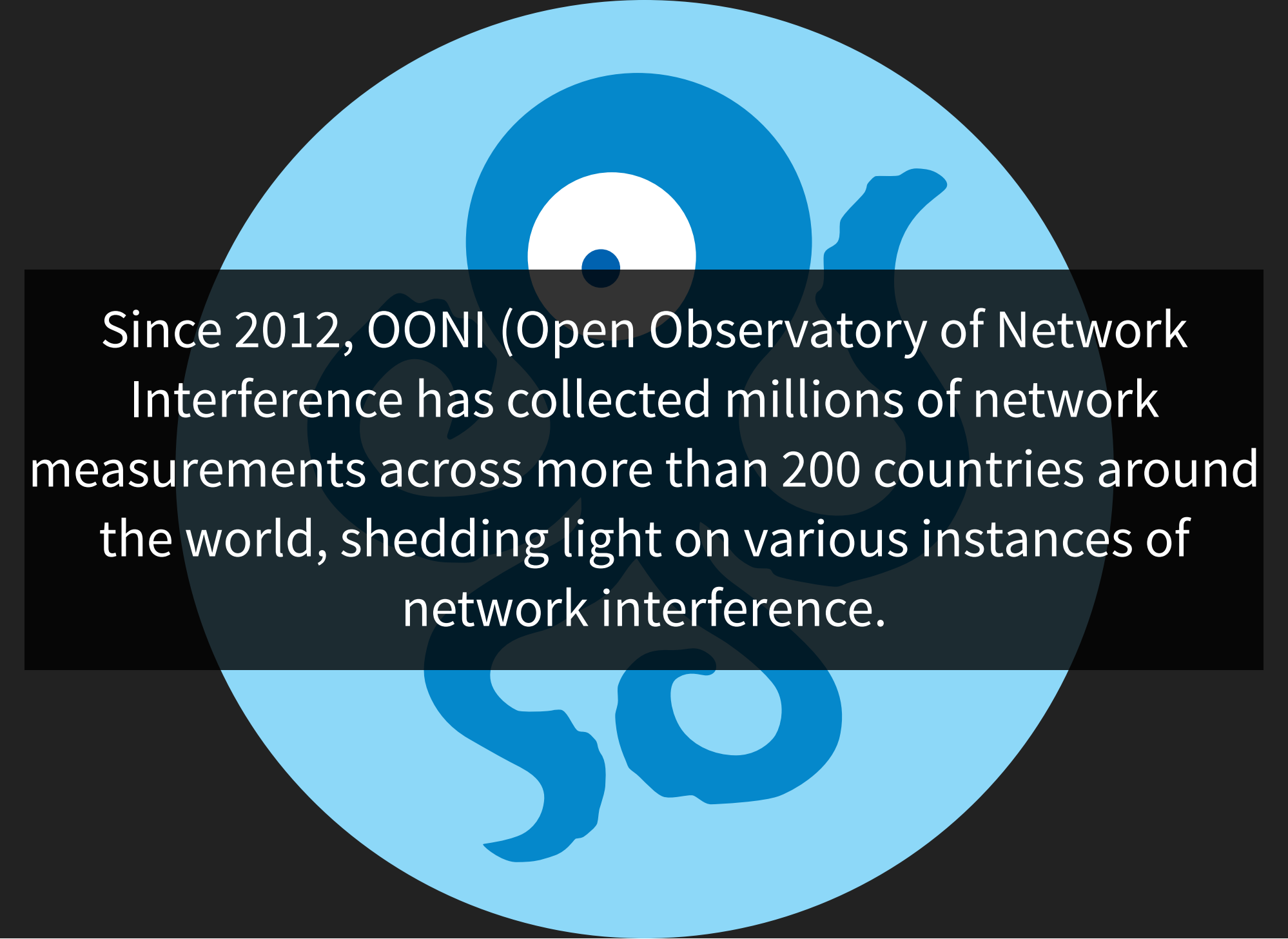
kzjgrjodst3ie7v2.onion/generate

Cpu: 5% | Mem: 77% * Swap: 11% | eth0: 0.0KB|0.0KB Reims: 39F | Sun Dec 01 2013 18:19:32

