Tor Browser

Steve Revilak
https://masspirates.org/

Cryptoparty @ MGHPCC

February 14, 2015

What is Tor?

Tor is ...

> *"free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security."*

(quote from `https://www.torproject.org/`)

In short, Tor conceals the source of web traffic, along with the content of that web traffic.

Why use Tor? (1)

Source: NSA *Tor Stinks* presentation.

`https://www.documentcloud.org/documents/801434-doc2.html`

Why Use Tor? (2)

Tor Stinks... (U)

- We will never be able to de-anonymize all Tor users all the time.
- With manual analysis we can de-anonymize a **very small fraction** of Tor users, however, **no** success de-anonymizing a user in response to a TOPI request/on demand.

Source: *ibid*

Why Use Tor? (3)

I see two ways to interpret the NSA's *Tor Stinks* presentation:

1. Tor is a good system for preserving anonymity on the web, and the NSA has trouble "breaking" it.
2. Tor is horribly broken, so the NSA wants us all to use it.

Being the optimist, I'm more inclined to side with the former.

Installing and Running Tor

- You can download Tor from the Tor Project's web site `https://www.torproject.org`
- Tor Browser should look familiar to Firefox users – it's a customized version of Firefox.
- Browse to `https://www.maxmind.com/en/geoip_demo` with Tor. What do you see? Try again with a regular web browser, and compare the results.

Meet Alice and Bob

Alice's Dilemma

- Alice wants to send a letter to Bob.
- Alice doesn't want Bob to know that she sent the letter.
- So, Alice enlists the help of Tom, Dick, and Harry

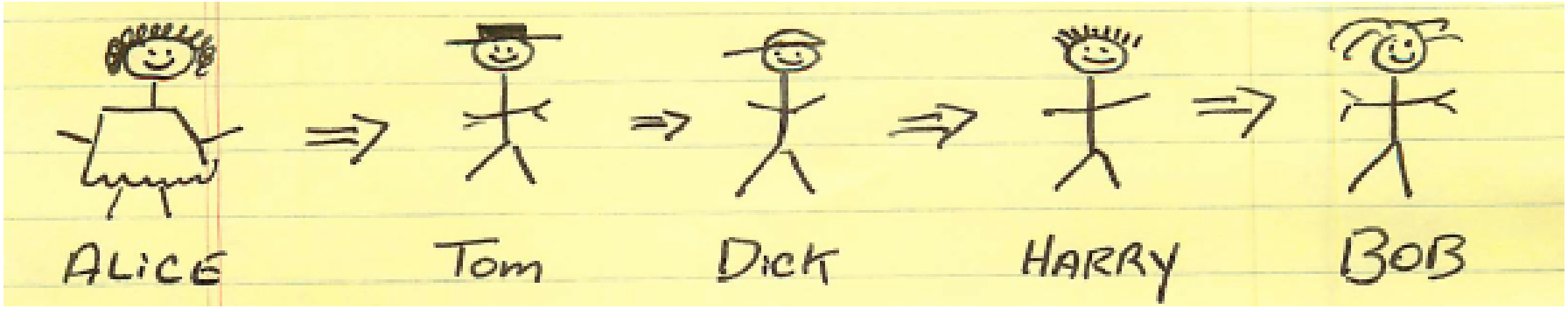
What follows is a rough analogy of how Tor works.

