Secure Communications

Tor and the Dark Web

MSc in Information Security & Digital Forensics.

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

What is the Dark Web?

Essentially the normal web (often called the **surface web**) is where most users spend most of their time browsing or surfing the internet. Facebook, google, twitter etc.

However there are large parts of the web that search engines such as google do not index (this is the **deep web**), they don't have the content of these sites included in their search results so normal users just searching for content will never be directed to these **hidden deep web** sites.

The **Dark Web** is a small sub-section of this **Deep Web,**

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

What is the Dark Web?

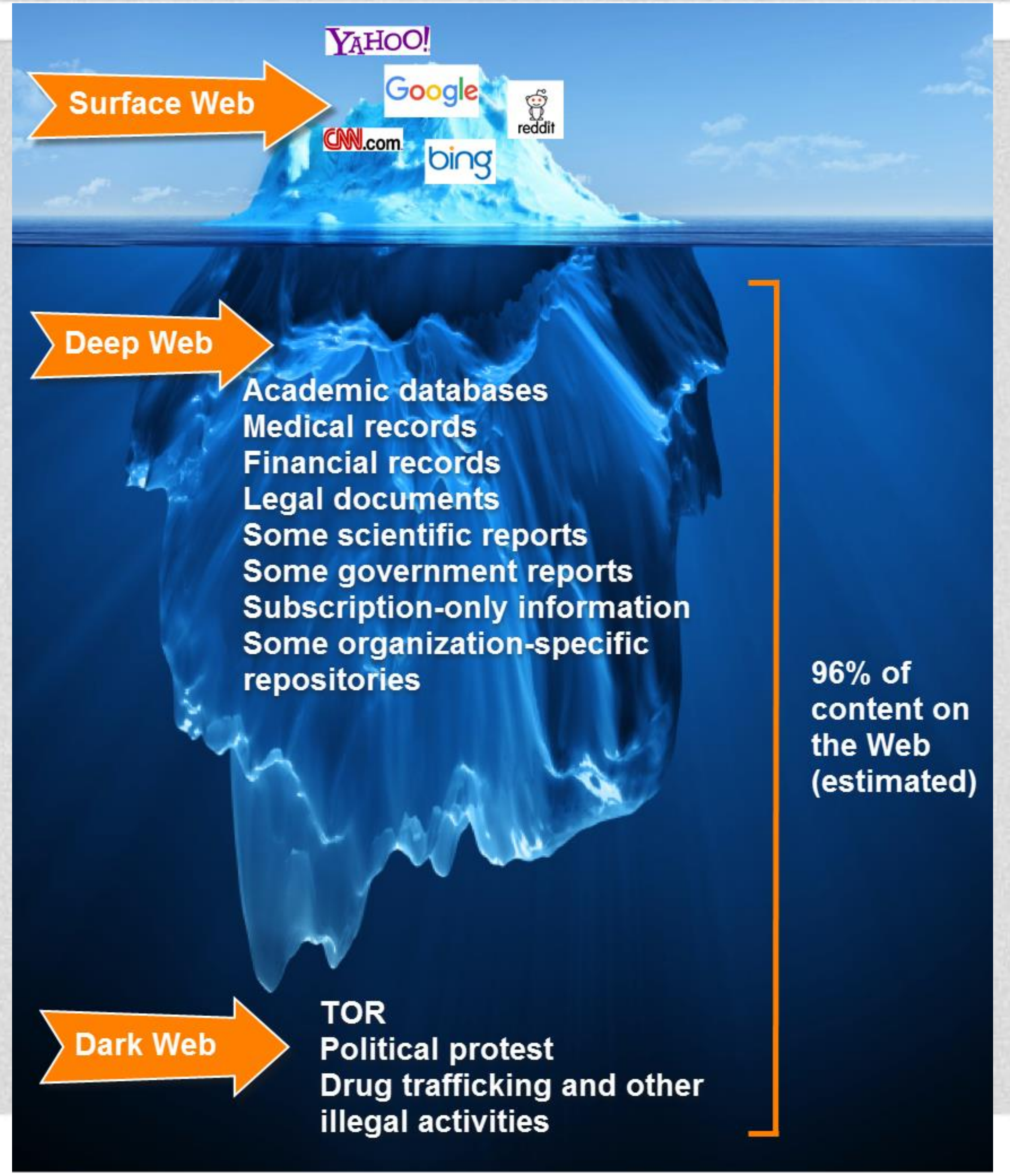
The dark web is the World Wide Web content that exists on darknets, overlay networks etc. which use the Internet but require specific software, configurations or authorization to access.

The dark web forms a small part of the deep web

although sometimes the term deep web is mistakenly used to refer specifically to the dark web.

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

What is the Dark Web?