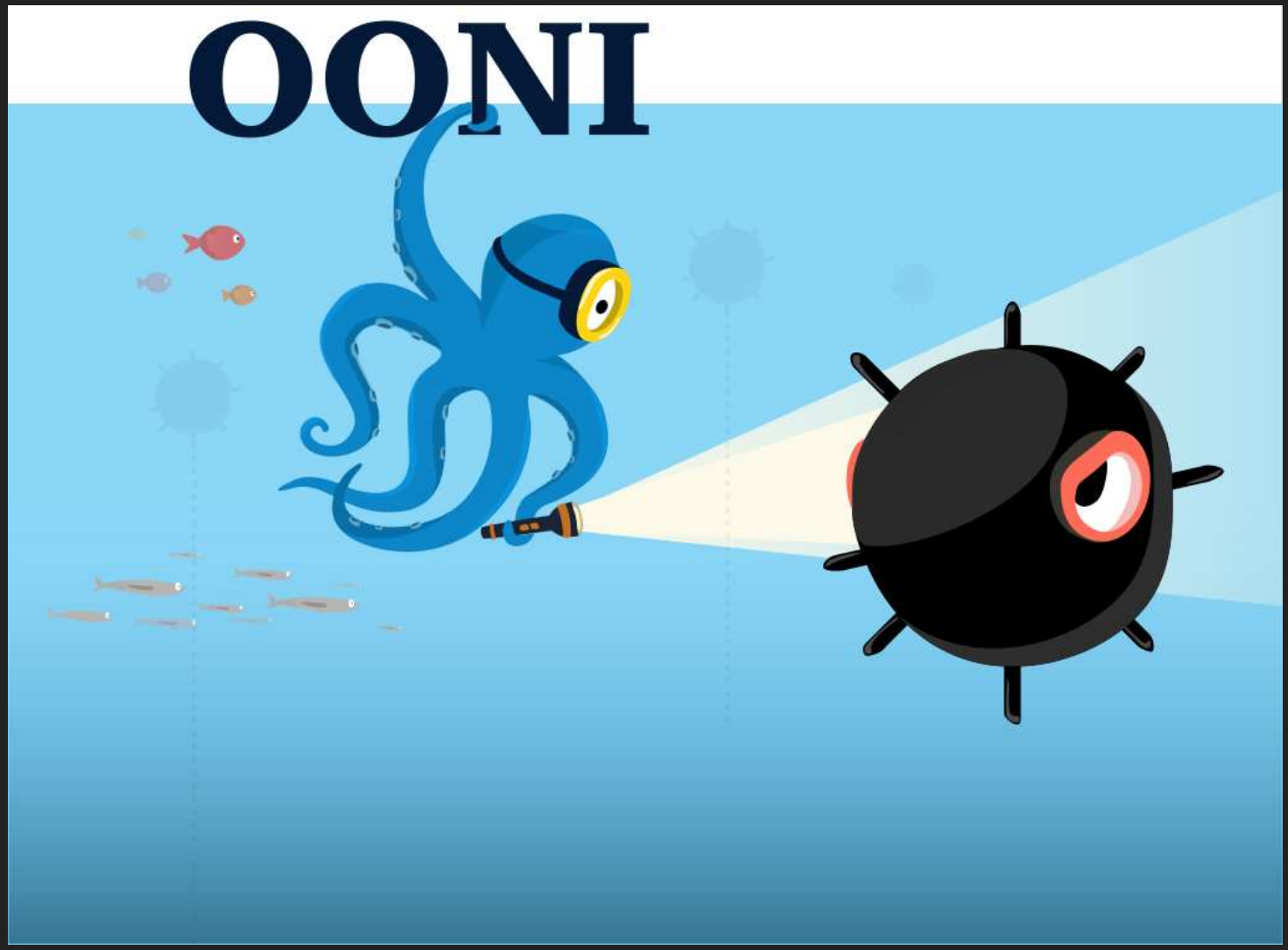

Ricochet
En ligne
CONNECTÉ
Lecteur 1
1
REQUÊTES
John Brooks
Lecteur 1
Lecteur 1
25/05/2015 10:56
Salut !
Salut Korben !
ça fonctionne, c'est cool. A qui ai je l'honneur ?
Oui, c'est cool. Je suis un lecteur de ton site, Paul.
enchanté !
j'ai commenté qu'une fois un article sur Mario64 porté sur plateforme x86


OnionShare
instructions.rtf (1.2 KiB)
leaks (196.9 MiB)
Add
Delete
Stop Sharing
Source: OnionShare git repository
http://ryypdaqg5st7zjeg.onion/figure-mummy
Copy URL
8.6 MiB, ETA: 4m22s, 13%
Download page loaded
v1.1


OnionShare
ryypdaqg5st7zjeg.onion/figure-mummy
Search
onionshare_jedtgt.zip
64.2 MiB (compressed)
This zip file contains the following contents:
Source: onionshare.gitrepo.story
Type Name Size
leaks 196.9 MiB
instructions.rtf 1.2 KiB



Since 2012, OONI (Open Observatory of Network Interference has collected millions of network measurements across more than 200 countries around the world, shedding light on various instances of network interference.


OONI

WHAT IS OONI ?

Detect censorship and signs of network tampering

Shares observations and data about the nature, methods, and prevalence of censorship and network tampering around the world, through the use of open methodologies and FLOSS tools

