Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.



MAINS MASTERY 2026 · GS PAPER III · QUESTION 9 · STUDENT EDITION

Fake News, Internal Security and IT Rules Amendments

THE QUESTION, AS SET IN UPSC CSE MAINS 2026

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

Directive: Explain how + Discuss | 10 marks | 150 words

Internal Security: disinformation and IT Rules

1 **PYQ Deep Decode** — Demand, hidden demand, answer design
2 **PYQ Intelligence** — 2013 to 2026: security and regulation
3 **Additional information** — Threats, amendments and safeguards
4 **Pitfalls and variations** — Six corrections and alternate demands
5 **The model answer** — 152 words, headed points, legal nuance
6 **Other ways to write it** — Threat matrix and chronological outline
7 **Quick recall** — Sixteen facts for revision
8 **Write it yourself** — Seven checks, sources and next steps

Guranchal Ma'am, Founder, UPSC Gurus · upscgurus.in

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

1 PYQ Deep Decode

Read the question the way the examiner set it: the demand, the hidden demand, the structure that follows from both, and how the answer should be presented, opened and closed.

1.1 The demand

The question combines **a security threat with a regulatory response**. First, it asks you to **explain how fake news and disinformation threaten Internal Security and Public Order in India**. The answer must trace the mechanisms through which false or manipulated information produces security consequences, rather than merely describe the existence of misinformation. Second, it asks you to **discuss the salient features of amendments to the Information Technology Rules, 2021**, showing how the amended provisions address those threats. The two parts must be connected: **threat, mechanism, regulatory response and significance**. The final judgement concerns whether combating disinformation can remain consistent with **freedom of expression, due process and independent public discourse**.

Words in the question	What they ask you to do	What goes wrong if you miss them
Explain how	Establish the causal chain: how false or manipulated information spreads, influences behaviour and produces identifiable security or public-order consequences.	Listing fake-news examples without explaining their effects.
fake news and disinformation	Focus on misleading information, particularly deliberate manipulation, fabricated evidence, impersonation and coordinated dissemination. Distinguish disinformation from mistaken sharing.	Equating all errors, criticism, satire and dissent with deliberate disinformation.
Internal Security	Examine threats to national security, social stability, counter-terrorism operations, institutional credibility and responses to hostile information operations.	Restricting the answer to interpersonal disputes or ordinary online rumours.
Public Order	Trace the consequences for communal harmony, local peace, crowd behaviour, panic and possible mobilisation towards violence.	Using Internal Security and Public Order interchangeably.
in Indian context	Anchor the explanation in India's linguistic diversity, communal sensitivities, messaging networks, elections, border tensions and documented Indian cases.	Writing a generic global essay on social-media misinformation.
In this regard, discuss	Connect the regulatory provisions to the threats identified; explain their purpose, operation and significance, not merely recite their names.	Producing two disconnected answers, one on misinformation and another on IT law.
salient features of amendments	Distinguish the 2022, 2023, 2025 and 2026 changes, identify the operative provisions and acknowledge the judicial invalidation of the contested 2023 government fact-checking provision.	Presenting the original 2021 Rules as amendments, omitting the 2026 changes, or treating a struck-down provision as enforceable law.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

THE DEMAND IN ONE LINE

Explain how disinformation becomes a threat to India's security and public order, then discuss the amended IT Rules through their specific platform duties, takedown procedures, grievance safeguards and synthetic-media provisions.

1.2 The hidden demand

The central tension is that **false information can harm security, but excessive governmental control over information can also undermine constitutional democracy**. An effective answer therefore does not assume that every disputed statement must be removed or that every restriction is censorship. It asks whether the regulatory response is **lawful, necessary, proportionate, transparent and open to challenge**.

This is not an abstract concern. The **6 April 2023 amendment** empowered the Central Government to specify a fact-checking unit for identifying certain information concerning its business. In **Kunal Kamra v. Union of India**, the Bombay High Court, by its majority judgement of **26 September 2024**, struck down the impugned amendment to Rule 3(1)(b)(v), finding constitutional and statutory defects. The Union's appeal was before the Supreme Court in 2026; the ruling did not abolish the **PIB's separate public fact-checking activity**.

Equally, the **2025 amendment** added procedural requirements for official takedown intimations, while the **2026 amendment** accelerated takedowns and introduced safeguards relating to synthetically generated information. The final part must therefore test the relationship between **regulatory speed, accountability and safeguards against wrongful suppression**.

