NEbraskaCERT
Tor in 2020
By Aaron Grothe

October 21. 2020

Introduction

The following are three questions I often get asked:

- How do I get some bitcoins to pay off some ransomware?
- What is TOR? Is it good? What is an .onion site
- When is the next NEbraskaCERT meeting :-)

This one is of course about TOR.

BTW - the next NEbraskaCERT meeting is November 18th and it will be the panel meeting.

Goals for this Talk

The following are the goals for this talk

- EARN-IT Act
- Tor Usage
- Talk a bit about TOR's history
- Talk a bit about getting started with Tor
- Small Demo
- Discuss other options for TOR
- Q & A

EARN IT Act of 2020

The EARN-IT Act of 2020 is a proposal that allows any state to bring a lawsuit against a service provider, if they fail to deal with child sexual abuse material on their service OR they allow end-to-end encryption without providing the menans to decrypt to enforcement officals.

Something like this would have major impacts on commerce and everything else that goes over the internet.

Brings back the idea of when we were limited to 40-bit encryption and it was treated as a muntion.

EARN IT Act of 2020

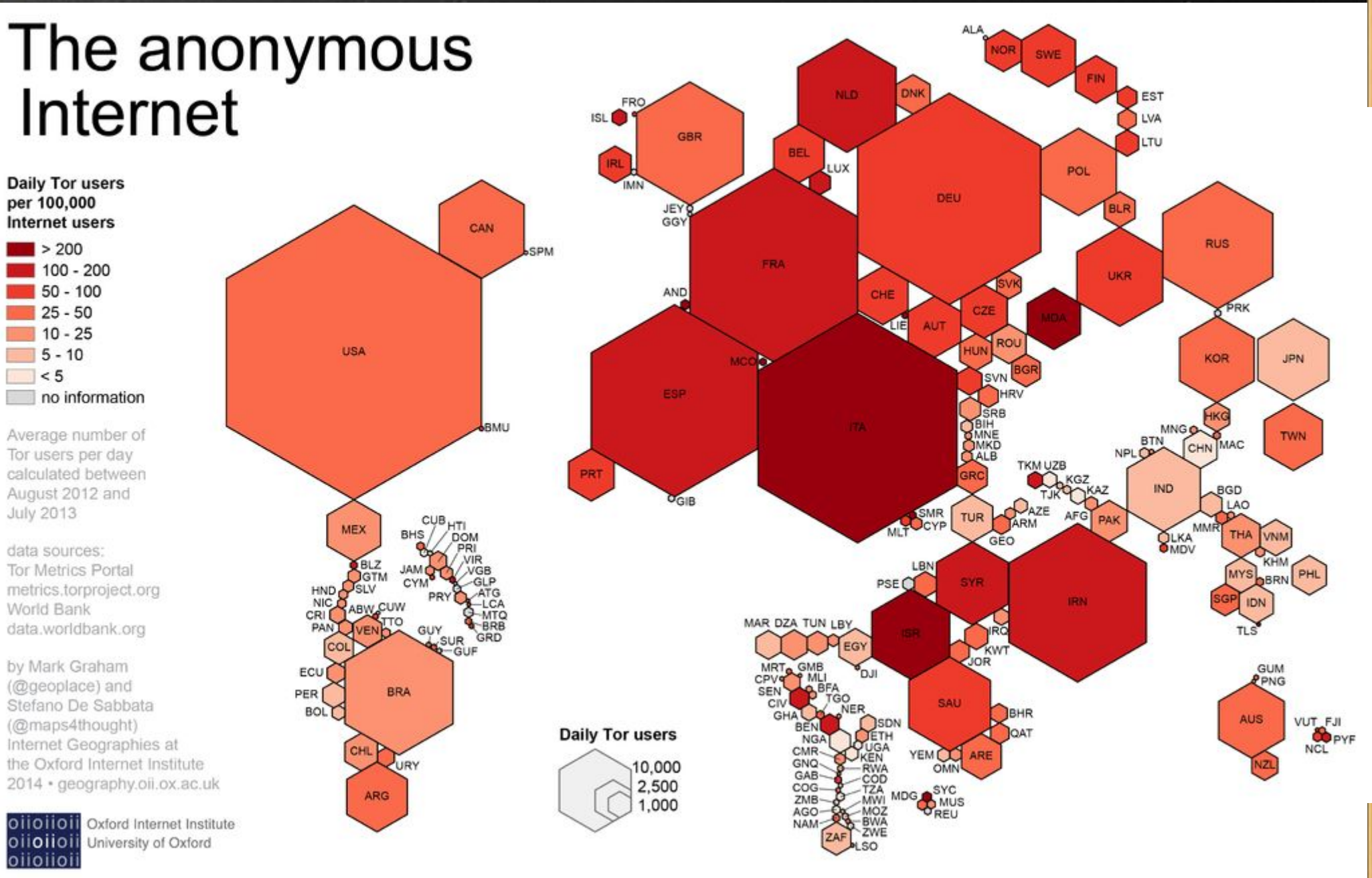
From Senator Deb Fisher's Office in response to my letter about this

