# THE DEEP WEB

# WHAT IS THE DEEP WEB?

Put simply, it is the part of the Internet that is hidden from view.

4% OF WWW CONTENT

96% OF WWW CONTENT

## SURFACE WEB

Also known as the 'Visible Web', it is content that can be found using search engines such as Google or Yahoo. It is under constant surveillance by the government.

## DEEP WEB

Also known as the 'Invisible Web', it is the content that cannot be indexed by search engines. And it is hard to keep track of.

The Deep Web is estimated to be **500X** the size of the Surface Web.

# HOW DO YOU ACCESS IT?

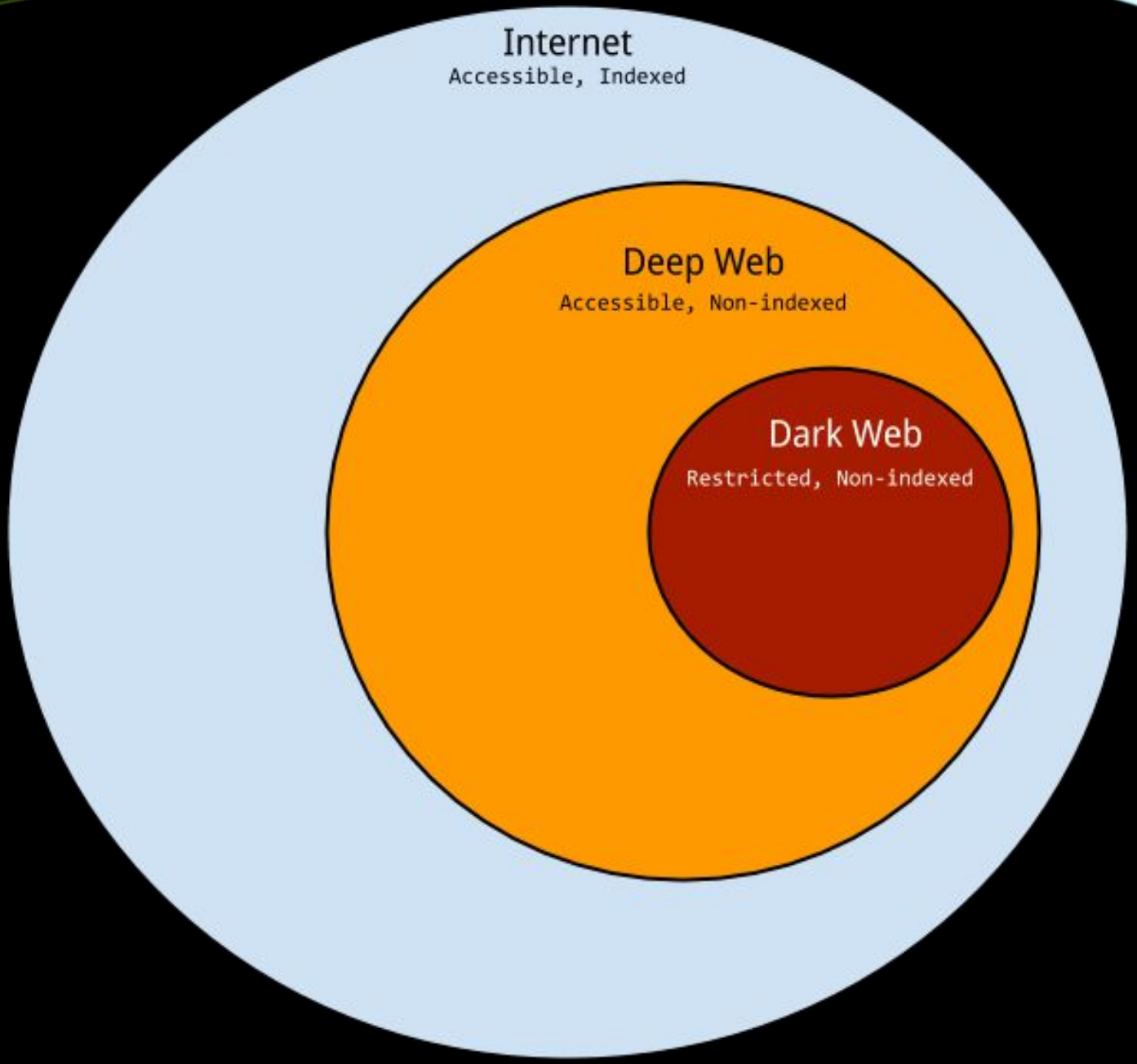
In order to access the Deep Web, you need to use a dedicated browser. TOR (The Onion Router) is the most commonly used, but other options such as I2P and Freenet offer an alternative solution.

