

# Distributed Detection of Tor Directory Authorities Censorship in Mexico

UNAM/DGAPA/PAPIME PE102718

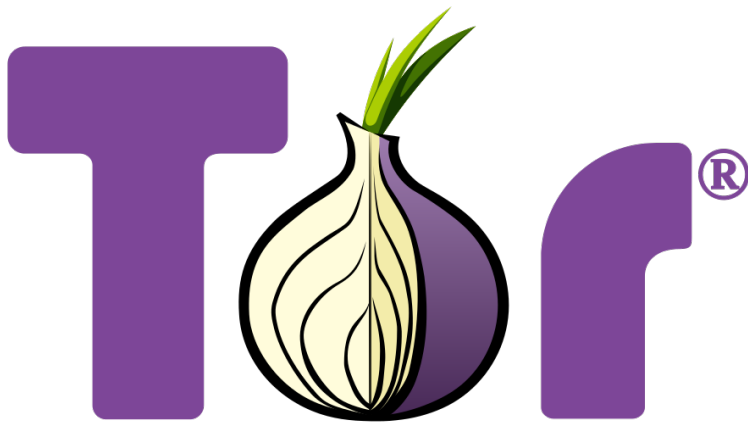
Gunnar Wolf • IIEc-UNAM / FI-UNAM

TICS • ICN • NexConn, Valencia, Spain

# Contenidos

- 1 Introduction
- 2 Probable Tor censorship in Mexico
- 3 Results and discussion

# The Tor network



# Motivation

- *Anonymity loves company*

# Motivation

- *Anonymity loves company*
- *Anonymity loves diversity*

# Motivation

- *Anonymity loves company*
- *Anonymity loves diversity*
- $\hookrightarrow$  Tor wants *more volunteers* offering *anonymizing relays* to further the anonymity guarantees against *state-level attackers*
  - As widely distributed across jurisdictions as possible
- $\hookrightarrow$  Many users *believe* in Tor's mission and want to support it, offering their available resources
  - $\approx$  6300 relays worldwide for  $\approx$  2 million daily users\*
- April 2017: Tor Project's *Global South* working group

# Anonymizing relays in Tor

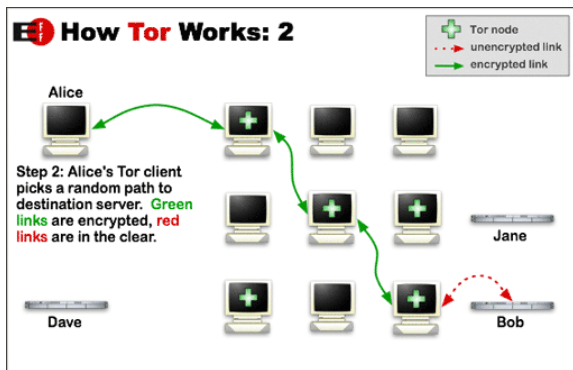
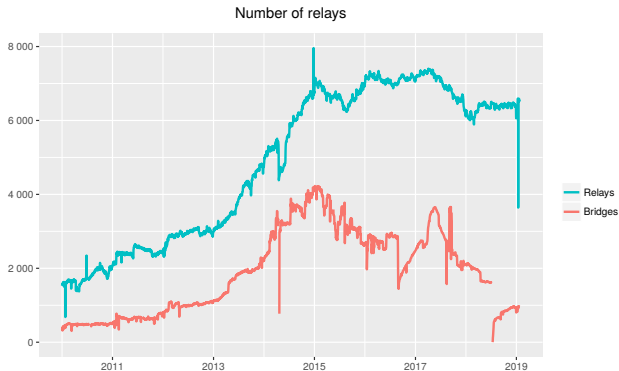


Image source: <https://2019.www.torproject.org/images/htw2.png>

# Number of relays over time



Number of relays and bridges over time, 2010–2019

Source: <https://metrics.torproject.org/networksize.html>



# Contenidos

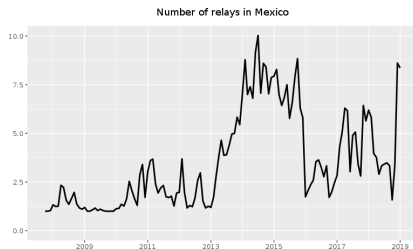
- 1 Introduction
- 2 Probable Tor censorship in Mexico
- 3 Results and discussion

# Uneven Tor participation by geographic origin

- *Users* of the Tor network by 2014: 10,000  $\approx$  15,000 daily users
  - Same range as Sweden or Austria
  - Ten times the population
  - Far worse score on human rights, freedom of the press
- *Providers* to the Tor network (relay or exit node operators): Barely a *blip* on the radar
  - ... See the censorship in late 2015?

