

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

Use of internet and social media by non-state actors for subversive activities is a major security concern. How have these been misused in the recent past? Suggest effective guidelines to curb the above threat.

UPSC Civil Services Mains 2016 · GS III · 12 marks · Indian Economy

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

Core demand of the question

- Show how non-State actors have used the internet and social media for subversion
- Give recent Indian and global examples of misuse
- Suggest legal, technical, and social guidelines that stay within a constitutional frame

Revision summary

Terror groups and riot organisers use social media to recruit, instruct, raise funds, and spread rumour.

The **2012 North-East exodus** rumours and ISIS-style online radicalisation are clear recent misuses.

Lawful blocking, **UAPA**, and IT Act intercept powers must stay narrow after the 66A judgment.

Platforms need log preservation and fast removal of unlawful content on a legal order.

Literacy, counter-speech, and financial tracking beat a long blanket internet shutdown.

Introduction

Phones and social platforms let a **non-State actor** - a terror group, a riot organiser, a hostile intelligence proxy, or a criminal gang - reach millions **without a radio station**. Recruitment, rumour, and live attack coordination now travel on the same apps as family chat. That is a major internal-security concern. The answer must name **how the tools were misused** and then offer **guidelines that target crime**, not the ordinary political speech the Supreme Court protected when it struck down **Section 66A** in **2015**.

Body**How the tools are misused**

- **Recruitment and radicalisation:** polished videos and private chat pull a youth from grievance to a module; **ISIS** and other groups industrialised this after 2014.
- **Instruction and operational security:** bomb-making notes, encryption, and dead-drop accounts replace a physical handler.
- **Rumour as a weapon:** fake images of violence can start a riot or a **flight of people**, as in the **2012 North-East exodus** rumours on SMS and social media.

- **Communal incitement:** forwarded clips, often old or foreign, timed for a procession or an election.
- **Fundraising:** online wallets, charities that are fronts, and publicity for kidnappings.
- **Live terror:** attackers on the move using phones for media and for handlers, as seen in several urban assaults worldwide and in Indian investigations after 26/11-era plots.
- **Cyber crime overlap:** phishing and malware to fund or to steal data from officials.
- **Separatist and insurgent propaganda** aimed at the diaspora and at local youth in Kashmir and the North-East.

Recent-past illustrations

- Global jihadist use of Twitter, YouTube, and Telegram-style channels for brand and for lone-wolf calls.
- Indian cases of modules busted with **Facebook and WhatsApp** trails; police often find the handler abroad.
- **Mass rumour** moving faster than a district's public-address system.
- Use of virtual private networks and foreign servers to sit outside easy summons.

Effective guidelines to curb the threat

- **Law with a narrow aim:** use **Unlawful Activities (Prevention) Act**, **Information Technology Act** blocking and interception powers (**sections 69 and 69A**), and ordinary IPC offences against incitement - with **judicial or high-level executive oversight** so the 66A-era vagueness does not return.
- **Intermediary rules:** time-bound removal of **unlawful content** on a lawful order; a local office and a compliance officer for large platforms; preservation of logs for investigation. Do not demand a general pre-censorship of all speech.
- **CERT-In, NTRO, and State cyber cells** that share indicators of compromise and of terror handles in hours, not months.
- **Open-source and undercover capability** in police, with language skills, instead of only a blocking request.
- **Financial trails:** freeze wallets and hawala that sit behind the page; involve the Financial Intelligence Unit.
- **Counter-speech:** official fact pages during a rumour spike; community voices that are trusted in that town, not only a Delhi press release.
- **Digital literacy** in schools and madrasas and through the police beat: how to spot a fake video, whom to call.
- **Crisis protocol:** when a riot clip spreads, **district magistrate, police, and platforms** on one call; targeted restriction if a court or statute allows, rather than a long, blanket shutdown that also blinds the honest citizen and the police.
- **International cooperation:** Budapest Convention-type mutual assistance, and requests to firms that store data abroad.
- **Prison and probation:** monitor known radicalisers' accounts; deradicalisation that is more than a locked SIM.
- **Protect encryption for the honest user** while using **targeted lawful intercept** on identified suspects - a mass backdoor is itself a security hole.

Flow diagram

Non-state actors -> Internet social media
Internet social media -> Recruit rumour finance ops
UAPA IT Act 69 69A -> Curb threat
Intermediary takedown logs -> Curb threat
Literacy counter-speech FIU -> Curb threat

Conclusion

Non-State actors have used the internet to recruit, to riot through rumour, to raise money, and to run operations. Indian rumour panics and global jihadist media are the recent proof. Guidelines that work are precise law, platform compliance, cyber fusion, money trails, counter-speech, and literacy - not a return to vague speech crimes or a permanent blackout. Curb the handler and the lie; keep the citizen online.

Facts & figures

Shreya Singhal 2015

Supreme Court struck down IT Act **section 66A** as vague; later cyber policy must not revive a catch-all speech offence.

IT Act **sections 69 and 69A**

Powers of interception and of blocking public information on specified grounds, to be used with procedure and oversight.

2012 North-East exodus

Rumour and threats on SMS and social media that pushed people from the North-East to leave some Indian cities.

CERT-In

Indian Computer Emergency Response Team: national node for cyber incidents and coordination with other agencies.

Unlawful Activities (Prevention) Act (UAPA)

Unlawful Activities (Prevention) Act: the principal anti-terror statute used against groups that also operate online.

WRAP Exams · Write. Read. Analyse. Practice. · <https://wrapexams.com/upsc/mains-answers/gs-3/2016/use-of-internet-and-social-media-by-non-state-actors-for-subversive-activities-is-a-major-security-concern-how-have-these-been-misused-in-the-recent-past-suggest-effective-guidelines-to-curb-the-above-threat/> · ask@wrapexams.com · wrapexams.com