



**Civils Cafe**

IAS Study Circle

Best Online Coaching Institute

Lead by IAS, IPS, IPOS officers

# DARKNET

## MOST IMPORTANT NOTES FOR MAINS

SCAN TO EXPLORE



☎ 730 699 4905 ☎ 9048 073 888  
[www.thecivilscafeias.com](http://www.thecivilscafeias.com)

📘 thecivilscafeias  
📱 civilscafeiascc



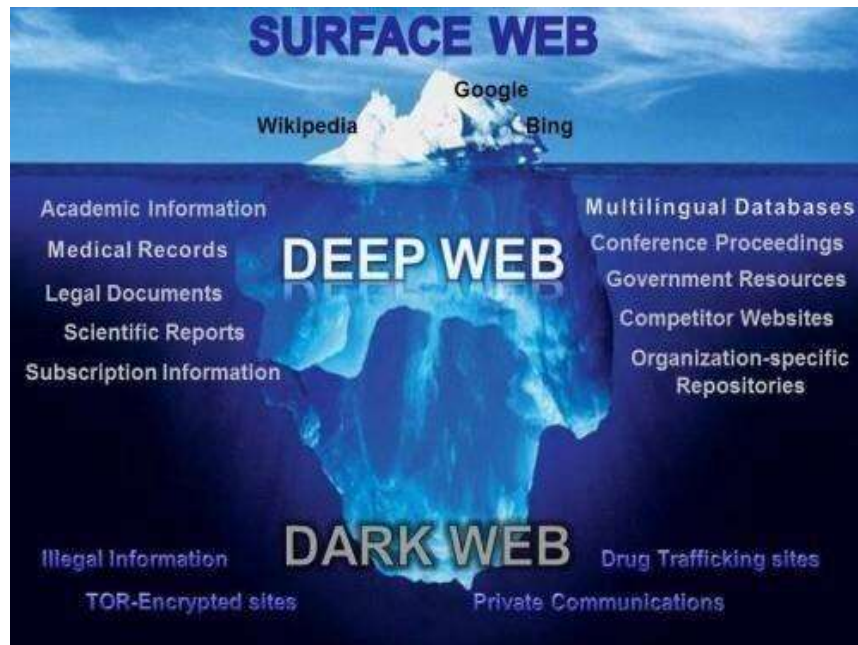
**GS 3 -INTERNAL SECURITY**  
**DARK NET**  
IAS Study Circle  
Have fun. Achieve dreams.

A dark net or darknet is an overlay network within the Internet that can only be accessed with specific software, configurations, or authorization, and often uses a unique customised communication protocol.

The darknet or dark web is a component of the greater "deep web," a network of encrypted Internet content that is not accessible via traditional search engines. They are accessed through specific software's such as The Onion Router (Tor) or The Invisible Internet Project (I2P).

### **Dark Net vs. Deep Web**

1. The dark net is part of the greater deep web. The deep web encompasses all unindexed sites that don't pop up when you do an Internet search.
2. The dark net is most often used for illegal activities such as black markets, illegal file sharing, and the exchanging of illegal goods or services.
  - The anonymity of the dark web attracts drug-dealers, hackers, and child pornography peddlers.
3. Not all activities associated with the deep web are nefarious. In most cases, these pages are not searchable through traditional channels because they are password-protected and require specific tools or authorization (like a log-in) in order to access them.
4. In order to hide exchanges in this hidden economy, bitcoin is often used as a currency.



- **Example of the Dark Net**

- One of the most famous examples of a darknet website was called the Silk Road marketplace. Silk Road was used for buying and selling a variety of illegal items, including recreational drugs and weapons.
- Silk Road was founded in 2011 and is often considered the first darknet market. Although it was shut down by the FBI in 2013, it has spawned a number of copycat markets.

### **Concerns Regarding Dark net**

#### **1. Threat to security-**

- **For communication:** Secret communication by the terrorists and other anti-national.