OPEN DATA MODEL

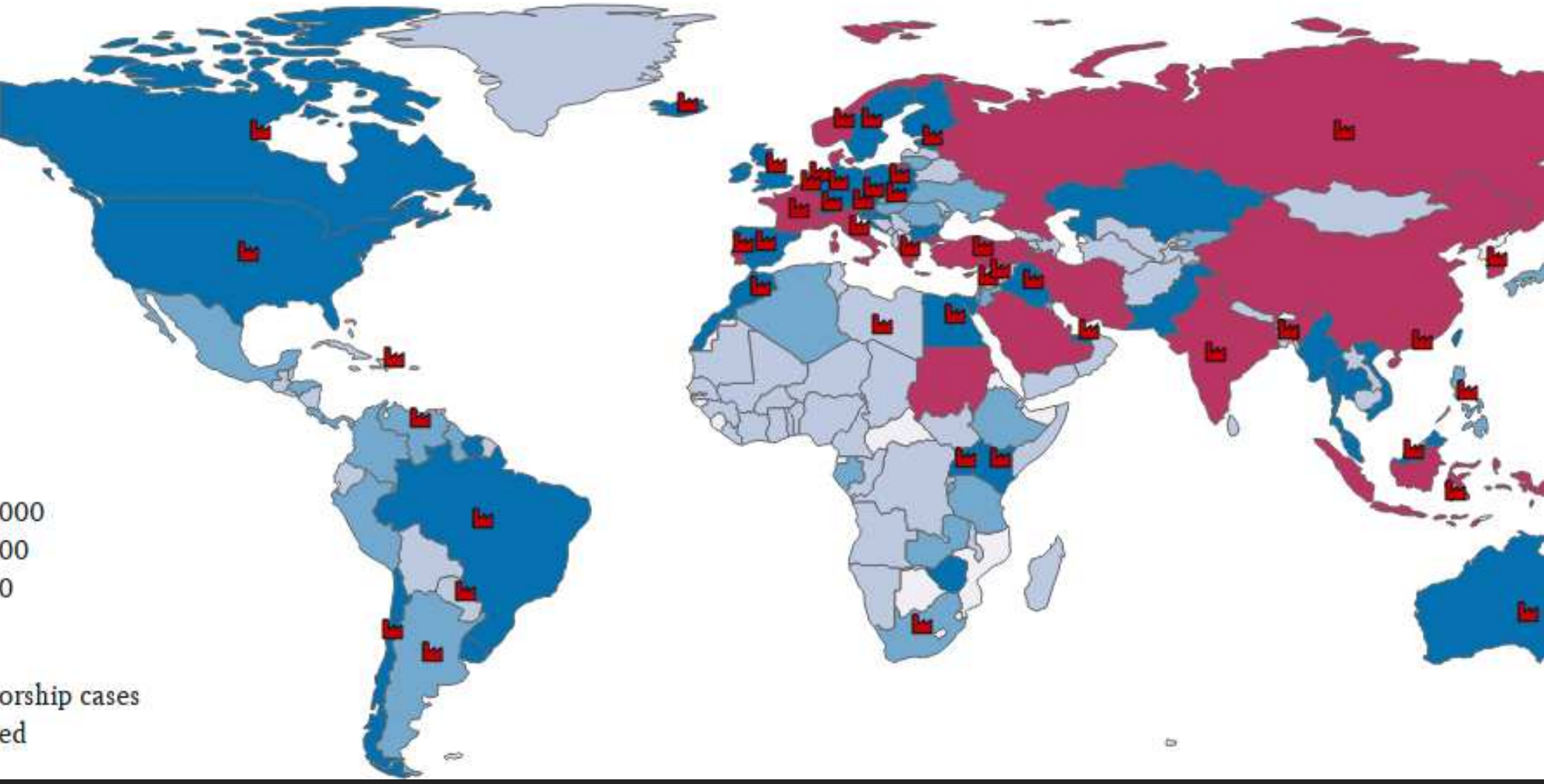
- Network measurement data (reports) submitted by volunteers
- Complete dataset (from 2012) available to use/download

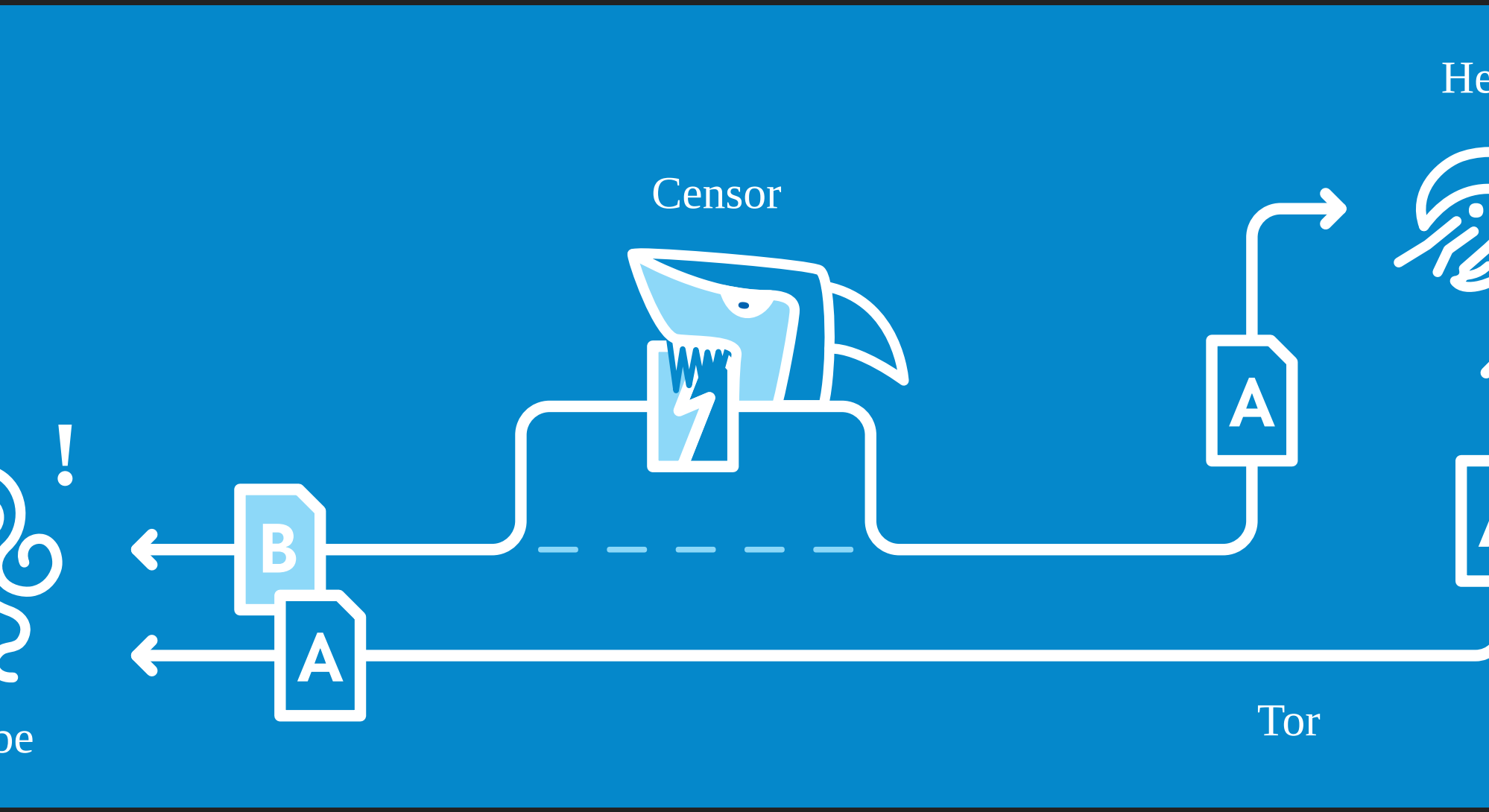
EVIDENCE OF INTERNET CENSORSHIP

- Transparency: What is blocked, where and how? What is the *health* of the network that we are using?
- Legality: Can the blocking of specific types of sites and services be legally justified?
- Story-telling & Advocacy: What is the impact of censorship on human rights?