The strongest answer distinguishes the harm, the legal instrument and the constitutional limit. These are three different questions.

Security problem	Regulatory instrument	The safeguard that matters
Deliberately misleading content	2022: Rule 3(1)(b)(v), intermediary due diligence concerning deceptive or intentionally misleading information.	Distinguish demonstrable falsehood and unlawful conduct from lawful opinion, criticism and satire.
Rapid circulation of unlawful content	2025 and 2026: Rule 3(1)(d), reasoned official intimations and the revised three-hour removal deadline.	Authorised officers, specified legal grounds, precise identification of content and periodic review.
AI-generated impersonation and deepfakes	2026: Rule 3(3) and additional Rule 4 duties concerning synthetic media.	Target unlawful synthetic content while allowing legitimate, disclosed and non-deceptive uses.
Erroneous or arbitrary moderation	2022: Rule 3A, Grievance Appellate Committees.	Accessible appeals, reasoned decisions and opportunities for effective redress.

WEAK

Fake news threatens national security. The Government should ban fake news and punish everyone spreading it under the IT Rules.

STRONG

Disinformation can convert fabricated evidence into communal mobilisation or hostile security narratives. The amended IT Rules strengthen intermediary due diligence, grievance appeals and rapid action against unlawful content, but the Bombay High Court's 2024 fact-checking judgement shows why the State's powers must remain constitutionally constrained.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

1.3 The structure

The question contains **two explicit demands in sequence**: threats to Internal Security and Public Order, followed by amendments to the IT Rules, 2021. The constitutional tension forms a **short final part**. The shares refer to the body between the introduction and conclusion; they are a teaching guide, not a UPSC rule.

Introduction	1. Security and public-order threats about two-fifths	2. Amendments to IT Rules about two-fifths	3. Rights and safeguards about one-fifth	Conclusion

Part 1 Threats posed by fake news and disinformation — about two-fifths

Internal Security	Hostile propaganda, cross-border information operations, radicalisation, manipulation of sensitive security developments and weakened institutional trust.
Public Order	Communal rumours, fabricated incidents, retaliatory mobilisation, panic and disturbances of local peace.
Amplification	Coordinated accounts, algorithmic recommendation, forwarding networks, emotional manipulation and convincing synthetic media.
Indian vulnerabilities	Religious and linguistic diversity, high-stakes elections, border tensions, localised rumours and the difficulty of rapid multilingual verification.

Part 2 Salient features of the amendments — about two-fifths

2022	Misleading information in Rule 3(1)(b)(v); constitutional-rights obligations; grievance timelines; Rule 3A appellate mechanism.
2023	Government-business fact-checking amendment; its relevant provision subsequently struck down by the Bombay High Court in 2024.
2025	Rule 3(1)(d): court orders or reasoned, authorised official intimations; senior-officer safeguards and review.
2026	Three-hour unlawful-content takedown; faster grievance redressal; synthetic-media identification, labelling, provenance and verification duties.

Part 3 Constitutional freedoms and procedural safeguards — about one-fifth

Constitutional test	Articles 14, 19(1)(a), 19(2) and 21; legality and proportionality.
Procedure	Reasoned orders, independent scrutiny, appeals, transparency and protection from indiscriminate censorship.
Beyond removal	Independent verification, media literacy, credible public communication and platform accountability.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

1.4 How to present it

The first demand is **causal**, while the second is **legal and chronological**. For a 150-word answer, the most efficient form is **three numbered parts with compact headed points**. Part 1 traces the harm through brief examples; Part 2 names the operative amendments by year and provision; Part 3 gives a reasoned constitutional qualification. A short flow showing how disinformation becomes a security consequence is useful for understanding, but an elaborate diagram would consume space needed for the legal amendments.

Form	Fit here	Reason
Three headed parts with numbered or labelled points	**Best**	Preserves the question's order, separates two distinct demands and leaves room for constitutional judgement.
Threat-to-rule matrix	Good	Connects each security concern to a regulatory response; demands careful treatment of judicially invalidated provisions.
Long chronological account of IT Rules	Weak	Turns the answer into a legal history and neglects the first explicit demand.
General essay on fake news	Weak	Misses the amendments, the dates and the rule-specific obligations.

1.5 The introduction and the conclusion

The introduction serves the whole question. It links the speed and credibility of digital disinformation to security and public-order threats, while recognising that intermediary regulation is the policy response. It should not begin with a lengthy definition of fake news or an unrelated statistic.