# Uneven Tor participation by geographic origin

- *Users* of the Tor network by 2014: 10,000  $\approx$  15,000 daily users
  - Same range as Sweden or Austria
  - Ten times the population
  - Far worse score on human rights, freedom of the press
- *Providers* to the Tor network (relay or exit node operators): Barely a *blip* on the radar
  - ... See the censorship in late 2015?



Number of relays in Mexico, 2008–2019

Source:

<https://metrics.torproject.org/>,  
processed by Vasilis Ververis

# Censorship: Architecture or policy?

End-users cannot get relays working in Mexico. Why? Is it a deliberate policy?

## Questions to answer:

- Do ISPs *actively interfere* with connections?
  - Technical measures *purposefully set up* to block Tor?
- Does the ISP perform *Deep NAT*?
- Does the ISP allow end users to reconfigure their routers and receive incoming connections?
  - Rights to set up the modem. Whose property is it, all in all?
  - Can users reconfigure their modems? (valid security concerns!)
- Which ISPs are *most amenable* for setting up relays?

# How to get our data

**Challenge** Set up a quick call for participation

- Ask individuals to make a *quick* check on their networks and report back to us

**Constraint** Users might test from *different platforms*.

- They might test *only once* from a given device
- $\leftrightarrow$  We don't install any nonstandard software, work only with OS-provided tools

**Decision** Ask participants to provide *traceroute* reports to the eleven Tor DirAuths

- $2 \approx 8$  minutes per probe
- Requires interaction with the command line (non-user-friendly!)
- Unix, Windows outputs equally parsable
- (Mobile platforms are left out)

# Data reporting interface

## Censura de conexiones hacia Tor desde ISPs mexicanos

Estamos iniciando un proyecto que nos lleve a mapear qué tan amigables u hostiles son los diferentes ISPs mexicanos para hospedar relays de Tor. Para eso, un paso muy importante es mapear qué redes nos permiten o no tener comunicación con las autoridades de directorio (DirAuths).


Les agradeceré que nos ayuden a recabar esta información, para lo cual les pedimos:

### Tu nombre, alias, o alguna identificación.

Si no quieres compartirlo, puedes dejarlo en blanco.

### Tipo de conexión

Indicanos qué tanto conoces y puedes confiar en la administración de la conexión que nos estás presentando

- Doméstica
- Universitaria (fija)
- Universitaria (inalámbrica)
- Laboral / empresarial
- Pública, negocio pequeño
- Pública, cadena o negocio grande
- Intrusada 
- Celular
- Otra

### ISP que utilizas

Este es uno de los puntos que resulta más importante para nuestro estudio. Indica el nombre del proveedor de servicios. En caso de que no lo conozcas (por ejemplo, si estás reportando desde un punto público de WiFi), intentaremos obtener esta información desde las rutas que nos adjuntas — ¡Pero lo más confiable es que nos des la información!

### Estado

¿Desde dónde se toman estas rutas?

### Reporte

Este es el campo más importante de los que te pedimos. Pega a continuación el resultado de trazar la ruta a las nueve autoridades de directorio (DirAuths) de Tor. Para hacerlo, en sistemas Unix (lo cual cubre, por lo menos, a Linux, Mac y los BSDs) puedes utilizar el siguiente comando:

```
for i in 171.25.193.9 86.59.21.38 199.58.81.140 194.109.206.212 204.13.164.118 131.188.40.189 128.31.0.34 193.23.244.244 154.35.175.225
128.31.0.39 199.254.238.52; do traceroute $i; done
```

Desde la línea de comando (CMD.EXE) en Windows, debería funcionar con:

```
C:\> COPY CON 1.bat
for %i in (171.25.193.9 86.59.21.38 199.58.81.140 194.109.206.212 204.13.164.118 131.188.40.189 128.31.0.34 193.23.244.244 154.35.175.225
128.31.0.39 199.254.238.52) do tracert %i >> tor.txt
&
C:\> 1.bat
```

Esto generará un archivo `tor.txt`, que puedes abrir con cualquier programa (p.ej. Notepad) y pegarlo en el formulario a continuación. Pueden ser hasta unas 350 líneas, y dependiendo de tu red, puede tomar unos cinco minutos en realizarse. La lista de direcciones IP que te presento viene de la página del [estado de salud del conector](#) del proyecto Tor, así como del [código fuente](#) del cliente Tor.