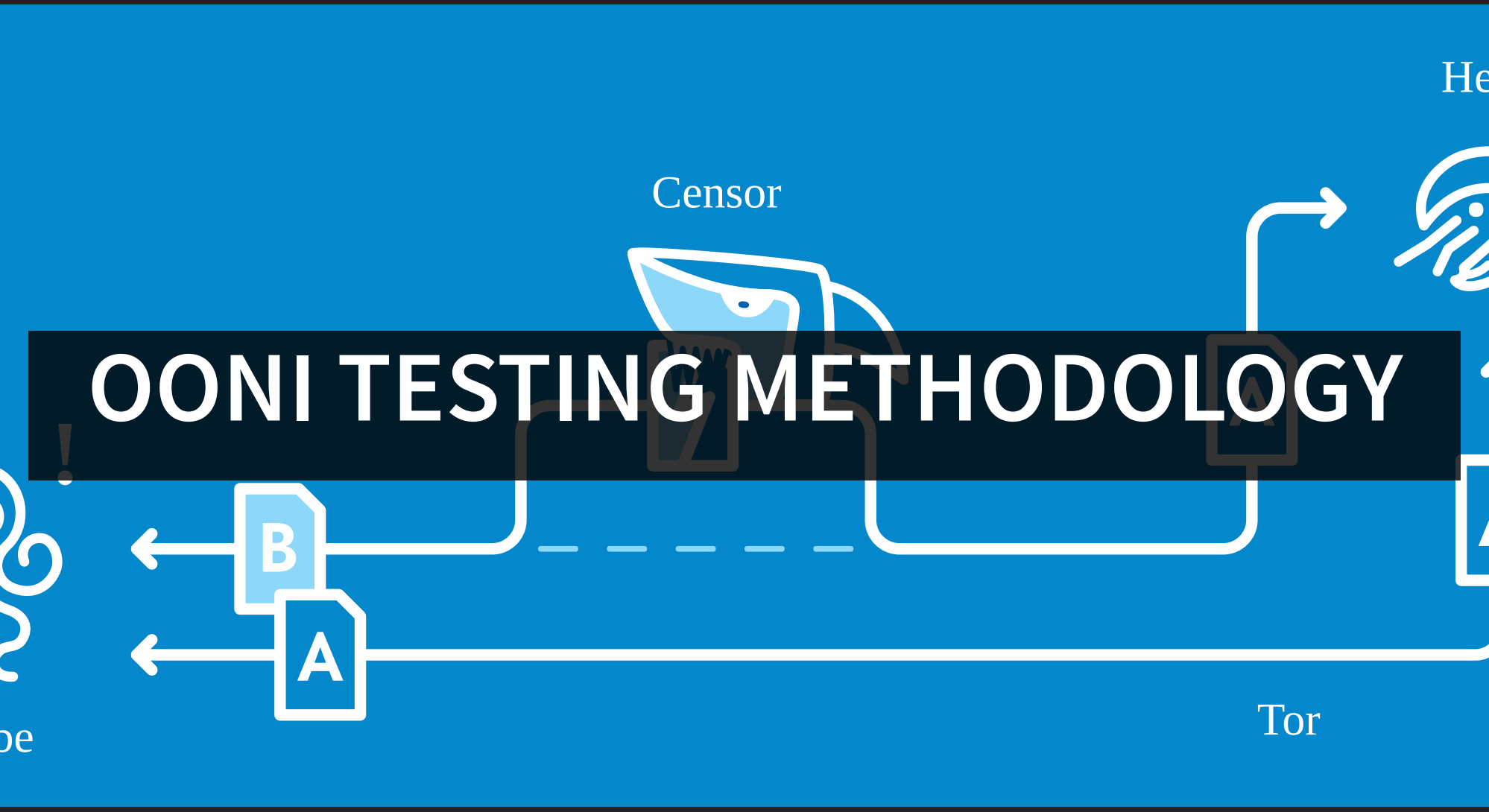
DATA REPRESENTATION

OONI explorer

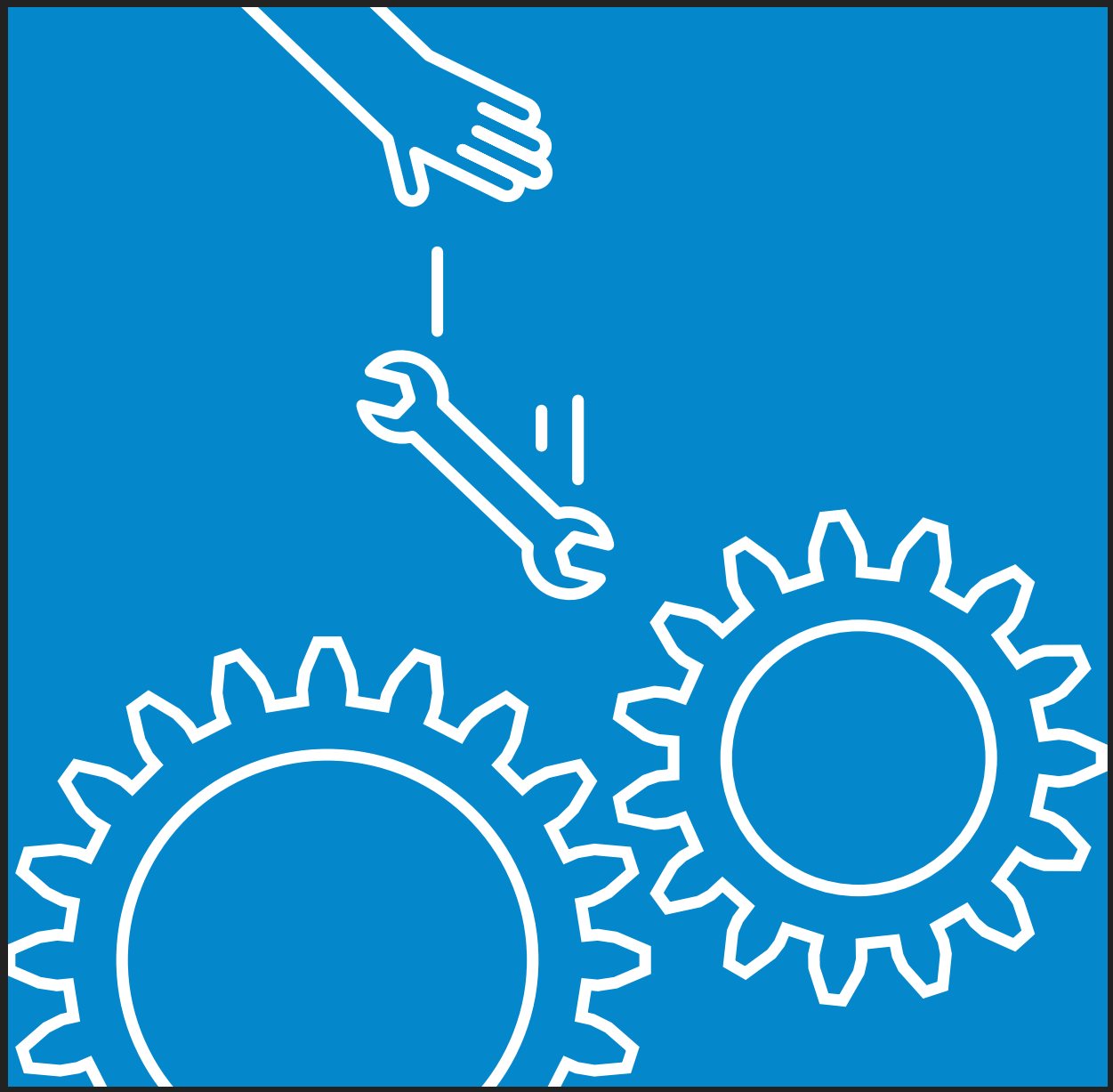

000
00
0
orship cases
ed


He
Censor
!
B
A
A
A
be
Tor

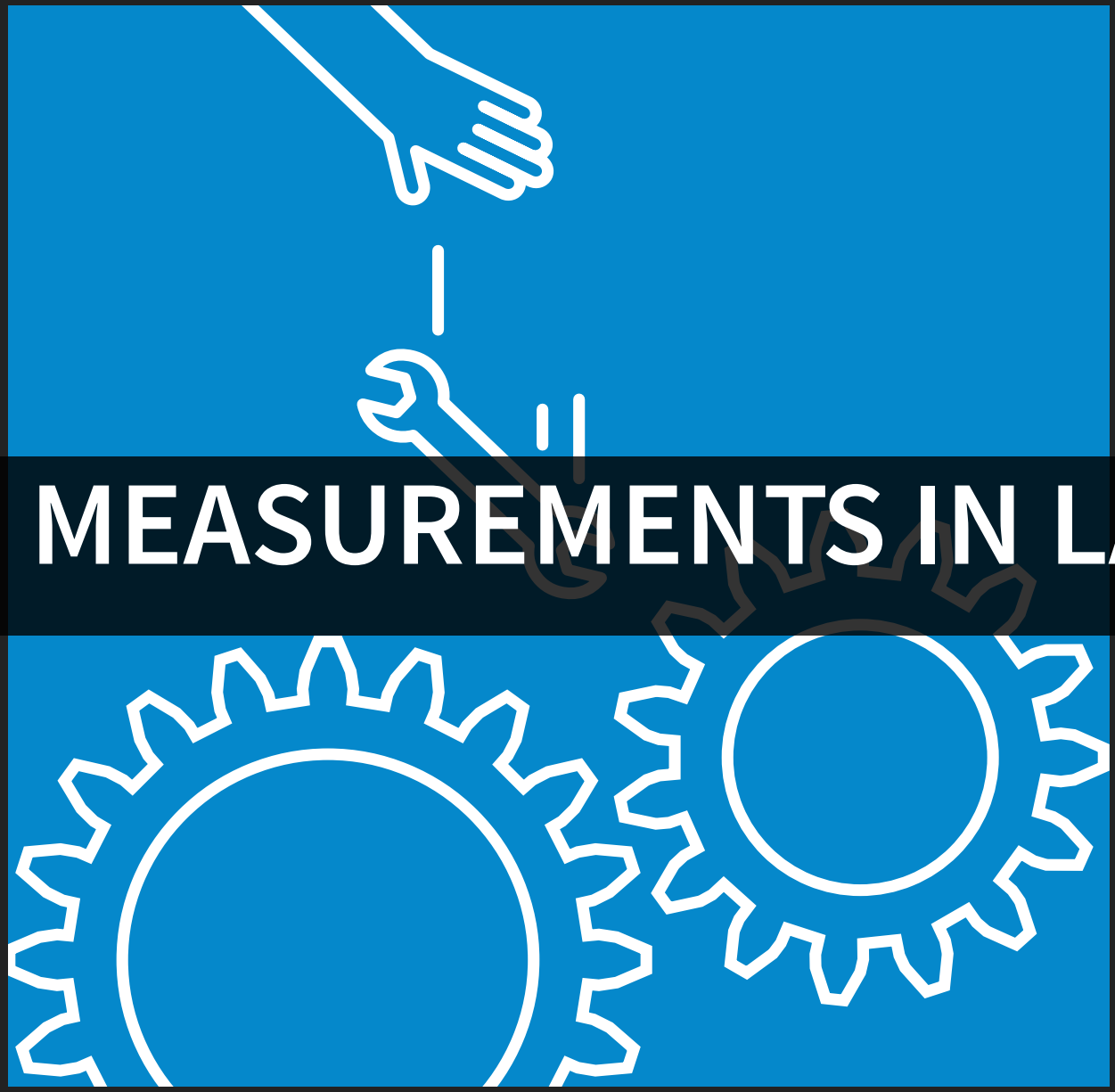
OONI TESTING METHODOLOGY



- Blocking of websites
- Blocking of instant messaging apps
- Blocking of censorship circumvention tools (Tor, VPN, Psiphon, Lantern)
- Detection of *middle boxes* proxy technologies that could be responsible for censorship and/or surveillance
- Speed and network performance tests (NDT)



OONI MEASUREMENTS IN LATAM



PIRATEBAY BLOCKED IN ARGENTINA

asurement

Web Connectivity 2017-03-23 06:24:01 UTC

20170323T062328Z_AS7303_UYQj7sql3cX8qzQXjRGZ4QCHf6lCnALEmLqcOjoFxpyIshSmI4

st runtime: 1.82408 seconds

be

