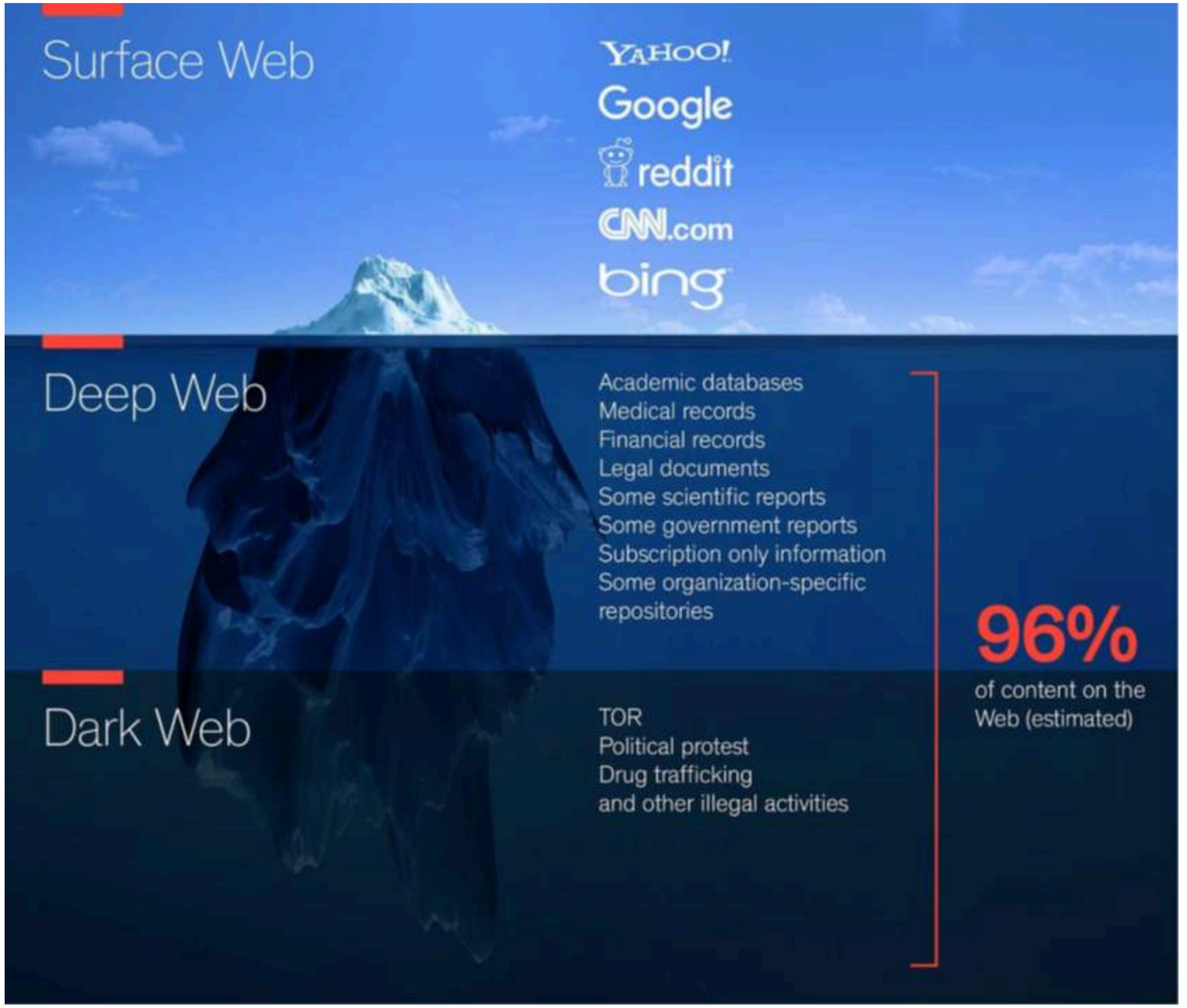
Dark web

Cyberboswachters

Tim Dams

The internet is an iceberg



The internet iceberg: surface web, deep web and dark web.