Alice's Plan

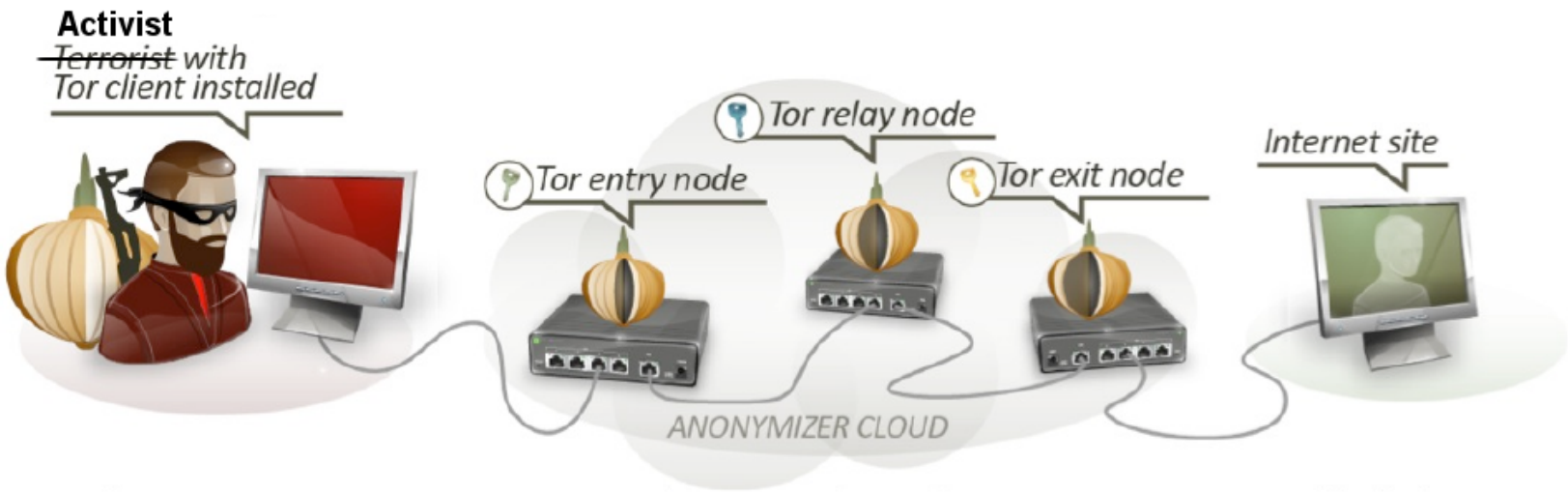
- Alice writes a letter to Bob, *without* signing it.
- Alice puts the letter in an envelope addressed to Bob,
- and puts that in an envelope addressed to Harry,
- and puts that in an envelope addressed to Dick,
- and puts that in an envelope addressed to Tom
- Alice mails the letter to Tom

Mailing the Letter

- Alice mails the letter.
- Tom gets the letter, and mails the contents to Dick
- Dick gets the letter, and mails the contents to Harry
- Harry gets the letter, and mails the contents to Bob
- Bob reads Alice's letter
- As far as Bob can tell, the letter came from Harry. (Harry is an "exit node".)