Network: Telecom Argentina S.A., AR (AS7303)	**Name:** ooniprobe-android	**Version:** 1.1.2

This measurement contains data that could be a sign of network tampering or censorship.

site

https://thepiratebay.se

on for blocking: dns

measurements for URL

NEWS WEBSITE NTN24 BLOCKED IN VENEZUELA

asurement

Web Connectivity 2017-03-03 03:48:36 UTC

20170303T034153Z_AS8048_3ndo86P4sVdRgJ7N9CPMX5ft97YeHCbpCkofTTKol42forLpfN

st runtime: 4.69504 seconds

be

Network: CANTV Servicios, Venezuela, VE (AS8048)	**Name:** ooniprobe	**Version:** 2.0.1

This measurement contains data that could be a sign of network tampering or censorship.

site

http://ntn24.com

on for blocking: dns

measurements for URL

WHATSAPP BLOCKED IN BRAZIL

```
###############################################
# OONI Probe Report for http_requests (0.2.5)
# Mon May  2 23:17:02 2016
###############################################
probe_asn: AS26615
probe_cc: BR
software_name: ooniprobe
software_version: 1.4.2
test_helpers: {}
test_name: http_requests
test_start_time: '2016-05-02 21:17:02'
test_version: 0.2.5
...
agent: agent
body_length_match: null
```

OONI RESULTS (1/4)

- March 2017: Thailand blocked news and censorship circumvention tool websites
- December 2016: Malaysia block pages and censorship
- December 2016: Ethiopia DPI used to block media websites during major political protests

OONI RESULTS (2/4)

- December 2016: Belarus blocked Tor
- October 2016: Zambia blocked websites during general elections
- May 2016: Uganda blocking of social media

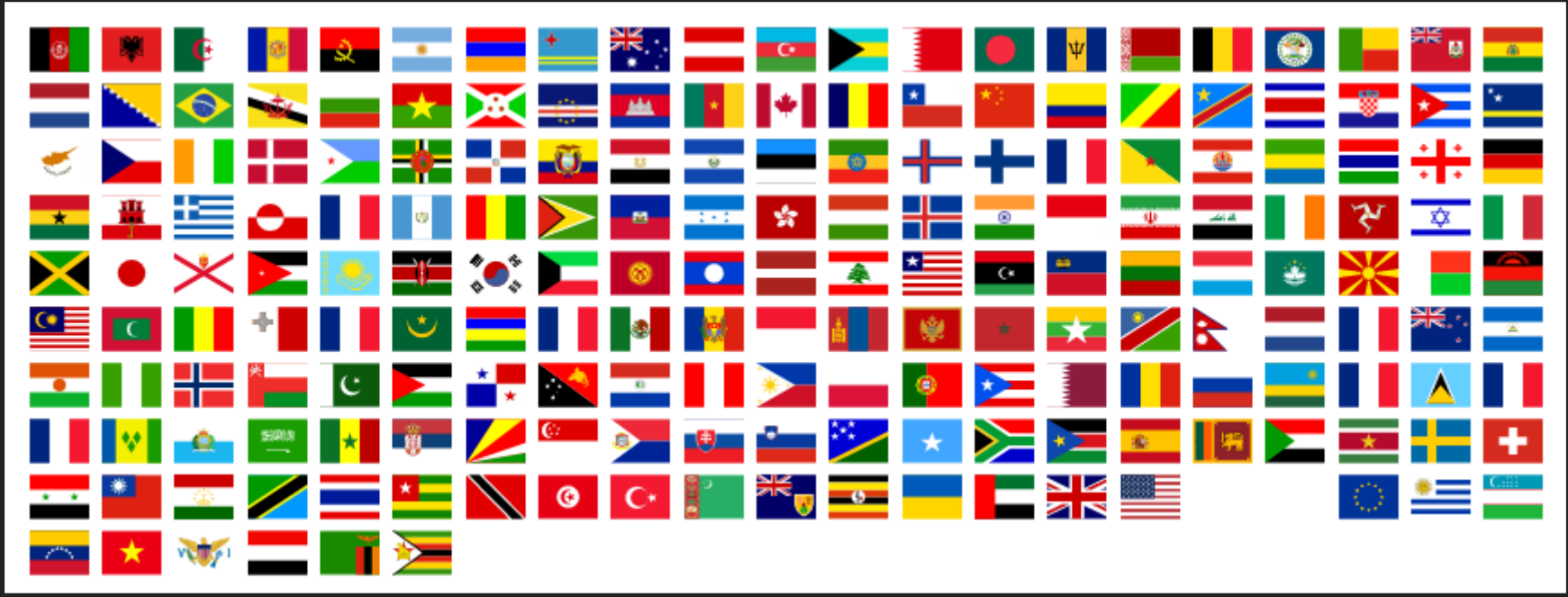
OONI RESULTS (3/4)