The conclusion settles the demand. It judges the effectiveness of the amended framework against the constitutional requirement that action be proportionate, reviewable and supported by trustworthy public communication. Protecting public order and protecting lawful expression must be treated as complementary obligations.

2 PYQ Intelligence 2013 to 2026

Why misinformation and intermediary regulation were topical before the 2026 examination, how UPSC's earlier cyber-security questions developed, and which connected areas deserve preparation.

2.1 Why the subject was topical in 2026

Between 2022 and August 2026, India witnessed **regulatory amendments, judicial scrutiny and documented misinformation affecting elections, communal harmony and national-security communication**. The emergence of accessible generative AI intensified concern about convincing synthetic audio and video. The 2026 Mains GS Paper III examination was held on **23 August 2026**. UPSC does not disclose why it chooses a question, so these developments are **context, not evidence of its intention**. All developments in the table predate that examination.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

When	What happened	Why it matters for this question
25 February 2021	MeitY notified the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**, G.S.R. 139(E), under the Information Technology Act, 2000. The Rules established intermediary due diligence, grievance mechanisms and additional duties for significant social media intermediaries; Part III addressed digital-media publishers.	The parent framework that subsequent amendments modify.
23 to 26 September 2022	The Ministry of Information and Broadcasting issued orders on 23 September to block **45 YouTube videos from 10 channels**, announced on 26 September. The Ministry said the material included fake news and morphed videos that could encourage communal hatred and disturb public order; the videos had over **1.3 crore cumulative views**.	A documented example of the connection between manipulated online material and public-order concerns.
28 October 2022	MeitY notified **G.S.R. 794(E)**. The amendments revised Rule 3(1)(b), expressly covering misleading origins and intentionally communicated misinformation or patently false information, and inserted **Rule 3A** for Grievance Appellate Committees. They also strengthened user-rights obligations and grievance redressal.	The first major amendment directly relevant to the question's disinformation and accountability demands.
27 January 2023	The Central Government established **three Grievance Appellate Committees** under Rule 3A. They provide an online mechanism for appealing decisions of intermediaries' Grievance Officers.	The distinction between an intermediary's first decision and an administrative appeal against that decision.
6 April 2023	MeitY notified **G.S.R. 275(E)**, including amendments on online gaming and a provision allowing a government-specified fact-checking unit to identify information concerning the business of the Central Government as fake, false or misleading.	The origin of the later constitutional controversy concerning governmental authority to determine disputed truth.
7 November 2023	MeitY issued an **advisory** to significant social media intermediaries urging due diligence concerning misinformation and deepfakes, prompt action on complaints and compliance with the IT Rules. The advisory referred to removal within the then-applicable 36-hour timeline.	Shows the policy response to synthetic-media harms before the specific 2026 rules.
2 April 2024	The **Election Commission of India** launched its **Myth vs Reality Register** to counter false claims about electoral rolls, EVMs, VVPATs and election procedures.	Misinformation can undermine confidence in electoral institutions without necessarily causing immediate street violence.
6 May 2024	The ECI directed political parties and their representatives to refrain from disseminating deepfakes and misinformation during campaigning. Parties were directed to remove identified offending content within **three hours** of its coming to their notice.	An election-specific ECI direction; it must not be confused with the general intermediary takedown deadline introduced in February 2026.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