# Contenidos

- 1 Introduction
- 2 Probable Tor censorship in Mexico
- 3 Results and discussion**

# Numerical

- Time frame Five months  
Number of reports 79  
States covered 12 (out of 32 countrywide)  
Dominant ISP Telmex (as expected!)

ISP	Reports
Telmex	32
Axtel	10
Izzi	7
Total Play	7
AT&T	6
Megacable	4
Alestra	2
UNAM	2

Only one: Avantel, Bestel, Cablevisión, Express VPN, Maxcom, Prrovsor, Nextel, Telcel



# At a glimpse

Percentage of reachable ISPs from a given particular proxy.

Universitaria (fija)	UNAM	55%	<a href="#">Ver</a>	Ciudad de México	201.114.174.1	2018-08-25 05:00
Doméstica	Infinitum	33%	<a href="#">Ver</a>	Ciudad de México	201.114.174.1	2018-08-25 05:01
Doméstica	Infinitum	0%	<a href="#">Ver</a>	Morelos	187.225.168.1	2018-08-26 05:02
Doméstica	Infinitum	0%	<a href="#">Ver</a>		187.134.200.1	2018-08-28 03:35
Otra	AT&T movil	38%	<a href="#">Ver</a>		201.175.158.1	2018-08-28 03:43
Otra	AT&T movil	77%	<a href="#">Ver</a>		201.175.158.1	2018-08-28 03:47
Laboral / empresarial	Axtel	54%	<a href="#">Ver</a>	Ciudad de México	187.162.66.1	2018-08-28 16:34
Laboral / empresarial	maxcom	0%	<a href="#">Ver</a>	Ciudad de México	187.248.22.1	2018-08-28 16:38
Doméstica	TotalPlay	72%	<a href="#">Ver</a>	Ciudad de México	187.190.26.1	2018-08-28 16:41
Doméstica	Axtel	54%	<a href="#">Ver</a>	Ciudad de México	200.194.38.1	2018-08-28 17:18
Universitaria (fija)		58%	<a href="#">Ver</a>	Ciudad de México	148.204.66.1	2018-08-28 18:16
Doméstica	Axtel	54%	<a href="#">Ver</a>	Ciudad de México	201.156.39.1	2018-08-28 18:22
Laboral / empresarial	AT&T Comunicaciones Digitales S de RL	54%	<a href="#">Ver</a>	Ciudad de México	201.130.57.1	2018-08-28 18:46
Laboral / empresarial	Total Play Empresarial	54%	<a href="#">Ver</a>	Ciudad de México	187.189.213.1	2018-08-28 19:01
Laboral / empresarial	Axtel Empresarial	54%	<a href="#">Ver</a>	Nuevo León	187.167.67.1	2018-08-28 19:01
Doméstica	IZZI	72%	<a href="#">Ver</a>	Ciudad de México	201.141.37.1	2018-08-28 20:34
Doméstica	TotalPlay	72%	<a href="#">Ver</a>	Ciudad de México	187.190.11.1	2018-08-28 20:35
Doméstica	Telmex	0%	<a href="#">Ver</a>	Chiapas	187.171.216.1	2018-08-28 23:15
Doméstica	Telmex	0%	<a href="#">Ver</a>	Ciudad de México	189.241.170.1	2018-08-29 00:53
Laboral / empresarial	AT&T Comunicaciones Digitales S de RL	54%	<a href="#">Ver</a>	Ciudad de México	201.130.57.1	2018-08-29 01:37
Doméstica	Telmex	27%	<a href="#">Ver</a>	Ciudad de México	187.207.239.1	2018-08-29 02:03
Doméstica	Nextel Mexico	0%	<a href="#">Ver</a>	Colima	201.175.158.1	2018-08-29 02:13
Doméstica	IZZI	0%	<a href="#">Ver</a>	México	189.217.3.1	2018-08-29 03:28