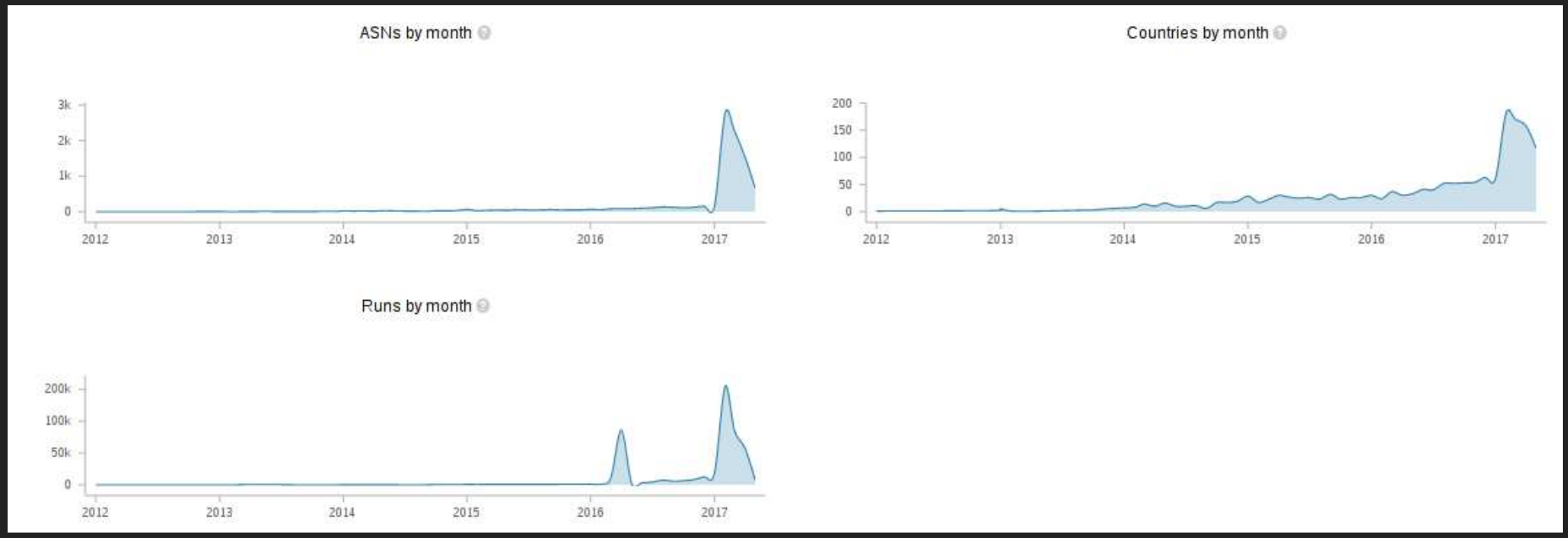
- May 2016: Brazil blocked WhatsApp
- June 2015: Greece and EEEP blocklists
- July 2013: Zambia, a country under Deep Packet Inspection

OONI RESULTS (4/4)

- May 2013: Uzbekistan and Turkmenistan Internet filtering and DPI
- April 2012: Hadara Palestine Internet agency Hadara restricts access to certain content for users in Bethlehem
- March 2012: T-Mobile USA Web Guard *Parental controls* blocked number of websites (Newgrounds, Cosmopolitan Magazine, and the Tor Project