As you know, Sen. Lindsey Graham (R-S.C.) introduced S. 3398, the Eliminating Abusive and Rampant Neglect of Interactive Technologies (EARN IT) Act on March 5, 2020. If enacted, this bill would amend the Communications Decency Act (CDA) of 1996, to allow civil suits against interactive computer services that "recklessly" distribute child pornography, and enable criminal and civil enforcement of similar state statutes.

The bill also would establish a commission to determine best practices for identifying and reporting child sexual exploitation online. Companies that do not meet those best practice standards could then lose their Section 230 liability protections. On July 2, 2020, S. 3398 was approved by the Senate Judiciary Committee by a vote of 22 to 0 and it is now pending before the full Senate.

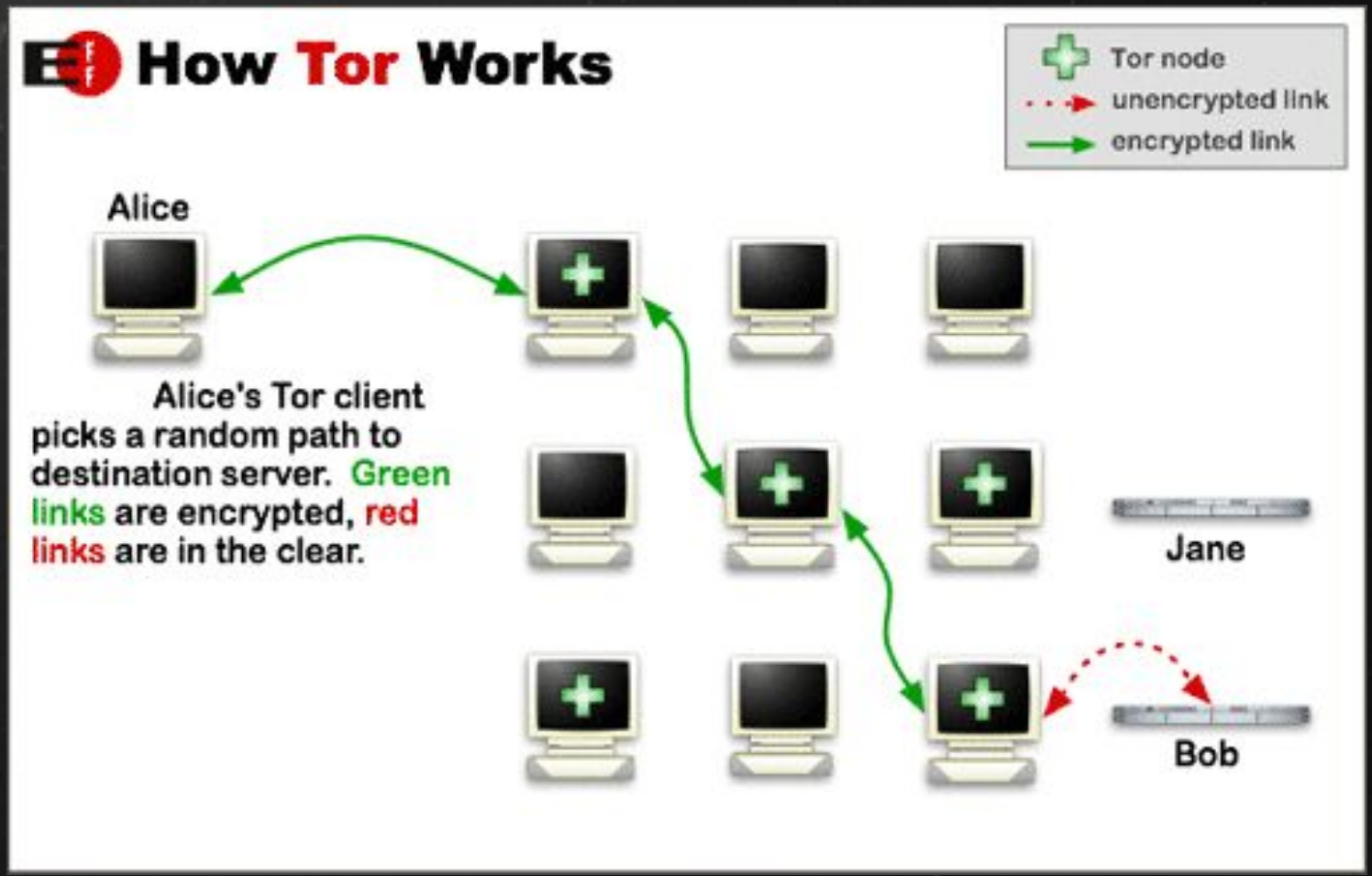
I am deeply disturbed by reports about the prevalence of online child sexual exploitation in our country and around the world. I believe we can balance the goals of the CDA, and specifically Section 230, which drives creativity and innovation, and still protect children from online predators. Our government should effectively prosecute illegal activity in both the physical and virtual spaces.