Surface Web

Deep Web

Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription-only information
Some organization-specific repositories

96% of content on the Web (estimated)

Dark Web

TOR
Political protest
Drug trafficking and other illegal activities

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

How do we access the Dark Web?

The **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 organisations and individuals.

Users of the dark web refer to the regular web as Clearnet due to its unencrypted nature.

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.

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

How do we access the Dark Web?

So access to each different darknet, may require a different configuration or different software, depending on which part we wish to visit.

To access the Tor Dark web, we need to access the Tor network.

A common way of easily joining the tor network is to use bundled Tor packages that included pre-configured browser and tor software to allow the user connect to onionland.

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Are Tor, Dark web and Deep web illegal?

NO!

While technologies such as Tor, or access the Dark web or Deep web are not illegal. They do contain a lot of illegal activity and illegal content, just as the surface web itself also does.

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

The Tor Network

The Onion Router (TOR) is a project started by and still largely funded by the US government, initially through the Office of Naval Research and DARPA.

The ideal was to protect Naval personal in hostile areas to allow them connect without giving away their locations.

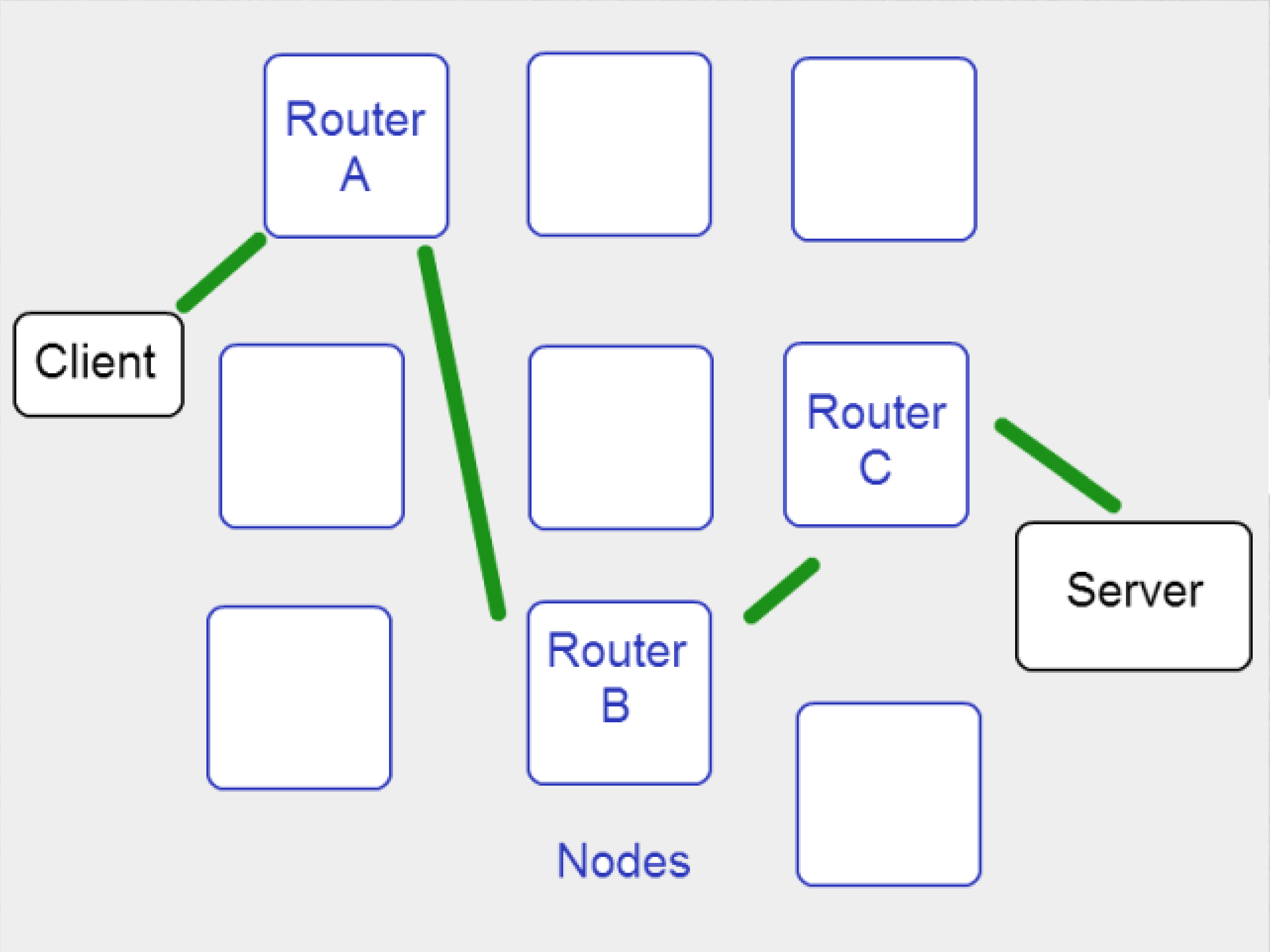
Users of the Tor network have their data encrypted and bounced throughout the Tor network before emerging at a random exit node. This exit node is the IP and location that the user appears to be connecting from, hence allowing users to hide their true IP and location.