OONI STATISTICS

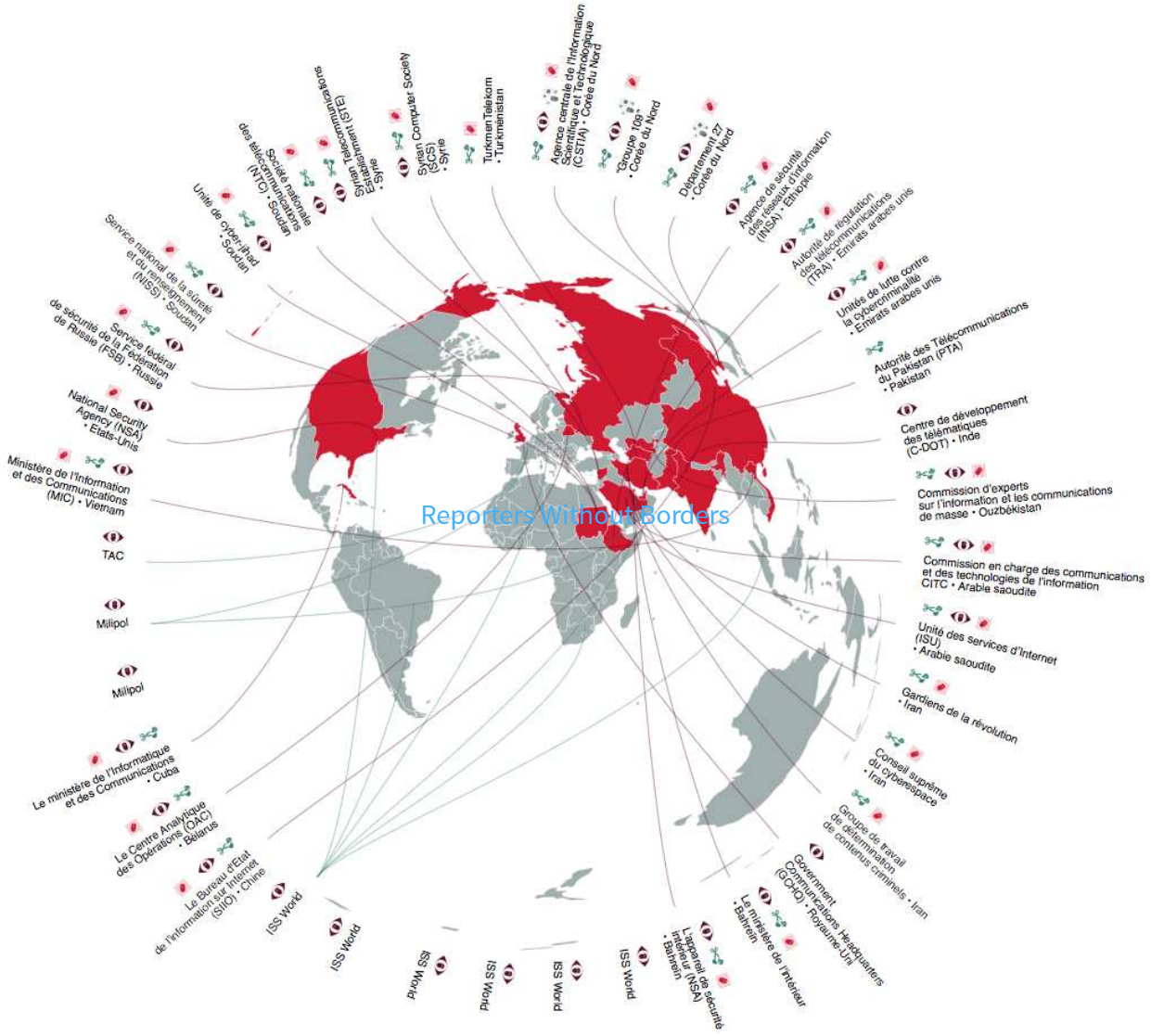




- Millions of network measurements collected from 200+ countries
- 2766+ unique ASNs

HELP

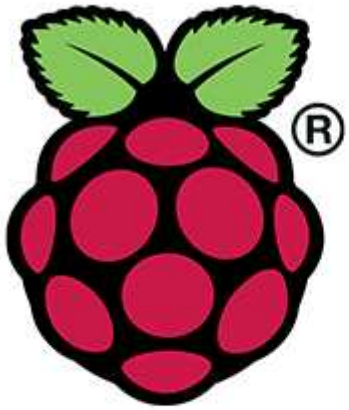
INTERNET HAS A LOT OF ENEMIES


Reporters Without Borders
Agence centrale de l'information Scientifique et Technologique (CSTIA) • Corée du Nord
Groupe 109 • Corée du Nord
Département 27 • Corée du Nord
Agence de sécurité des réseaux d'information (INSA) • Ethiopie
Autorité de régulation des télécommunications (TRA) • Emirats arabes unis
Unités de lutte contre la cybercriminalité • Emirats arabes unis
Autorité des Télécommunications du Pakistan (PTA) • Pakistan
Centre de développement des télématiques (C-DOT) • Inde
Commission d'experts sur l'information et les communications de masse • Ouzbékistan
Commission en charge des communications et des technologies de l'information CITC • Arabie saoudite
Unité des services d'Internet (ISU) • Arabie saoudite
Gardiens de la révolution • Iran
Conseil suprême du cyberespace • Iran
Groupe de travail de détermination de contenus criminels • Iran
Government Communications Headquarters (GCHQ) • Royaume-Uni
Le ministère de l'intérieur • Bahrein
L'appareil de sécurité intérieur (NSA) • Bahrein
ISS World
ISS World
ISS World
ISS World
ISS World
ISS World
Turkmen Telekom • Turkménistan
Syrian Computer Society (SCS) • Syrie
Syrian Telecommunications Establishment (STE) • Syrie
Société nationale des télécommunications (NTC) • Soudan
Unité de cyber-jihad • Soudan
Service national de la sûreté et du renseignement (NISS) • Soudan
Service fédéral de sécurité de la Fédération de Russie (FSB) • Russie
National Security Agency (NSA) • Etats-Unis
Ministère de l'Information et des Communications (MIC) • Vietnam
TAC
Milipol
Milipol
Le ministère de l'Informatique et des Communications • Cuba
Le Centre Analytique des Opérations (OAC) • Bélarus
Le Bureau d'Etat de l'information sur Internet (SIIO) • Chine

HELP REVEAL INTERNET CENSORSHIP

Install ooniprobe

Raspberry Pi



To install ooniprobe on Raspberry pi devices see our lepidopter install guide

OS X and Linux

To install ooniprobe on unix based systems read our installation guide

GET IT ON Google Play | Download on the App Store | GET IT ON F-Droid

- Available for: Linux, Mac OS, Raspberry Pi, IOS, Android
- Source code: https://github.com/TheTorProject/ooni-probe

HOW CAN YOU HELP TOR?

- Run a relay (or a bridge)
- Teach your friends about Tor, and privacy in general
- Help fix -- and fix -- bugs
- Work on open research problems (petsymposium.org)

Protect your privacy

https://www.torproject.org/download/download-easy.html/