The three layers

Layer	Description	Access
Surface Web	Everything Google indexes	Regular browser
Deep Web	Databases, gated sites, private accounts	Login required
Dark Web	Anonymous, encrypted, not indexed	Special software (TOR)

> **Note**
>
> The **Deep Web** is much larger than the Surface Web — think of all the corporate databases, medical records, cloud storage, … that are never indexed by Google.
>
> The **Dark Web** is a small but notorious part of the Deep Web.

The internet is not really anonymous

On the regular internet you are **almost always traceable**:

- via IP address, cookies, provider logs, trackers, …
- some countries go much further: **full control** or **blacklisting** of sites
  - → China, Saudi Arabia, Iran, Egypt, North Korea, Cuba, …

> **Note**
>
> Being able to express your opinion under a **pseudonym** (*nom-de-plume*) is important for a democracy. Not everyone — and certainly not the government — needs to know what you legally do in your free time.
>
> Privacy vs investigation remains a **difficult balance**.

Characteristics of the Dark Web

Anonymous

Connections are routed through several intermediate servers → it is virtually impossible to trace who visits what.

Encrypted

All communication is strongly encrypted → third parties cannot eavesdrop.

Decentralised

No central authority → hard to censor or take down.

Good *and* bad use

Legitimate use

- Journalists communicating safely from dictatorships
- Whistleblowers (e.g. WikiLeaks sources)
- Activists in countries with censorship (China, Iran, North Korea)
- Anonymous freedom of expression

Criminal use

- Trade in drugs, weapons and stolen data
- Sale of credit card details
- “Rent-a-hacker” services
- Ransomware-as-a-Service platforms
- Child abuse material

Important

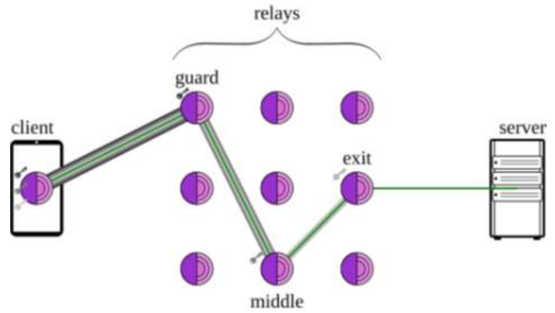
The Dark Web is **not illegal by definition** — but what you do on it can be.

Access via TOR

TOR = *The Onion Router*

- Your traffic is routed through **multiple relay servers** worldwide
- Each server only knows the previous and next hop → no single server knows the full path
- Dark web sites are recognisable by their `.onion` address

  → Only reachable through the TOR browser



Onion routing

TOR: drawbacks

Drawback	Explanation
Slow	Traffic passes several servers worldwide
Blocked	Some sites refuse TOR traffic
Firewalls	Corporate networks block TOR by default

> **Tip**
>
> Browsers such as **Brave** already integrate TOR — one click to surf anonymously.
>
> TOR also offers extra privacy on the **regular internet**, not just on the Dark Web.

Why should you know this?

As a cyber ranger you will inevitably encounter the Dark Web:

- Stolen data (passwords, credit cards, corporate secrets) is **traded** there
- Criminal tools and exploits are **for sale or rent**
- **Threat intelligence**: security teams monitor the Dark Web for early warnings
- Understanding **privacy technologies** like TOR helps with both defence and investigation

> ⚠ **Warning**
>
> **Never** visit the Dark Web from a work device or corporate network.
>
> Even passive browsing can expose you to illegal content or compromised servers.

Explore for yourself

Before you set off — check whether your IP is effectively protected:

- moanmyip.com/simple

A good **starting point** on the Dark Web itself:

- **The Hidden Wiki** → thehidden-wiki.org
  → collection of introduction points, search engines and interesting onions
- Extra list of onions: k00.fr/l1octcbo

> ⚠ **Warning**
>
> Go exploring, but **don’t click blindly through** — many sites are shady, illegal or compromised.