# Mains Practice Question

**Q.** What do you understand by Darknet? Examine the issues and security concerns associated with it. (250 words)

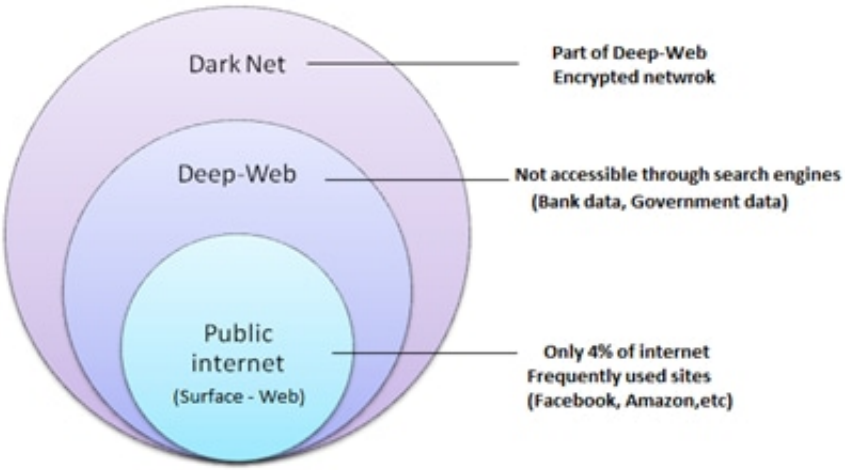
09 Oct, 2019 GS Paper 3 Science & Technology

## Approach

- Define Darknet and how it differs from other networks of internet.
- Mention the issues and concerns related to darknet.
- Give measures to effectively tackle the problem.

## Introduction

- Darknet is an encrypted layer of internet offering a high degree of anonymity and is accessible only by using special software like Tor (The Onion Router), or I2P, which stands for **Invisible Internet Project.**



*The three layers of internet*

//

## Body

### Issues related to Darknet

- **Misused for organized crime:** It is often misused for illegitimate activities over internet like pornography, terrorism, wildlife crimes, buying and selling of illegal or controlled substances, such as drugs, pharmaceuticals, weapons, etc. Thus it is infamously known as the **'underworld of the Internet'.**
- **Data Theft:** Hackers exploit security vulnerabilities of companies and may put up their data online for sale on the Darknet.

    - For ex: Food delivery firm Zomato's data was hacked by 'ethical hackers' in 2017 to highlight its cyber vulnerabilities.
- **Used against governments:** The network is also used by several activists against security forces to communicate without any government censorship.
    - For ex: The TOR network was used by activists during the Arab Spring.
- **Untraceability:** Dark Web operators transact in virtual currencies, the most popular being Bitcoins.
- **Challenges sovereignty of nations:** The transnational nature of organized crimes limits the capabilities of a single nation to curb the criminal activities.
- **Creates a market of illegal products:** It provides opportunity to maintain demand and supply of illegal products, thereby flourishing the markets of such products.

## Measures to tackle the problem

- **Institutional measures:** Developing cyber critical infrastructures for monitoring and effective control of Darknet activities.
    - Opening up of **Kerala Cyberdome** as a technological research and development centre by Kerala Police to crack down on the rising criminal activities over the Darknet is a welcome step.
- **Investing in cyber experts:** There is a need to invest in cyber experts for providing proper training and expertise to handle criminal activities over Darknet.
- **User Awareness and education:** User policies should be widely circulated covering acceptable and secure use of the online systems.
- **Investing in cyber-security:** Firms operating through online business should be encouraged to invest in cyber-security infrastructure to avoid any hacking of user data.
- **Enhancing international engagements:** Cyber crimes over Darket are spread beyond the national boundaries. Thus, there is a need to have coordination between investigating agencies of different countries. MoUs can be signed in this respect for mutual sharing of critical information.
- **Strict enforcement of laws:** Laws should be made more stringent and adapt with time to create a deterrent effect on criminals.
- **Physical monitoring:** Darknet only facilitates transaction and communication over the internet for illicit means. Investigating agencies should enhance capabilities to trace and detect crimes during physical delivery of illegal substances like drugs, wildlife animals, etc.

## Conclusion

Darknet is emerging as a challenge to the security and sovereignty of nations. Hence, there is an urgent need to invest in cyber physical infrastructures and enhance state's capabilities to tackle the menace of Darknet.