- **For purchase:** Terrorists also use the dark net for illegal purchase of explosives and weapons, using virtual currencies like Bitcoin and other crypto-currencies.
2. **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.
    - The Central Crime Branch of Bengaluru police, arrested 10 people who allegedly purchased drugs worth Rs 90 lakh through the darknet using bitcoins and sold them to students. Narcotic substances have been seized
  3. **Opaqueness:** 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.
  4. **Harm democracy:** Illegally gathered voter registration information using the dark web could be used to influence elections.
  5. **Threat to privacy-** This platform can be used illegally to encroach on the Right to Privacy of the others. In a study titled Cryptopolitik and the Darknet, it was highlighted that of the 2,723 websites on Darknet, 57 % host illicit content.
  6. **Anonymity:** The end-to-end encryption of dark net offers a high degree of anonymity and thus it is almost impossible to track.
  7. **Illegal business-** This can be used in drug smuggling, child pornography, which eventually affects the socio-economic fabric of the nation.

8. **Heaven of Hackers-** These platforms can be used by the hackers for cyber-related crimes like money laundering, phishing etc.

### Advantages

1. **Innovation and technology upgrade-** The unhindered flow of information promotes improved technology and innovation.
2. **To evade Censorship:** Individuals within closed societies and facing extreme censorship can utilise the dark net to communicate with others outside of their society.
3. **Useful for whistleblowers and journalists:** They can maintain secrecy in communication and leaking and transferring information.
  - Journalists seeking to interview citizens of repressive countries where communications are monitored might use the darknet.
  - The dark net can facilitate whistleblowing and news leaks, act as a tool to allow individuals to circumvent censorship networks, and can be used as a means of protecting political dissidents from reprisal.
4. **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.
5. **Interoperability of agencies-** To keep the communication between different security agencies in private.

### International scenario:

- The **International Telecommunication Union (ITU)** is a specialised agency within the United Nations which plays a leading role in the standardisation and development of telecommunications and cyber security issues.
- **Budapest Convention on Cybercrime:** It is an international treaty that seeks to address Internet and computer crime (cybercrime) by harmonising national laws, improving investigative techniques, and increasing cooperation among nations. It came into force on 1 July 2004. **India is not a signatory to this convention.**
- Internet Governance Forum (IGF): It brings together all stakeholders i.e., government, private sector and civil society on the Internet governance debate. It was first convened in October–November 2006.
- **Internet Corporation for Assigned Names and Numbers (ICANN):** It is a non-profit organisation responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the Internet, ensuring the network's stable and secure operation. It has its headquarters in Los Angeles, U.S.A.

### Indian Cyber security scenario

- **Information Technology Act, 2000:** The Information Technology Act, 2000 (amended in 2008) is the primary law for dealing with cybercrime and digital commerce in India.
- **National Cyber Security Policy, 2013:** The policy provides the vision and strategic direction to protect the national cyberspace.
- The **CERT-In** (Cyber Emergency Response Team – India): CERT-In has been operational since 2004. It is the national nodal agency for responding to computer security incidents as and when they occur.
- **Indian Cyber Crime Coordination Centre (I4C):** The Union Government has decided to set up I4C. It will be an apex coordination

centre to deal with cybercrimes.

- **Cyber Swachhta Kendra:** Launched in early 2017, the Cyber Swachhta Kendra provides a platform for users to analyse and clean their systems of various viruses, bots/ malware, Trojans, etc.
- **Cyber Surakshit Bharat:** Ministry of Electronics and Information Technology, launched the **Cyber Surakshit Bharat** initiative to spread awareness about cybercrime and building capacity for safety measures for **Chief Information Security Officers (CISOs)** and frontline IT staff across all government departments.
- The **Cyber Warrior Police Force(CWPF):** In 2018, the government announced its plans to introduce CWPF. It is proposed to be raised on lines of the Central Armed Police Force (CAPF).
- **Cyber-Crime Prevention against Women & Children' Scheme:** Implemented by the Ministry of Home Affairs, the scheme aims to prevent and reduce cyber-crimes against women and children

Governments across the world should strengthen their Cybersecurity Framework to deal with the threats posed by the darknet. 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.



**civils Cafe**  
IAS Study Circle  
Lead by IAS, IPS, IAS officers

# THE UNBEATABLES 2023

PRELIMS MAINS  
INTERVIEW BATCH

**ADMISSIONS OPEN**  
Mentored by Sasikanth  
Senthil IAS Ex

730 699 4905 9048 073 888  
www.thecivilscafeias.com

theivilscafeias  
civilscafeiasc

Copyright © by Civils Café IAS Study Circle. All rights are reserved. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of Civils Café IAS Study Circle.

© Civils Café IAS Study Circle.