When	What happened	Why it matters for this question
26 September 2024	Following a divided judgement and a third-judge opinion, the **Bombay High Court**, in **Kunal Kamra v. Union of India**, struck down the 2023 amendment to **Rule 3(1)(b)(v)** concerning the government-specified fact-checking unit. The majority held it unconstitutional and beyond the enabling statute.	The essential caveat: not every notified amendment remains enforceable. Freedom of expression and statutory limits are part of the answer.
7 to 10 May 2025	During **Operation Sindoor**, the Government reported widespread false claims, manipulated videos and hostile propaganda. Its subsequent account described official briefings, coordinated rebuttals and blocking directions covering **more than 1,400 URLs** during the operation.	A direct Indian illustration of disinformation as part of a national-security information environment. These are government-reported actions, not an independently established measure of campaign effectiveness.
22 October 2025 Effective 15 November	MeitY notified **G.S.R. 775(E)**, substituting Rule 3(1)(d). The amendment specified how intermediaries acquire legally relevant actual knowledge through competent-court orders or **reasoned intimations from duly authorised officials**, with senior-officer thresholds, identification of the unlawful content and monthly review. At this stage the specified removal period remained **36 hours**.	Introduced procedural checks on official removal directions before the accelerated 2026 deadline.
10 February 2026 Effective 20 February	MeitY notified **G.S.R. 120(E)**, addressing **synthetically generated information (SGI)**. It introduced a dedicated Rule 3(3), strengthened labelling and provenance requirements, added obligations for significant social media intermediaries, and reduced the Rule 3(1)(d) takedown period from **36 hours to three hours**. Certain grievance timelines were also shortened.	The most recent major pre-examination amendment directly relevant to deepfakes, unlawful content and rapid platform responses.
19 April 2026	During Assembly elections in Assam, Kerala, Tamil Nadu, Puducherry and West Bengal, the ECI reported action concerning **more than 11,000 social-media posts or URLs** identified since 15 March, including removals, FIRs, clarifications and rebuttals. The ECI reiterated obligations concerning misleading AI-generated content and election-related public order.	Evidence that election monitoring combines takedown requests with enforcement and corrective communication; the figure does not mean 11,000 items were all removed.

2.2 The skill UPSC keeps testing

UPSC's questions have progressed from recognising **the security implications of social networks** in 2013, to digital radicalisation, misuse by non-state actors, cybercrime and cross-border attacks, and then to the security implications of social media and encrypted messaging. The 2026 question adds a distinct demand: **explain information disorder as a security threat and discuss the amended legal duties imposed on digital intermediaries**. The questions below reproduce the recorded UPSC wording, including punctuation and spacing.

Year	The question as UPSC set it	What it asked of you	What changed in 2026
2013 GS III, Q22	What are social networking sites and what security implications do these sites present ?	Identify social networks and their security implications.	From broad security risks to the specific mechanism of disinformation and platform regulation.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

Year	The question as UPSC set it	What it asked of you	What changed in 2026
2015 GS III, Q18	Religious indoctrination via digital media has resulted in Indian youth joining the ISIS. What is ISIS and its mission ? How can ISIS be dangerous for the internal security of our country ?	Digital indoctrination, radicalisation and internal security.	Disinformation as a possible enabler of radicalisation, alongside communal mobilisation and hostile propaganda.
2016 GS III, 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.	Non-state misuse of digital platforms and regulatory remedies.	A direct regulatory successor, but now with specified amendments and judicial limitations.
2019 GS III, Q10	What is CyberDome Project? Explain how it can be useful in controlling internet crimes in India.	An institutional response to internet-enabled crime.	From a policing initiative to nationally applicable intermediary due diligence.
2020 GS III, Q9	Discuss different types of cyber crimes and measures required to be taken to fight the menace.	Classify online offences and match them with countermeasures.	Distinguish unlawful content and associated offences from misinformation that is not independently criminal.
2021 GS III, Q10	Keeping in view India's internal security, analyse the impact of cross-border cyber attacks. Also discuss defensive measures against these sophisticated attacks.	Cross-border threats and defensive capabilities.	Information operations and manipulated narratives become the focal threat, rather than network intrusion.
2022 GS III, Q19	What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy.	Cyber-security architecture and strategic adequacy.	Specific legal provisions replace the wider question of national cyber-security strategy.
2024 GS III, 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.	Measures against platform and encrypted-messaging security risks.	Amendment chronology, synthetic media, statutory deadlines and constitutional safeguards become explicit.

Also related, verbatim: 2017 GS III, Q9: "Discuss the potential threats of Cyber attack and the security framework to prevent it." 2023 GS III, Q19: "What are the internal security challenges being faced by India? Give out the role of Central Intelligence and Investigative Agencies tasked to counter such threats." 2026 GS III, Q16: "What is agentic Artificial Intelligence (AI)? Explain its working. Describe its applications with suitable examples. Discuss the advantages, risks and challenges associated with agentic AI systems."

