UPSCprep Free Daily Answer Writing Initiative

Subject: GS 3

Syllabus: Internal Security

Questions

Q1. The "dark net" though has certain advantages, has turned into a hotbed of illegal activities posing multi-dimensional threats. In light of this statement, define 'darknet' and how does it pose a security challenge for India? (150 words)   10

Q2. Identify the opportunities and challenges that social media presents to the law enforcement agencies in India to counter national security threats. Also mention the steps taken to address the challenges? (250 words)   15

Model Structures

Q1. The "dark net" though has certain advantages, has turned into a hotbed of illegal activities posing multi-dimensional threats. In light of this statement, define 'darknet' and how does it pose a security challenge for India?   (10 marks)

Introduction:

● The **dark net or dark web is part of the deep web** and refers to encrypted networks on the Internet that are not indexed by search engines such as Google, Yahoo or Bing.

Main Body:

Importance of dark net

● It is used for various purposes such as free access to various resources (academic research papers), maintaining secrecy in communication and guarding against leaking and transferring information.

Feature 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: 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.

However, despite its advantages, the dark net also poses challenges to India's internal security. These are:

- **Illegal activities:** Activities such as-
    - Sale of drugs and firearms.
    - Fake currencies.
    - Child pornography.
    - Human trafficking etc.
    - Ex- 'darknet' narcotics operatives - uses darknet to ship psychotropic drugs.
- **Cyber fraud:**
    - Details of bank account holders, registered phone numbers etc. have been reported to be on sale over the darknet, which can lead to identity theft.
    - Ex- A database containing more than 4,50,000 payment card details of Indian banks has been uploaded on the darknet (Group-IB, a cyber security company).
- **Culpability of offence:** As identities remain anonymous, enforcement agencies are unable to trace those who use the darknet to engage in illegal activities.
- **Use of crypto currencies:** Deals done on the darknet are mostly through crypto currencies like Bitcoin.
- **Terrorism:** terrorist organizations like the Al Qaeda have turned to the dark net to spread propaganda, recruit supporters and protect the identities of supporters, raise funds etc.

Recent Developments:

- In light of these challenges, the Centre for Development of Advanced Computing **(CDAC) is working with CSIR on developing a darknet/network telescope**-based cyber security monitoring and interference framework.
- Similarly, **Kerala police has established a specialised darknet lab in Cyberdome** and some officers have been trained as dark net analysts to monitor these activities.

**Suggestion to counter these challenges:**(These points can be added in any such type of questions)

- Need to **strengthen Cybersecurity Framework eg-** removing loopholes of IT Act 2000.
- **Cooperate with like minded countries** regarding securing the Cyberspaces worldwide through intelligence, information, technology and expertise sharing.
- **Investing in research and development** and training and capacity building of personnel in the field of Cybersecurity.

Conclusion:

- Dark net had proved a menace for the growing world and safe haven for rogue elements. Need of the hour is to have a strict vigil so that citizens can enjoy their right to privacy.

Additional information:

- The content on the Internet can be divided into surface web and deep web. While surface web can be accessed using search engines, deep web cannot be indexed by search engines.
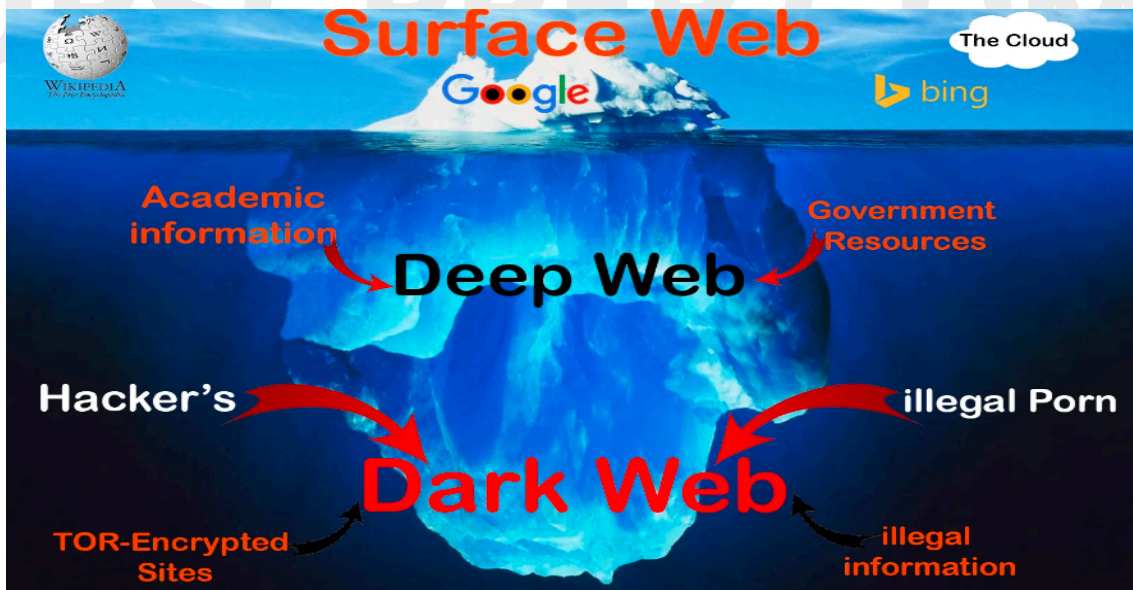
Q2. Identify the opportunities and challenges that social media presents to the law enforcement agencies in India to counter national security threats. Also mention the steps taken to address the challenges? **(15 marks)**

