

WRAP Exams · wrapexams.com

Prelims PYQ, Mains model answers, and copy evaluation. Write to the desk for this paper, a doubt, or the AI waitlist.

ask@wrapexams.com · +91 85951 84903 · wrapexams.com

Q20

Social media and encrypting messaging services pose a serious security challenge. What measures have been adopted at various levels to address the security implications of social media? Also suggest any other remedies to address the problem.

UPSC Civil Services Mains 2024 · GS III · 15 marks · Indian Economy

Indian Economy and issues relating to planning, mobilization of resources, growth, development and employment.

Core demand of the question

- State the security challenge from social media and encrypted messaging
- Describe measures already adopted at various levels
- Suggest further remedies that respect lawful speech and privacy

Revision summary

Social media amplifies incitement, deepfakes and fraud; encrypted messengers hide both family chat and terror planning.

- **India's tools:** IT Act (including 69/69A), IT Rules 2021, **CERT-In, I4C**, cyber police, poll-time takedowns and platform grievance officers.

Traceability versus **end-to-end encryption** remains the hard technical and legal knot.

- **Further remedies:** no universal backdoor, warrant-based access, cyber courts, forward limits, deepfake provenance, literacy and faster MLATs.

Security measures fail if they become a political speech filter rather than a riot-and-terror filter.

Introduction

Social media scales a rumour to a riot in an hour. **Encrypted messengers** hide a terror chat in the same app that hides a family grocer. That is the security challenge: **speed, anonymity, cross-border servers, and cryptography that works**. India has already written **rules, takedown powers and cyber police**. The remaining work is **capacity and literacy**, not only a louder demand for a **backdoor** that would break everyone's lock.

Body**The challenge**

Platforms amplify **communal incitement, fake mobilisation, deepfakes, radicalisation and financial fraud**. Hashtags can organise a **lynching or a stampede of panic**. Foreign **influence operations** ride the same rails. **End-to-end encryption** on WhatsApp-like services means even the company cannot read the payload; law enforcement then wants **traceability** of the first originator, which cryptographers say is hard to do without weakening the lock for all. **Closed groups** are where terror and child-abuse material also travel. **VPNs**

and offshore hosting frustrate a simple ISP block. The challenge is therefore **content, cash and command**, sitting on tools that also protect **journalists, dissenters and ordinary privacy**. Security with rights is not a slogan here; it is the design constraint.

- **Peg:** Open platforms (feeds) are an amplification problem; encrypted apps are an access-to-content problem.
- **Peg:** Deepfakes and UPI-linked phishing are the newer pair beside old communal forwards.

Measures already adopted

Statute: the **IT Act, 2000** (including sections on intermediaries and cyber offences) and the **Bharatiya Nyaya Sanhita** provisions on incitement, false information and terrorism-related speech, used with older IPC practice. **IT Rules, 2021** (and later amendments) impose **grievance officers, traceability language for significant messaging services, compliance with takedown orders, and a proposed government appeals body** that remains legally contested. **Section 69/69A** of the IT Act allow **interception, monitoring and blocking** under specified grounds. **CERT-In** directions on incident reporting, **I4C** (Indian Cyber Crime Coordination Centre), **State cyber police**, and the **National Security Council Secretariat / MHA** handle the operational layer. **RBI and I4C** have run **helplines (such as 1930)** against cyber financial crime. **Election Commission** and **MIB** issue takedown and silence-period directions in polls. At **platform level**, companies use **hash-matching, fact-check partners and India grievance offices**. At **international level**, India argues in **UN, G20 and FATF** spaces for cooperation against terror use of ICT, while remaining wary of a single Western speech code. Courts have both **upheld blocking** in some cases and **struck or stayed** overbroad official machinery when it looked like a censor board.

- **Peg:** IT Act plus 2021 Rules are the main domestic lever; **CERT-In** and **I4C** are the operational lever.
- **Peg:** Traceability versus encryption is the unresolved legal-technical fight inside those Rules.

Further remedies

Do not mandate a global decryption backdoor; it would be used by criminals against Indian firms and citizens as well. **Do build targeted lawful access** with a **court or senior independent warrant**, on metadata and, where a device is seized, on the endpoint. **Fast-track cyber courts** and **trained prosecutors** matter more than a new offence every year. **Platform design:** default **forward limits, labelling of political ads, provenance watermarks** for public-figure deepfakes, and **real-time crisis protocols** with SDMAs during riots. **Media and school literacy** so a forward is not treated as evidence. **Follow the money:** mule accounts and crypto off-ramps. **Mutual legal assistance** that actually returns a log from an Irish or Californian server in days, not years. **Community fact networks** in regional languages. **Protect whistle-blowers and journalists** so the same toolkit is not only a political takedown machine. The remedy set is **governance of speed**, not a fantasy of a fully transparent chat.

- **Peg:** Literacy plus warrant-based access plus faster MLATs is a rights-compatible package.
- **Peg:** A riot SOP that includes the platform liaison cell should be as normal as a police control room.

Flow diagram

Social feeds -> Rumour fraud radicalisation
Encrypted apps -> Rumour fraud radicalisation
IT Act and 2021 Rules Act and 2021 Rules -> Rumour fraud radicalisation
I4C CERT-In -> Rumour fraud radicalisation
Literacy warrants MLAT -> Rumour fraud radicalisation

Conclusion

Social media and encrypted apps scale rumour, fraud and terror planning. India already has the IT Act, 2021 Rules, **CERT-In** and **I4C**. Further remedies are literacy, warrants not backdoors, faster cross-border legal aid, and platform design that slows a riot without silencing a citizen.

Facts & figures

IT Act, 2000

Parent cyber statute, including intermediary liability, blocking (69A) and lawful interception (69).

IT Rules, 2021

Due-diligence rules for intermediaries, grievance systems, and contested traceability duties for significant messaging apps.

I4C

Indian Cyber Crime Coordination Centre under MHA, including public reporting channels for online crime.

CERT-In

Indian Computer Emergency Response Team; issues directions on incident reporting and cyber hygiene for firms.

End-to-end encryption

A design where only sender and recipient can read content; the service operator has no usable plaintext.

1930

The widely publicised helpline used for cyber financial fraud reporting in coordination with banks and police.

WRAP Exams · Write. Read. Analyse. Practice. · <https://wrapexams.com/upsc/mains-answers/gs-3/2024/social-media-and-encrypting-messaging-services-pose-a-serious-security-challenge-what-measures-have-been-adopted-at-various-levels-to-address-the-security-implications-of-social-media-also-suggest-any-other-remedies-to/> · ask@wrapexams.com · wrapexams.com