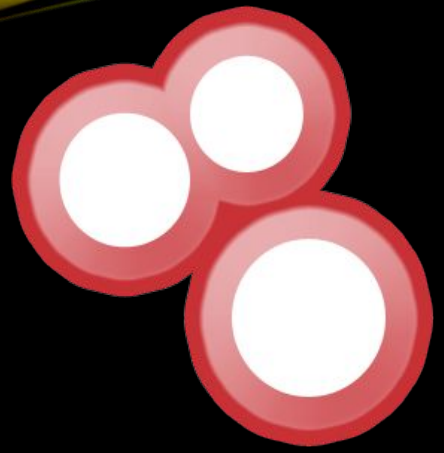
When using the Surface Web, you access data directly from the source.

**Surface Web/ Clearnet** – Normal websites (nsa.gov, 4chan.org)

**Deep Web** – Online databases, IoT devices(webcams etc)

**Dark Web/Darknet** – Tor Sites (.onion), I2P sites (.i2p)

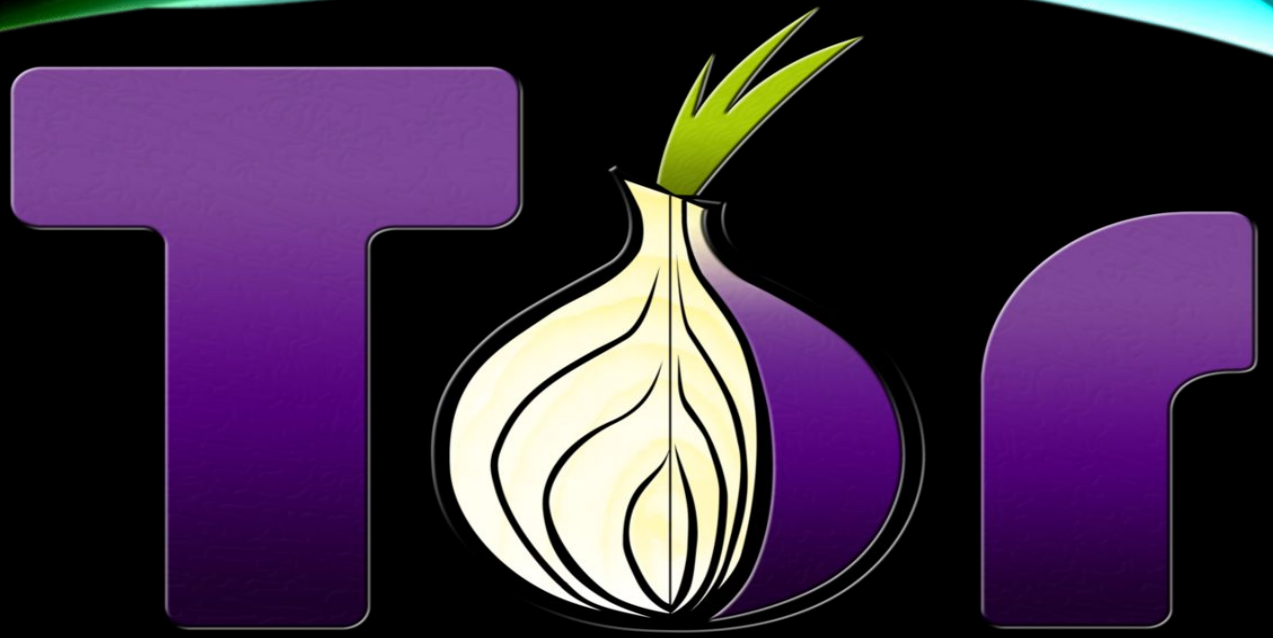




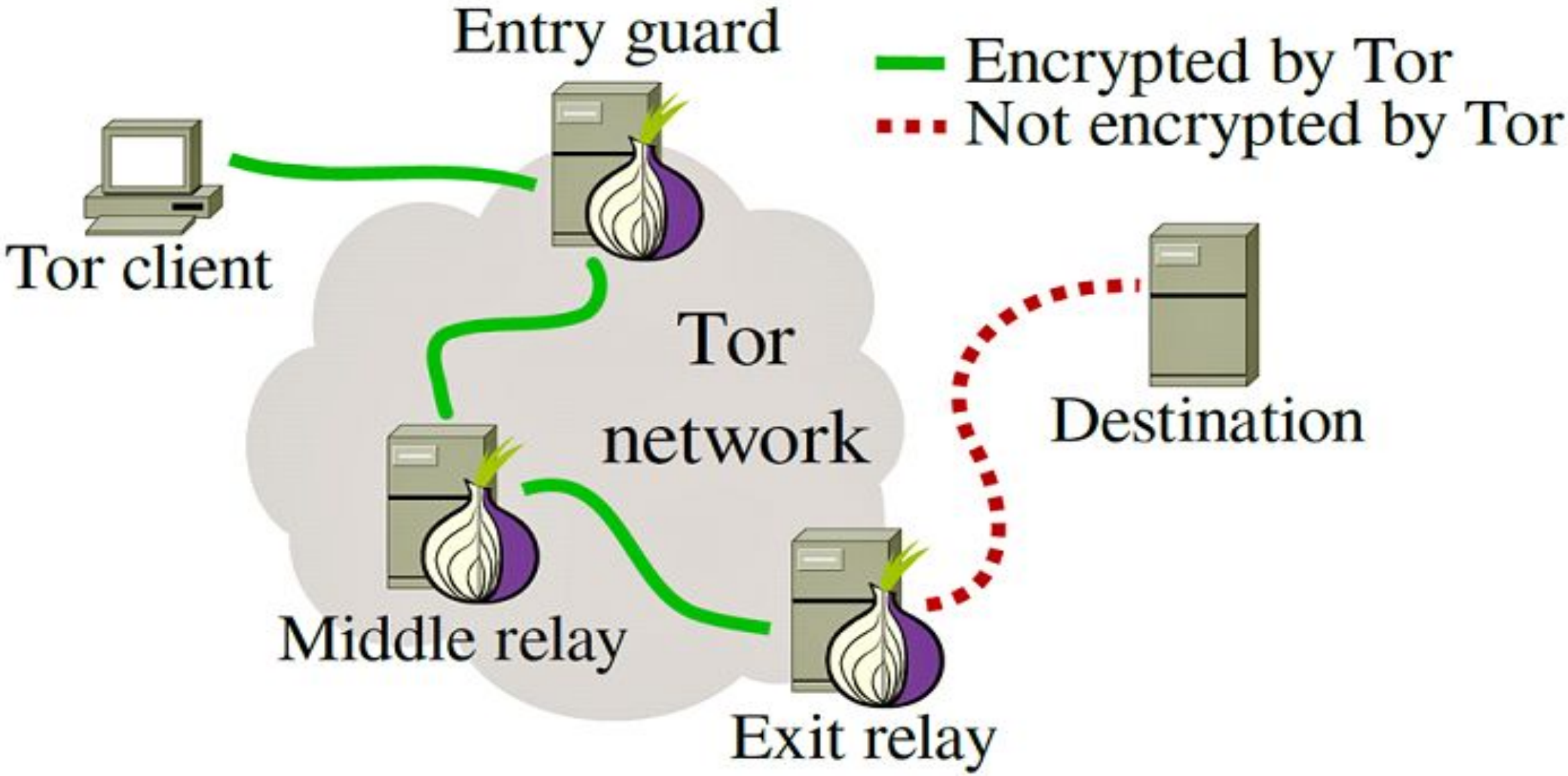
# SHODAN

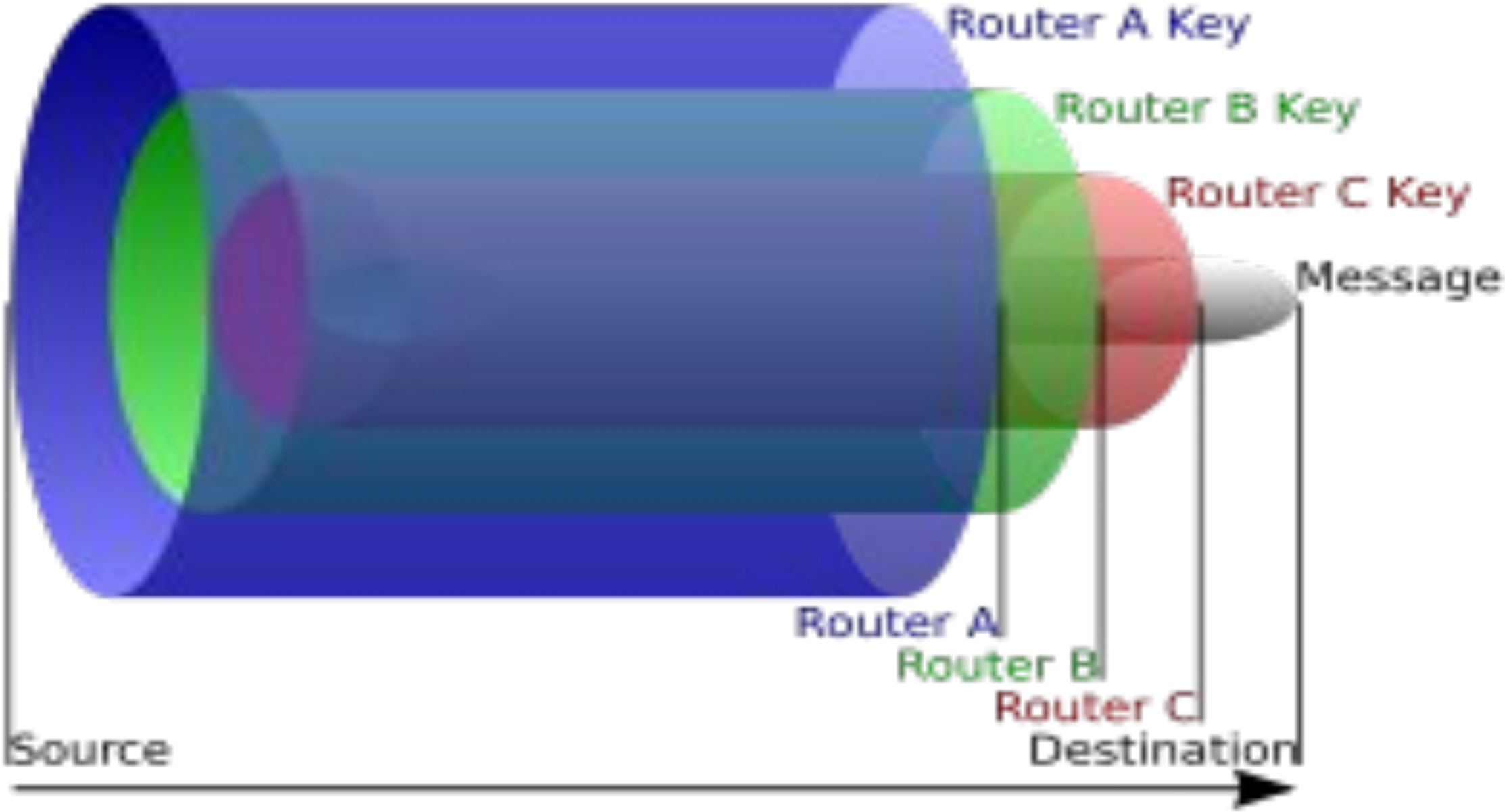
- *“A search engine for the Internet of Things”*
- *The “scariest search engine on the internet” as per CNN*
- *“Shodan has servers located around the world that crawl the Internet 24/7 to provide the latest Internet intelligence.”*

- Found on Shodan: routers, webcams, particle accelerators, nuclear plant control systems.




- Tor is a protocol, not a browser
- Stands for “The Onion Router”
- Circuit-switched
- NSA's favourite program


Entry guard
Encrypted by Tor
Not encrypted by Tor
Tor client
Tor
network
Destination
Middle relay
Exit relay


Router A Key
Router B Key
Router C Key
Message