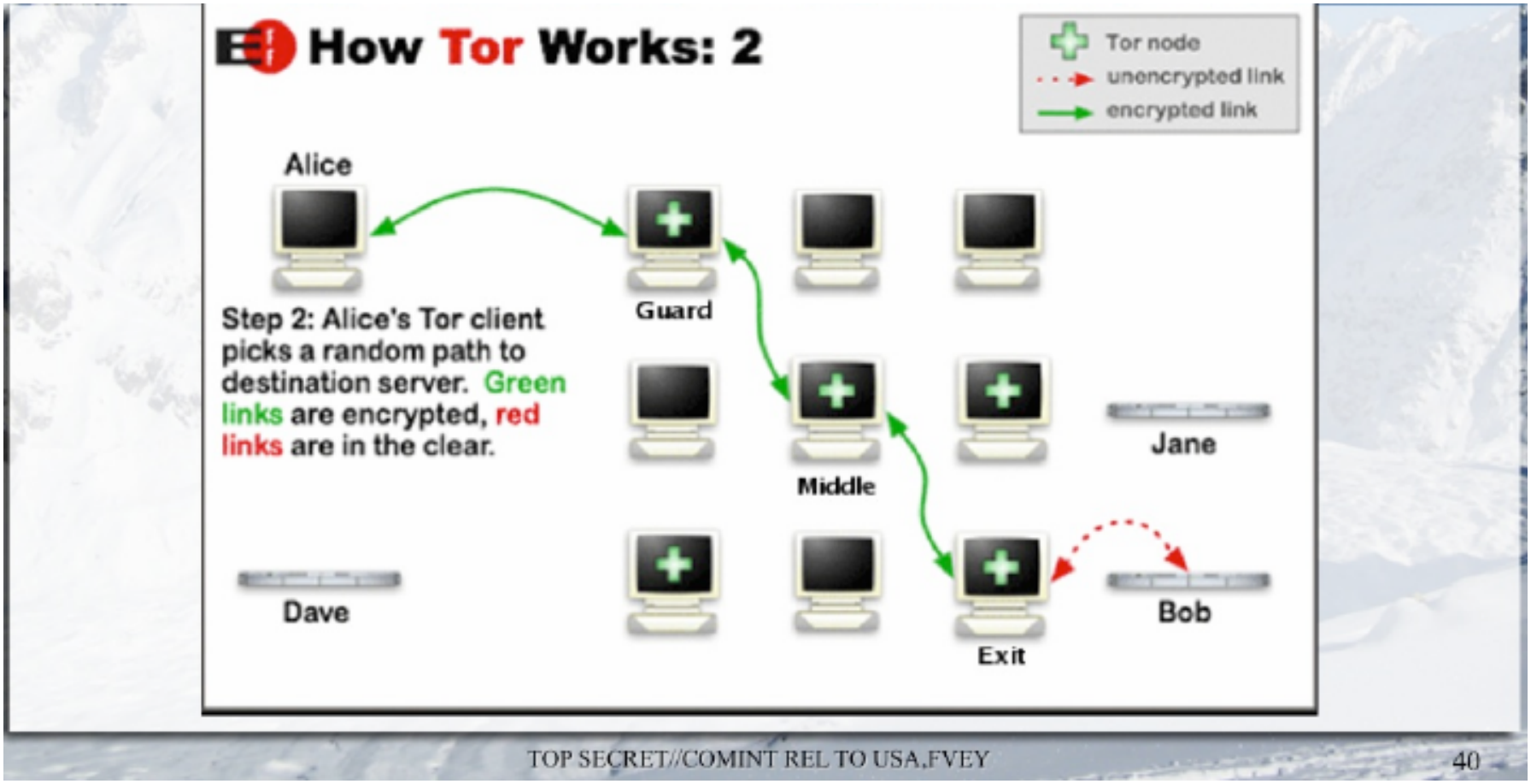


Tor's Version of the chain letter



Source: My EFF-inspired tweaks to a *Tor Stinks* graphic.