Tor Usage


The anonymous Internet
Daily Tor users per 100,000 Internet users
> 200
100 - 200
50 - 100
25 - 50
10 - 25
5 - 10
< 5
no information
Average number of Tor users per day calculated between August 2012 and July 2013
data sources:
Tor Metrics Portal
metrics.torproject.org
World Bank
data.worldbank.org
by Mark Graham (@geoplace) and Stefano De Sabbata (@maps4thought)
Internet Geographies at the Oxford Internet Institute
2014 • geography.oii.ox.ac.uk
Oxford Internet Institute
University of Oxford
Daily Tor users
10,000
2,500
1,000
ALA NOR SWE FIN EST LVA LTU
FRO ISL GBR IRL IMN JEY GGY
NLD DNK BEL LUX DEU POL BLR
FRA AND CHE LIE AUT CZE SVK MDA UKR RUS PRK
ESP PRT GIB MCO ITA HUN ROU BGR SVN HRV SRB BIH MNE MKD ALB GRC
KOR JPN HKG TWN MNG BTN NPL CHN MAC
TKM UZB KGZ TJK KAZ IND BGD LAO MMR THA VNM KHM MYS BRN SGP IDN PHL TLS
SMR MLT CYP TUR AZE ARM GEO AFG PAK LKA MDV
LBN PSE SYR IRN IRQ KWT JOR ISR
MAR DZA TUN LBY EGY DJI MRT GMB CPV SEN MLI BFA CIV TGO GHA NER BEN NGA SDN ETH UGA KEN RWA COD TZA MWI MOZ BWA ZWE ZAF LSO CMR GNQ GAB COG ZMB AGO NAM
SAU BHR QAT YEM OMN ARE
MDG SYC MUS REU
GUM PNG AUS NZL VUT FJI NCL PYF
USA CAN SPM BMU
MEX BLZ GTM HND SLV NIC CRI ABW CUW PAN VEN TTO COL ECU PER BOL BRA CHL URY ARG
CUB HTI BHS DOM PRI VIR JAM CYM VGB GLP PRY ATG LCA MTQ BRB GRD GUY SUR GUF

TOR?

- Tor stands for The Onion Router. Like an Ogre Tor has layers.



TOR Timeline

- The concepts of Tor "onion routing" was created by the US Naval Research Laboratory and further developed by DARPA in 1997
- First alpha release was in 2002
- In 2004 Naval Research Lab released the code to Tor under a free license and EFF continued to fund its development
- In 2006 the Tor Project was founded
- May-June 2013 - Snowden uses Tor as part of his disclosure process
- Prior to 2014 majority of funding came from U.S. Government
- In November 2014, Operation Onymous lead to belief by some that Tor had been exploited

Operation Onymous

November 5-6 - bunch of illegal website shutdown including

- Silk Road 2.0
- Cloud 9
- Hydra

Money Laundering and other sites were also compromised

Was it a 0-day exploit against Tor? Some believe it and others blame other things such as tracing bitcoin traffic.