Router A
Router B
Router C
Source
Destination

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.

NO GOOD! IT'S 4096-BIT RSA!

BLAST! OUR EVIL PLAN IS FOILED!

WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.

GOT IT.

# US Gov + TOR 4eva?

- Tor began in the US Naval Research Lab
  - One of original funders was DARPA :')
- 60% of budget still comes from US Gov
  - Especially US Dept of State
  - US gov believes in exporting Tor as a tool for evading censorship and surveillance: “to aid democracy advocates in authoritarian states"

# or US Gov + TOR 4NEVA

- FBI “Playpen” investigation
  - Seize server operating a hidden service offering CSAM
  - Operate server for weeks
  - Install malware using vulnerability in Tor browser
    - Old Metasploit exploit: “decloak”
    - Use Flash to initiate a regular internet connection, bypassing Tor and revealing user IP
  - Receive info from the computers of thousands of site visitors
  - ???
  - Profit

# or US Gov + TOR 4NEVA

- Department of Justice:
  - "A magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means; or (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts."
- “Remote access” = malware / spyware
- “Concealed through technological means” = using anonymity tools like TOR

# How does this relate to the “going dark” debate?

- “Going Dark” = prospect that most of the traffic and communications on the web will be encrypted
  - Refers to situations where law enforcement has the legal right but not the technological means to access a device
  - No encryption versus backdoors versus “hacking back”
- The DoJ has been pushing harder against encryption
  - Barr calls for backdoors
- EARN IT Act
  - Comply with a set of guidelines or lose your Section 230 immunity
  - So, what are the guidelines?
  - Pass the legislation and find out ;)

# What’s the deal?

- How can the US Government fund TOR and want to break encryption at the same time?
- Should TOR users be worried?
- If you were the government, would you fund TOR? Would you try to break it? Would you do both at the same time?