



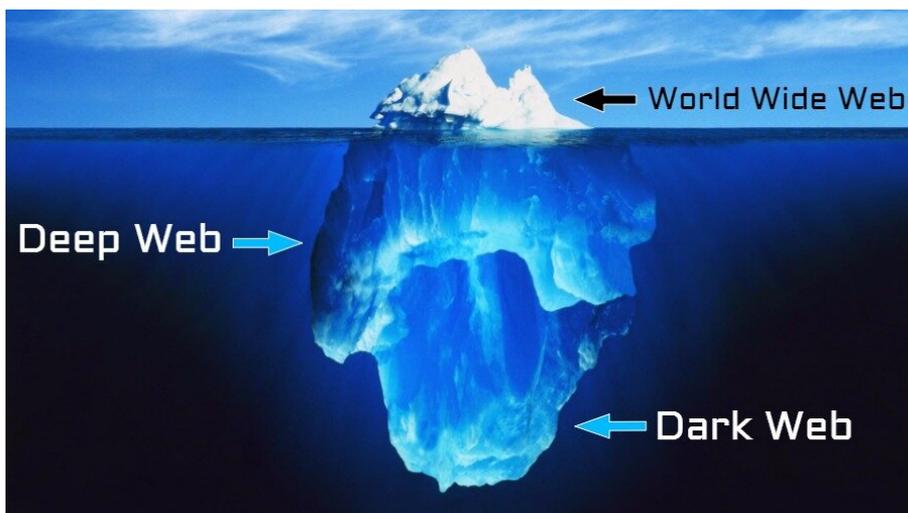
Dark Net

Introduction

- The darknet refers to encrypted networks on the Internet that are not indexed by search engines such as Google, Yahoo or Bing. It is a layer of the Internet accessible only by using special software like **Tor** (The Onion Router), or I2P (Invisible Internet Project).
- These are networks that are only available to a select group of people and not to the general Internet public, and only accessible via authorization, specific software and configurations.
- This includes harmless places such as academic databases and corporate sites, as well as those with shadier subjects such as black markets, fetish communities, and hacking and piracy.
- The terms "dark net" and "dark web" are occasionally used interchangeably, but with subtle differences in meaning. Dark net is a network built over the Internet whereas **dark web refers to websites on a darknet.**

Dark Net, Deep Web and Surface Web

- "Dark net" is commonly confused with "deep web." The deep web refers to unindexed sites which are unsearchable; in most cases, this is because those sites are protected by passwords.
- Part of the WWW (World Wide Web) which is not indexed by a search engine like Google is Deep Web and it about 500-600 times larger than the surface web.
- **Surface Web** -Also called the Visible Web, Indexed Web, Indexable Web or Lightnet -is that portion of the World Wide Web that is readily available to the general public and searchable with standard web search engines. It is the opposite of the deep web. It only constitutes 4-6% of the whole web.



Usefulness of DarkNet

- **To avoid Censorship:** Individuals within closed societies and facing extreme censorship can utilize the dark net to communicate with others outside of their society.

- **Anonymity and Secrecy:** Even individuals within open societies may have some interest in using the darknet, particularly as concerns about **government snooping** and data collection continue to grow worldwide.
- Useful for **whistleblowers and journalists** to maintain secrecy in communication and leaking and transferring information.

Concerns Regarding Darknet

- **Facilitates Illegal Activities :** A large portion of the activity which takes place on the dark net is illegal. The dark net offers a level of **identity security** that the surface net does not.
 - Dark net is the virtual equivalent of a black market.
 - Criminals looking to protect their identities in order to evade detection and capture are drawn to this aspect of the dark net. For that reason, it's unsurprising that a number of notable **hacks and data breaches** have been associated with the dark net in some way or another.
 - The relative impermeability of dark net has made it a major haven for drug dealers, arms traffickers, child pornography collectors and other criminals involved in financial and physical crimes so much so that one can buy anything from tigers to hand grenades to any kind of narcotic substances, provided the potential buyer finds the right website on the dark net.
 - One of the most famous examples of a dark network was the **Silk Road marketplace. Silk Road was a website used for the buying and selling of a variety of illegal items, including recreational drugs and weapons.** Although it was shut down by government authorities in 2013, it has spawned a number of copycat markets.
- Used by Activists and revolutionaries to organize themselves without fear of giving away their position to governments they oppose.
- Terrorists use dark net to provide information to fellow terrorists, to recruit and radicalize, to spread propaganda, raise funds, and to coordinate actions and attacks.
- Terrorists also use the dark net for illegal purchase of explosives and weapons, using virtual currencies like Bitcoin and other crypto-currencies.
- Security experts are claiming that hackers and fraudsters have started to offer access to SCADA and ICS systems via discussion forums on the dark web, potentially compromising vital infrastructure networks across the world.
 - SCADA systems are used to run facilities like nuclear power stations, oil refineries and chemical plants, so if cyber-criminals gained access to major networks, then the consequences could be lethal.

Way forward

- Given the increased importance of cryptocurrencies in the financial world, it's possible that dark nets will become more of a feature for everyday Internet users in the future. In the meantime, they may also still provide criminals with a means of eluding capture, although true anonymity is never guaranteed, even when using encryption of the type found in these networks.
- Governments across the world should strengthen their Cybersecurity Framework to deal with the threats posed by dark net. They must cooperate with each other regarding securing the Cyberspaces worldwide through intelligence, information, technology and expertise sharing.
- India should invest enough in research and development and training and capacity building of personnel in the field of Cybersecurity.
 - **Kerala Police Department's initiative, Cyberdome,** a premier facility dedicated to prevent cybercrime and mitigate cybersecurity threats to the State's critical information infrastructure, is a step in right direction which other concerned authorities across the nation can learn from.

[For Mind Map](#)

PDF Refernece URL: <https://www.drishtias.com/printpdf/dark-net>