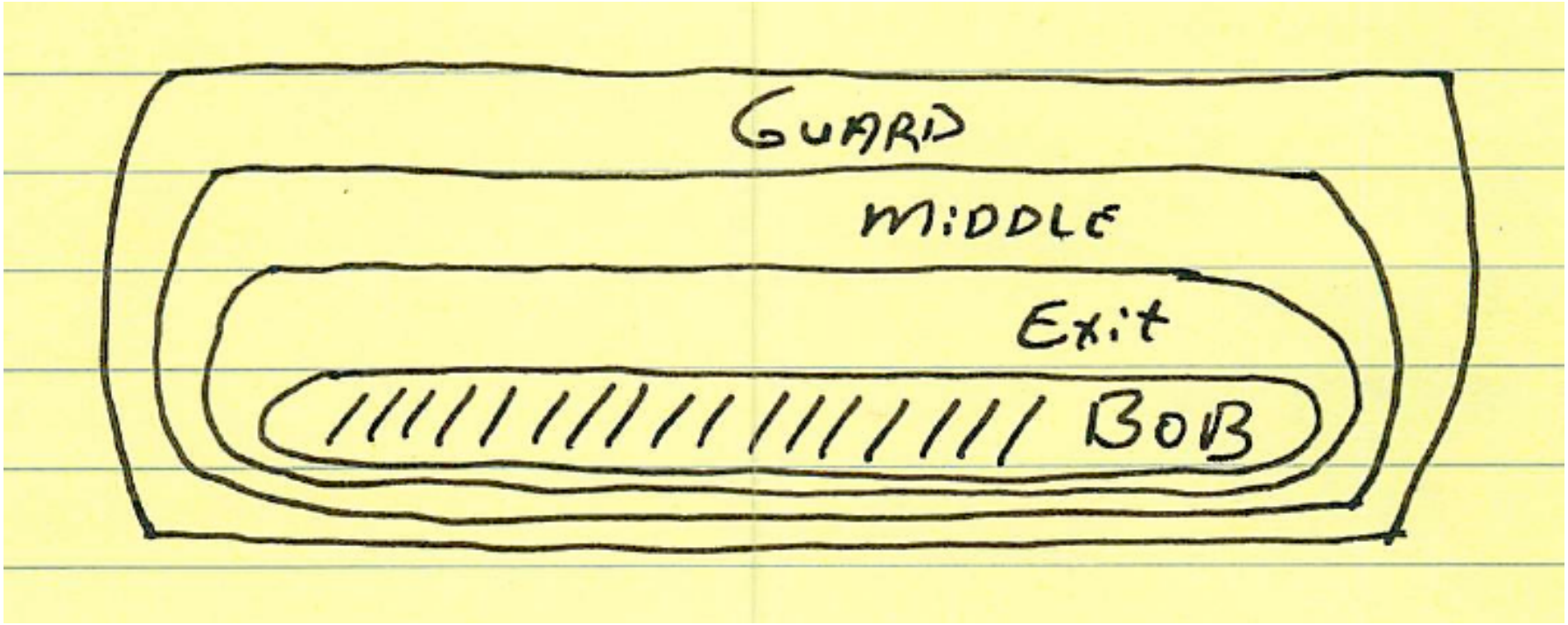
How Tor Works



Source: NSA *Advanced Open Source Multi-Hop* presentation
`https://www.documentcloud.org/documents/801435-doc3.html`

How Tor Works (3)

Here's what Alice's "Letter" looks like:



These layers of encryption constitute an *onion*.

Inside the NSA's war on Internet Security

Dec 28, 2014 article on NSA/GCHQ counter-security techniques (defeating Tor, HTTPS, VPNs, etc).

