Darknet: Anonymity, Crime and the Balance of Privacy

Cyber security, internal security and digital rights (General Studies-III) | News context: the India-Myanmar narcotics control talks of June 2026 and the darknet challenge in national coordination. | Published: 23 October 2026

Why in the News

Reports of the June 2026 meeting between India and Myanmar on narcotics control cooperation raised the question of trafficking through the darknet. The discussion spoke of the need for information sharing, coordinated action, control of chemicals and digital investigation.

The official information of the national narco-coordination meeting of 26 June also mentioned challenges such as darknet networks, crypto payments and supply through parcels. This makes clear that the internet and physical trafficking are not two entirely separate worlds. A deal may happen online, but delivering the goods and using the money need other networks too.

First understand: what is the darknet?
A darknet is a network built over the internet that requires special software, configuration or authorisation to access. The web services within it are also called the 'dark web'. In practice the two terms are often used together, but it is useful to understand the difference between the network and the content inside it.

The three contexts of the internet:

Term	Simple meaning	Is every use a crime?
Surface or clear web	Public content indexed by ordinary search engines	No; yet crime can take place on a public website too
Deep web	Content not indexed by ordinary search engines, such as data behind a private account	No; the private parts of email and online banking are ordinary examples
Dark web	Services inside special networks, which may have arrangements to hide identity or location	No; both legitimate privacy use and criminal misuse are possible

So 'not visible in search' and 'illegal' are not the same thing. Likewise, the whole deep web is not the dark web. Popular figures on what percentage of the internet bears which name often mix different measurements and definitions. Such ratios are not needed to understand the concept.

How does anonymity help?

Some networks route communication through several intermediate points, making it hard to identify a direct link between user and destination. The aim is that no single point has the full information. Tor is one such network; it should not be treated as a synonym for all darknets.

There is also a difference between reaching an ordinary website over Tor and connecting to a special service running inside that network. In Onion Services the communication stays within the network. What is explained here is the technical concept, not a process for reaching any website or market.

A privacy arrangement does not mean complete invisibility. Tor's own technical information notes that a capable party watching both ends of a communication can match timing and traffic patterns. Other information tied to identity can also matter in an investigation. So the claim that 'no one can ever be traced' is wrong.

Recognise legitimate uses:

Privacy can be important for journalists, researchers, sensitive sources and people facing surveillance or repression. Securing professional and personal communication is also a legitimate concern. The existence of anonymity technology does not by itself become proof of crime.

Yet the same technology can help criminals hide their identity. The difficulty for policy is to act against criminal activity without unnecessary harm to the privacy of legitimate users. Turning privacy protection and crime investigation into two opposing slogans is not a solution.

The digital-physical pairing in trafficking:

Contact and promotion: information on illegal goods does not spread only on the dark web. The open internet and social media can also be misused. So calling all digital trafficking darknet crime is not correct.

Payment: crypto-assets can be misused for illegal payments. But not all crypto transactions are illegal, and not every system provides complete anonymity. The link between the digital trail of a payment and a real identity is a separate investigative question.

Distribution: after a digital deal, the goods need a parcel, a courier or another physical arrangement. For this reason coordination among cyber specialists, financial investigation and ordinary narcotics control units can be necessary. Removing a website alone does not guarantee that the whole supply chain has ended.

Challenges of investigation:

Cross-border networks: the operator, the server, the payment and the buyer may be in different countries. Gathering evidence and taking action involve different laws and institutions. A declaration of international cooperation and actually obtaining evidence in a case are different stages.

Digital evidence: account, message or payment information must be preserved in a lawful manner. A name appearing in a screenshot alone does not prove a crime. The authenticity of the information, its link to the person concerned and the safe custody of evidence are important.

Institutional capacity: the team investigating the underlying trafficking offence also needs an understanding of digital processes. Leaving everything to a separate cyber cell can cause delay. Training, clear responsibility and a shared working method are necessary.

Shifting markets: when one platform shuts down, activity can move to another medium. So the closure of a single website is not a sufficient measure of long-term success. The effect on the network, the finances and the supply must also be seen.

Caution with statistics:

Cases registered, arrests, seizures and convictions are different indicators. They should not be treated as substitutes for one another. A rise in cases may be because crime rose, because detection improved, or both. Drawing conclusions from a number without context is risky.

Likewise, an estimate of markets from past years in an international study is not a direct figure for India's current situation. No comparison can be made without checking the sample, the time, the country and the unit of measurement. Illegal markets are hidden by nature, so uncertainty should be kept explicit.

A framework for better policy:

Crime-focused action: attention should be on specific offences such as the illegal trade in narcotics, fraud or data, and on their evidence. The mere use of a technology should not be made sufficient proof of guilt.

Shared investigation: lawful and secure information sharing among the agencies concerned. It is necessary to connect cyber, financial and physical supply evidence. Unnecessary duplication and unclear jurisdiction should be reduced.

Accountability: investigation should have statutory authorisation, a defined scope and oversight. Sensitive information should be used for a limited purpose. As technical power grows, accountability should grow too.

Health and support: the drugs problem is not solved by catching and seizing alone. Prevention, treatment, rehabilitation and a sensitive approach towards affected persons are also necessary. Criminal supply and the need for health support should be recognised as different things.

Conclusion:

The darknet should be seen neither as a mysterious and invincible world of crime, nor should its misuse be taken lightly. In a sound understanding, the technology, the activity and the evidence stay separate. India's challenge is to act effectively on the digital and physical networks of crime, while also protecting legitimate privacy and due process.

Mains Practice:

Question: "The challenge of darknet-related crime demands coordinated investigation of digital, financial and physical networks, going beyond bans on technology." Discuss with reference to privacy and due process. (250 words, 15 marks)

▼ See the answer outline
Introduction: give a brief definition of the darknet and its legitimate and illegal uses.

Main Body: explain the challenges of cross-border investigation, payments, parcels, digital evidence and institutional capacity. Suggest crime-focused action, authorised information sharing and oversight. Add the treatment and rehabilitation dimension.

Conclusion: emphasise keeping effective crime control together with privacy-respecting, accountable investigation.

Sources and limits

- June 2026: India-Myanmar talks and the darknet challenge
- 26 June 2026: official information on the NCORD meeting
- United Nations: the dark web, social media and drug supply
- Tor: technical limits of anonymity
- Technical properties of Onion Services
- Europol: legitimate use, crime and the coordination of investigation
- **Limits:** sources differ on darknet-activity figures; inconsistent numbers have not been given, and older reports have not been treated as proof of the 2026 India-level position. No claim is made about the percentage share of the internet or total cases. Not all cryptocurrency use is treated as illegal or fully anonymous. No instructions are given for accessing markets, buying, or evading investigation. The 3 June news is presented as a report of a bilateral meeting, not as the meeting's detailed record.

Prelims (facts) article on the same subject: Darknet, anonymity and privacy - key facts