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

How Tor Works

The Tor network is composed of volunteers who use their computers as "nodes."

When a Tor user visits a website, Tor creates a path through randomly assigned nodes that the packet will follow before reaching the server.

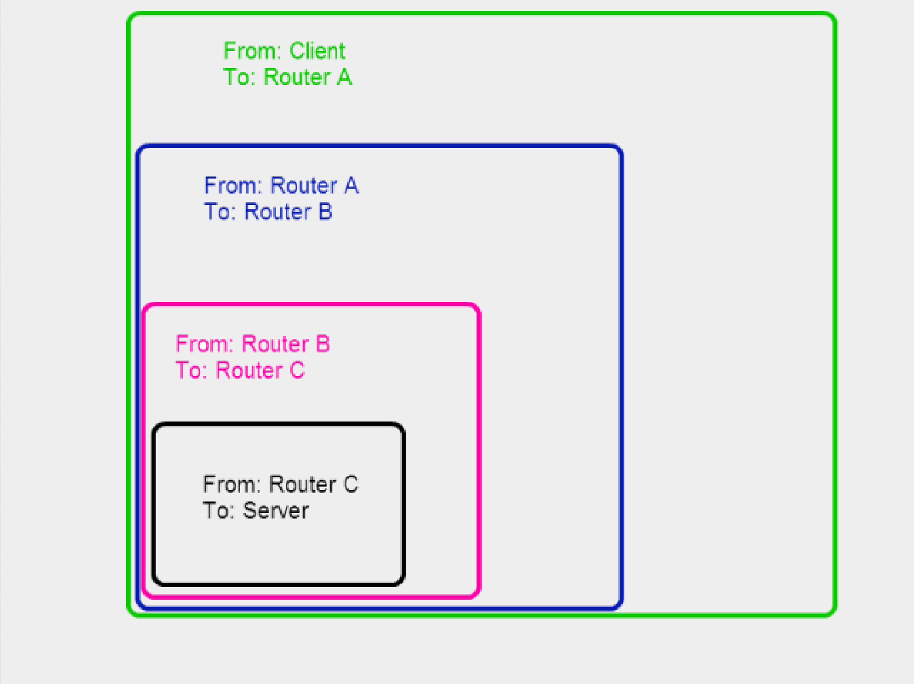


Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

How Tor Works

Normally, a packet will include the sender's address and the destination, not unlike a letter. When using Tor, the packet is wrapped in successive layers of packets, like a nesting doll.

Or like the layer of an onion.. Hence the name.



Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Limitations, hazards, and general safety

While Tor is useful for browsing the Web anonymously, it is not without problems. Naturally, it has drawn attention from government organisations like the NSA and FBI, who consider Tor a target of particular interest.

While the Tor network is quite secure from traffic analysis, the Tor browser, like any other, is vulnerable to attacks and exploits.

The Tor browser is, specifically, a modified version of Firefox, and as such is vulnerable to the same kinds of attacks as Firefox. By infecting an individual user's computer with malware, one can track their activity or access their device.

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Limitations, hazards, and general safety

Merely using Tor can make one an attractive target for the government, even if you only use the network for legal purposes.

Leaked NSA documents have revealed that they particularly focus on “dumb users,” people using Tor who may not be knowledgeable about Internet security and through whom the NSA can gain footholds in the Tor network.

Given access to enough nodes, the NSA (or anyone else) could observe packets traveling and shedding layers, from which point they could reconstruct the path travelled.

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Limitations, hazards, and general safety

First, it is important to disable most scripts and plugins, such as Flash, which can operate independently of browser setting and even transmit data about users.

Torrenting, a file-sharing process in which multiple people download different pieces of a file, sharing the bits they have already downloaded until the file is complete, is also something to be avoided. Torrent programs must broadcast your IP address so that peers can connect to you and share files, thwarting the entire point of onion routing.

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Limitations, hazards, and general safety

Finally, anyone browsing Tor’s hidden services should be careful about what they click on.

While many pages are socially acceptable or at the very least legal, such as sites for whistle blowers or Bitcoin exchanges, others are havens for disturbing, even criminal behaviour.

The cover of darkness helps rebels and monsters alike, and even naively stumbling onto a webpage containing illicit content could land you in legal trouble.

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie

Thank You !

End of Section

Mark Cummins
Institute of Technology Blanchardstown
Phone: +353 1-885-1156
Email: mark.cummins@itb.ie