# Something Dark

## PEERING INTO THE DARK WEB

JEFF BEDSER, ITHREAT CYBER GROUP, SSAC

ICANN 60
ANNUAL GENERAL
ABU DHABI, UNITED ARAB EMIRATES
28 October–3 November 2017

# Warning…

- The dark web is filled with some awful things that cannot be unseen
- Ask yourself if this is really the job for you before starting
- Review the risk/reward as it may create other headaches

# Understanding The Underweb

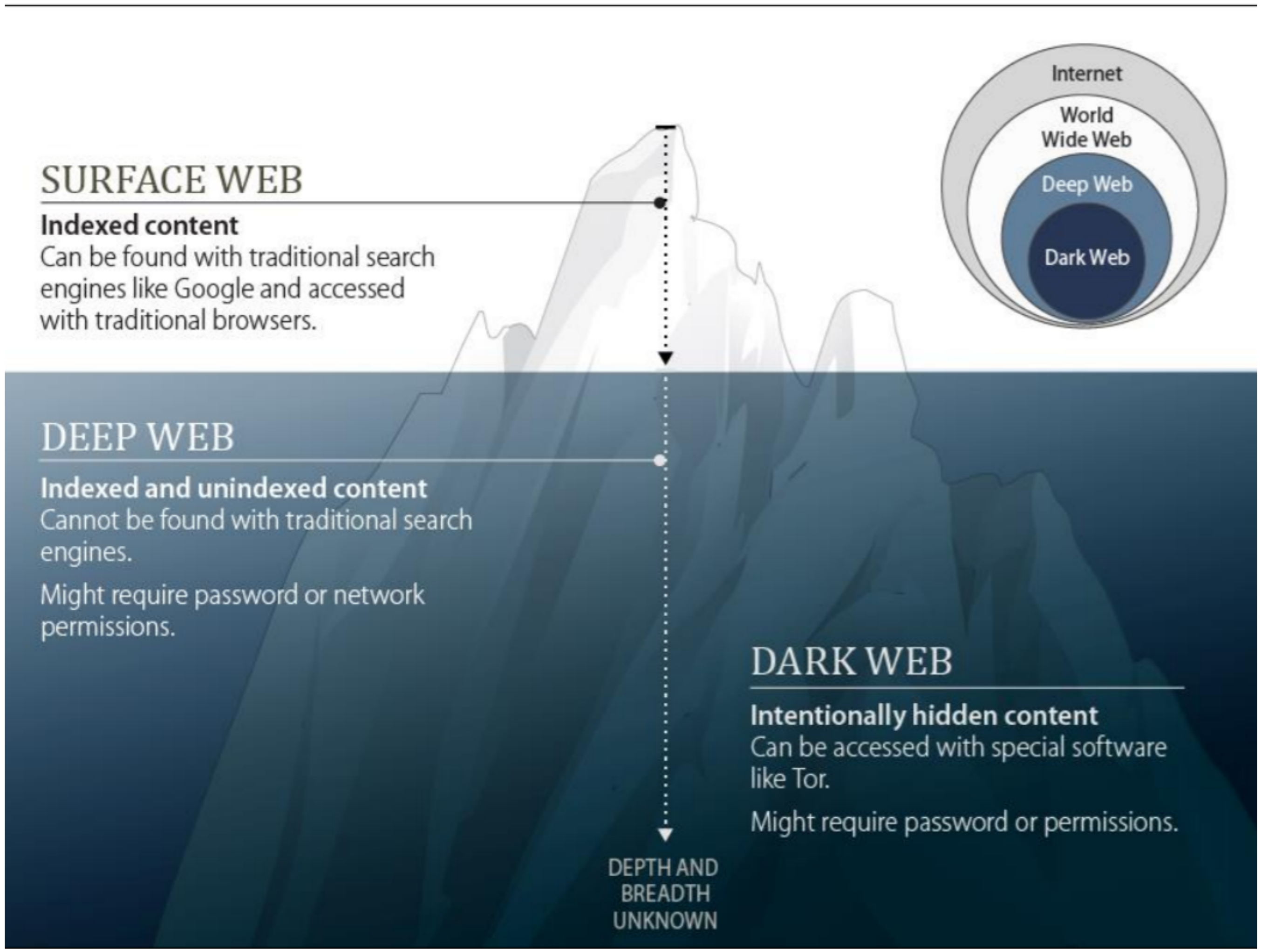
THE BASICS

# What is the “dark web”?

“…darknets which constitute the dark web include small, friend-to-friend peer-to-peer networks, as well as large, popular networks like Tor, Freenet, and I2P, operated by public organizations and individuals…

The Tor dark web may be referred to as onionland, a reference to the network's top level domain suffix .onion and the traffic anonymization technique of onion routing.”

-Wikipedia.org



SURFACE WEB

**Indexed content**
Can be found with traditional search engines like Google and accessed with traditional browsers.

DEEP WEB

**Indexed and unindexed content**
Cannot be found with traditional search engines.

Might require password or network permissions.

DARK WEB

**Intentionally hidden content**
Can be accessed with special software like Tor.

Might require password or permissions.