`http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html`

GCHQ Circuit Tracing Project

UK TOP SECRET STRAP1 COMINT

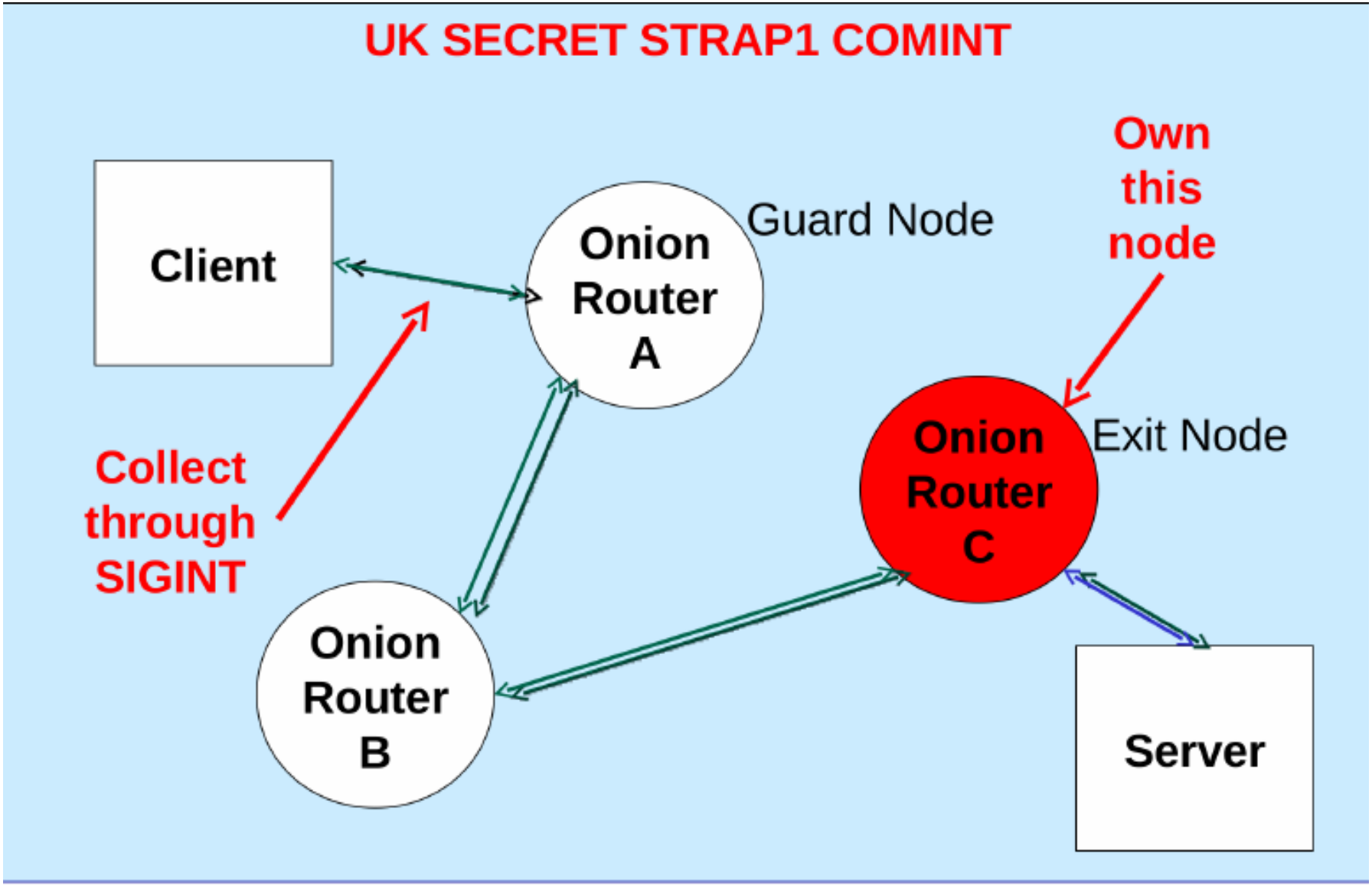
Side note: Circuit tracing

- One suggestion was to track packets through each hop in the TOR network
- We experimented with spotting all links in circuits created by GCHQ
- Visibility was too low to be a sensible approach
  - 13 out of 8294 potential inter-TOR-router links were seen
- We will directly correlate:
  - exit node traffic, and
  - traffic between client and guard node

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [redacted]

© Crown Copyright. All rights reserved.

Attacking Guard and Exit Nodes (1)



GCHQ

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [redacted]

© Crown Copyright. All rights reserved.

Attacking Guard and Exit Nodes (2)

- Guard and Exit node attack relies on GCHQ owning some number of exit nodes (to demux circuit ids), *and*
- Being able to collect a significant amount of client $\Leftrightarrow$ guard node traffic.
- This attack is completely defeated if Client runs a non-exit Tor node.

Tor Caveats

- Tor is slower than using an ordinary web browser.
- Web sites that rely heavily on Geolocation (e.g., Google) might get confused about your "unusual location".
- You may need to change your browsing habits (see `https://www.torproject.org/download/download-easy.html#warning` for elaboration).

Tor Wrap Up

- Using Tor is just as easy as using any other web browser.
- Tor protects you from surveillance by proxying web traffic through a network of Tor nodes.
- The network of Tor nodes conceals your location; encryption protects the content of your traffic.