I thought Tor was totally anonymous

Couple of Caveats:

- If you can DDOS enough exit nodes you can increase your odds of getting the traffic
- Exit relays don't use additional encryption, so please use encryption on top of Tor
- Tor use is obvious. If you're the only person using Tor on your home ISP segment they can figure it out
- Have to make sure to start using it and keep using it. DPR got caught because years before the Silk Road he posted to a usenet news group without hiding his name

Who Uses Tor?

Source:
https://techlog360.com/edward-snowden-said-about-tor-project/

Who else uses Tor?

Bad People

- Drug Dealers
- Money Launderers
- Other Criminals
- Child Pornographers

Good People

- Journalists in repressive countries
- Human Rights Activists
- Researchers
- Paranoid People

Trying Out Tor

The simplest way to use Tor is to use the Tor Browser

https://www.torproject.org/download/

Based on Mozilla - ESR releases

Simple as a download, verify the gpg signature and you're good to go

How to validate Download

https://support.torproject.org/tbb/how-to-verify-signature/

Demo

Let's try out a few sites

Check your using Tor

https://check.torproject.org/

Check your IP address

https://www.whatismyip.com/

Demo (cont'd)

Let's try out a few sites

Check your using public IP address

https://ipleak.net/

Make sure you're not leaking DNS

https://dnsleaktest.com/

Demo (Cont'd)

Onion Sites: Onion Sites are sites that are not visible on the regular net. Welcome to the Dark Web.

Hit what I think is one of the funniest websites:

https://www.facebookcorewwwi.onion/

You're hitting the site that collects the most personal information with an anonymizer

Demo (Cont'd)

Lets see how well it does at avoiding fingerprinting

https://panopticlick.eff.org/

Panopticlick sees how safe your browser is against tracking

Question here is fingerprinting

If you want real anonymity use regular tor with Links :-)

How fast is it?

Speed test from speedof.me from regular browser

How fast is it? (Tor)

Speed using Tor Browser

Tor Project Browser

Pros

- Simple
- Pretty secure
- Good first entry to Tor
- Available for Linux, Mac OS X, Windows, Android and Iphone
  - Don't know if I'd trust any of them except Linux

Cons

- Plugins can potentially bypass protections
- Security is not as good as some other solutions
- Might get foreign language pages

Other Options

We'll talk about a couple of other options as well

- Tails
- Whonix
- Tor on OpenWRT
- Raspberry PI
- Roll your own

Tails

Tails is a distribution that can be booted off a live DVD or a live USB. Richard Snowden approved.

The goal here is to leave no traces on the underlying machine on which it is run.

It is a complete solution, that is nice to use when you can't devote a machine to the process.

Kanguru offers USB sticks with physical write protect switch. Don't trust SD cards as the write protect switch is just a suggestion.

Whonix

Consists of two virtual machines - a workstation and a tor gateway

The gateway box has two ethernet connections - one to workstation and one to internet

The workstation has only one ethernet connection - only to gateway box

Supports KVM, Virtualbox and Qubes OS as hosts.

Whonix has a lot of documentation on their site and provide a lot of good information.

Tor on OpenWRT

If you're running OpenWRT on your router you can install tor on it pretty easily

```
# opkg update
# opkg install tor
```

Lot more configuration to do, but that gives you a start

https://openwrt.org/docs/guide-user/services/tor/client

Tor on OpenWRT (Cont'd)

Gl.inet has some pretty simple routers that are available from less than $25

They used to offer a tor package, but they don't support it any more.

Your quality of life will depend on how much Ram/Flash Ram storage your device has.

Roll Your Own

Tor is available for Debian/Fedora/Ubuntu etc.

You can install and setup your own Tor client on a system pretty easily. There are how to guides for most operating systems

Keep in mind persistence grants more information and data for people to collate. The safer solutions like Tails and Whonix offer amnesiac options

Summary

Rick Deckard: Replicants are like any other machine, are either a benefit or a hazard. If they're a benefit it's not my problem. - Bladerunner

Tor is interesting and has some real uses. It has been used by a lot of people and has been analyzed by a lot of people over the years.

It is easy to try out, hope you give it a spin.

Links

Tor Project: https://www.torproject.org/

Tails: https://tails.boum.org/

Tor page on Wikipedia: https://en.wikipedia.org/wiki/Tor_(anonymity_network)

Whonix: https://www.whonix.org/

OpenWRT Tor: https://openwrt.org/docs/guide-user/services/tor/client