Introduction:

- With over 500 million active Internet users, social media usage in India is also on the rise. In this context,

Main Body:

Factors for rise in social media:

- Increasing internet penetration.
- Young demography.
- Digital initiatives.
- Local language.

Opportunities provided by Social Media:

- **Increased engagement with citizens:** enables increased engagement with citizens to build secure communities.
  - Information provided by Police using facebook, twitter etc.
- **Improved intelligence capabilities:** It offers real-time, first-hand information, which can be used for developing "actionable intelligence".
  - Identifying possible flash points of disturbances by using tools such as big data analysis etc. and sharing across agencies.
- **Enhanced preparedness:** by preparing standard operating procedures for times of emergency.

Challenges posed by Social Media:

- **Increased number of cyber-crimes:**
  - Sale of contraband items.
  - Selection of targets and victims.
  - Spreading malware, committing cyber frauds, impersonation, hacking etc.
  - Ex- incidents have been found of 'honey trapping' Indian soldiers, scientists etc.
- **Unregulated space for propaganda:** Terrorists and extremists are using social media to propagate their ideology and recruit members.
  - Ex- radicalisation done by ISIS and use of tremendous online following by Burhan Wani to strengthen Hizbul Mujahideen in Kashmir Valley.
- **Fast paced spread of misinformation:** Foreign entities are using social media as a weapon in their psychological operations to cause unimaginable disruptions.

- ○ Ex- Pakistan's ISI uploaded fake inflammatory videos, which triggered an exodus of people from North-eastern India staying in Bangalore and Pune.
- **Ineffective laws:** The Indian legal framework that includes IT Act, 2000 and National Cyber Security Policy, 2013 is both inadequate and faces limitations.
  - ○ Ex- denial by WhatsApp to help trace the origin of posts which led to lynching of 5 men in Maharashtra.
- **Democratic rights:** It is also difficult for India to strictly regulate social media because freedom of speech and privacy are fundamental rights.

Steps taken by India:

- **NETRA (NETwork TRaffic Analysis):** for real-time detection of suspicious "keywords" and "keyphrases" in internet content.
- **Social Media Labs:** to detect suspicious activity, and track mobilisation using social media for protests, and support domestic law enforcement.
- **Crime and Criminal Tracking Network System (CCTNS):** predictive policing i.e. real time tracking of internet data including social media data, for domestic law enforcement.

Way forward(Steps needed):

- **Institutionalise the blueprint** for a National Social Media Policy.
- Implement and institutionalise the Framework of Guidelines on social media engagement.
- Create awareness on the challenges posed by social media.
- Create organisational ecosystems, circumvent hierarchies, encourage outreach.
- Empower agencies, build talent, and use specialists.
- The National Cyber security Policy, 2014 must be regularly upgraded to tackle the upcoming challenges.
- A National Media Analytics Centre (NMAC) as proposed by the National Security Council.

Conclusion:

- The need of the hour is to strengthen the regulatory framework to utilise the maximum advantage of social media and render it ineffective for anti-social elements.

UPSCPREP.COM

Write
UNLIMITED

For 2 Months

Write answers to questions of your choice - We will evaluate them for you!

Course Link: **JOIN NOW**