**Source:** Congressional Research Service (CRS).

**Note:** Proportions in the figure may not be to scale.

# Uses

## FOR BETTER…

- To circumvent government censorship
- To provide whistleblowers protection
- To avoid monitoring

## FOR WORSE…

- Enables sales of illegal firearms, drugs, counterfeits, etc.
- Shelters pedophile activities
- Hire hitmen, hackers, etc.
- Crime land…

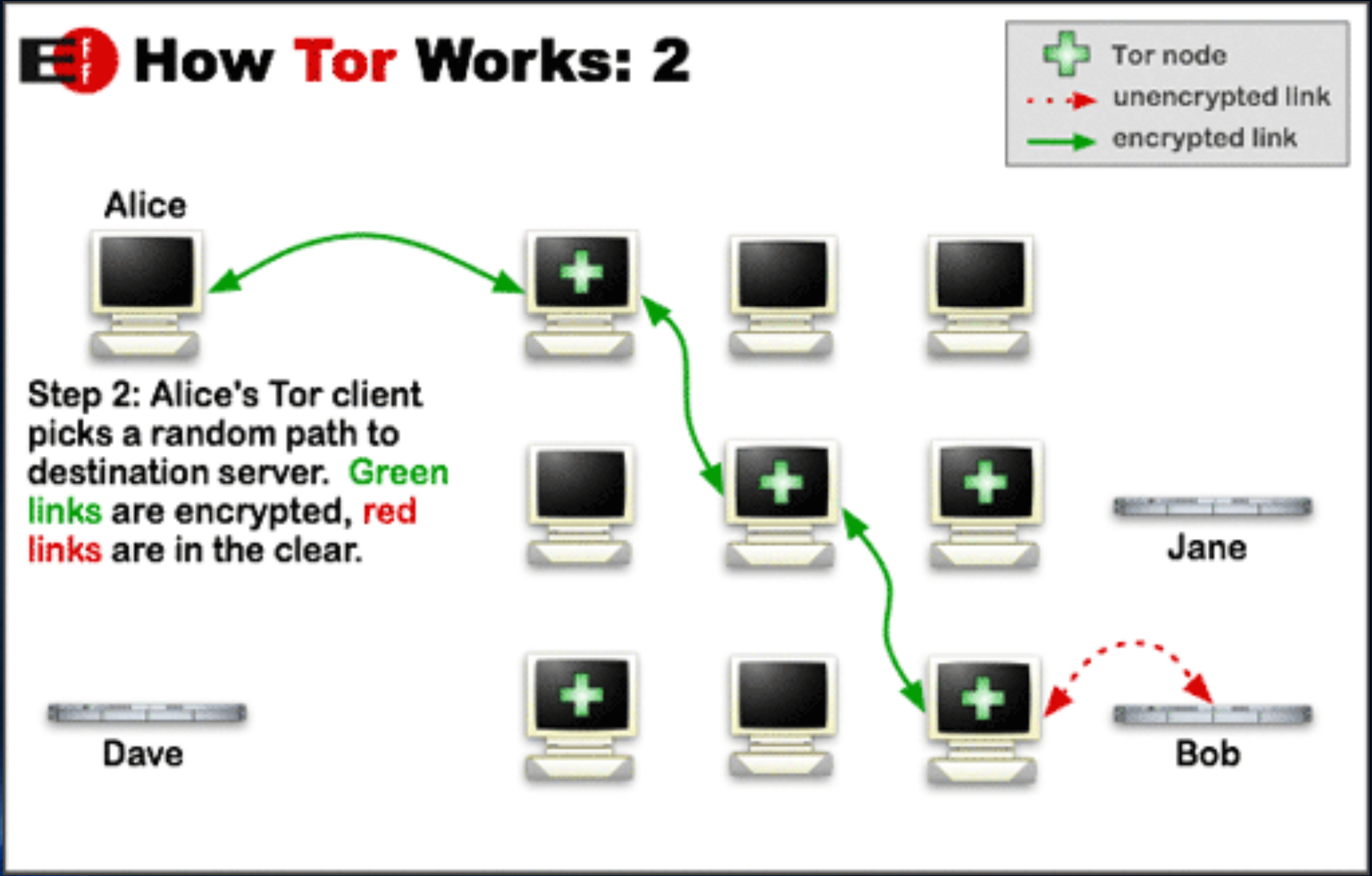
# Differences Between the Dark Web and Open Web

- Requires special software to access
- Resistant to indexing, not easily searched
- Indices are similar to Yahoo! in 1995 (Directories vs. Search Engine)
- Communications within the network are *always* encrypted
- Internet within an Internet

# Three Major Dark Webs

- The Onion Router (Tor) - Focus for this presentation
  - The biggest, most well known dark web.
  - Most Internet-like
- Invisible Internet Project (I2P)
  - Up and coming
  - Focuses on services (ie: instant messaging, email, websites, etc).
- Freenet
  - Distributed file sharing
  - Offers communications

# How Tor Works



How Tor Works: 2

Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

# About .onion Sites

- Use of Tor allows for the creation of .onion sites
- Can only be accessed when using Tor
- No master database of all .onion sites
- Domains are often randomly generated

# Realities for Investigations

- The network was designed to provide anonymity
- Best chance at finding and identifying someone is to get him/her off Tor and onto open web
- They don’t take PayPal, so be ready for crypto currency
- Have to be very careful to not use any personal information or accounts
- There’s no Google, so you may not find what you’re after
- Cultural distrust of others

# Review of What We Covered

- Discussed various dark web software and how Tor works
- Covered resources, limitations, expectations

# Question?
# Comments?

ICANN 60
ANNUAL GENERAL

ABU DHABI, UNITED ARAB EMIRATES
28 October–3 November 2017