CARRY THIS METHOD TO ANY "DIGITAL THREAT AND REGULATION" QUESTION

1. **Classify** the threat precisely: misinformation, disinformation, cybercrime or hostile information operations.
2. **Trace** the mechanism from online activity to a concrete harm.
3. **Separate** national security, public order, individual harm and electoral integrity.
4. **Name** the applicable legal provisions and explain what each changes.
5. **Check** chronology, commencement dates, judicial decisions and the actual scope of enforcement.
6. **Conclude** with the constitutional and institutional safeguards that make regulation legitimate.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

2.3 What to prepare next

LAWS, INSTITUTIONS AND JUDGEMENTS

IT Act, 2000	Section 69A, blocking powers; Section 79, conditional intermediary protection; Sections 66C and 66D, identity theft and cheating by personation using a computer resource.
IT Rules, 2021	Original platform due diligence, grievance officers, significant social media intermediary obligations and digital-media publisher Code of Ethics.
2022 amendment	Rule 3(1)(b)(v); Rule 3A; user rights and grievance procedures. Gazette G.S.R. 794(E), 28 October 2022.
2023 amendment and judicial review	G.S.R. 275(E), 6 April 2023; disputed government-business fact-checking provision invalidated by the Bombay High Court on 26 September 2024.
2025 and 2026 amendments	G.S.R. 775(E), effective 15 November 2025; G.S.R. 120(E), effective 20 February 2026. Official intimation safeguards, accelerated deadlines and synthetic-media duties.
Shreya Singhal v. Union of India	Supreme Court, 24 March 2015: Section 66A struck down; intermediary takedown obligations interpreted in light of legally cognisable actual knowledge.

IDEAS AND DISTINCTIONS

Misinformation versus disinformation	False or misleading information can circulate without deliberate intent; disinformation involves intentional deception. The distinction concerns the conduct, not simply whether a claim is incorrect.
Information warfare	Coordinated efforts to influence perceptions, trust and decisions, including during conflict, without necessarily compromising computer systems.
Public Order and national security	Public Order concerns collective peace and stability; Internal Security encompasses wider threats, including terrorism, insurgency and hostile information activity.
Safe harbour	Section 79 gives qualified protection to intermediaries for third-party content, subject to statutory conditions and due diligence.
SGI and provenance	Realistic synthetically generated audio-visual information; labelling and embedded identifiers can assist viewers in assessing authenticity.
Constitutional boundaries	Article 19(1)(a) protects speech; Article 19(2) permits specified reasonable restrictions. Article 14 guards against arbitrariness, while Article 21 informs privacy and due-process concerns.

3 Additional information

Everything needed to answer this question well. Tier 1 contains the mechanisms of security harm, the actual amendments and their significance. Tier 2 places them within the wider governance debate on information integrity, online platforms and constitutional freedoms.

TIER 1 · ESSENTIAL: SECURITY THREATS, AMENDED RULES AND SAFEGUARDS

How false information becomes a security threat

Fabricate
False claim, edited clip, deepfake
→
Amplify
Forwarding, networks, algorithms
→
Mobilise
Fear, anger, distrust, retaliation
→
Disrupt
Public order, security, institutions

A teaching flow, not a universal causal sequence. Disinformation creates a security or public-order incident when audiences believe and act upon it in a particular social context; many false claims cause no such incident.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

Threat	Mechanism and Indian context	Why it matters
INTERNAL SECURITY: HARMS BEYOND THE INDIVIDUAL		
Hostile information operations	Organised networks, including foreign-linked actors, may circulate fabricated military claims, impersonate official sources or reuse unrelated footage as current conflict imagery. During **Operation Sindoor (May 2025)**, the Government reported such campaigns and described its factual rebuttals and blocking actions in a PIB release of 30 July 2025.	False situational awareness can cause panic, confuse audiences and erode confidence in official security communication.
Radicalisation and recruitment	Extremist actors may employ selective images, fabricated narratives and emotionally charged propaganda to encourage hatred or recruit supporters. UPSC's 2015 question on ISIS indoctrination through digital media belongs to this wider field; not every extremist message is itself factually false.	Disinformation can support a broader process of ideological mobilisation, violence and recruitment.
Undermining institutions	Fabricated messages attributed to public authorities, security agencies or election officials can mislead citizens about official actions. The **ECI's Myth vs Reality Register (2 April 2024)** addressed election-related falsehoods about procedures and voting technology.	Institutional distrust can weaken compliance, public confidence and the legitimacy of lawful decisions.
Operational distraction	False emergency alerts, fabricated threats and misleading images can trigger unnecessary verification or divert administrative attention. Risks are especially significant during conflict, disasters and other high-pressure events.	Security agencies must devote resources to checking false claims while communicating genuine information.
PUBLIC ORDER: WHEN DIGITAL CLAIMS PROVOKE PHYSICAL CONSEQUENCES		
Communal mobilisation	Fabricated allegations or old videos presented as fresh incidents can be circulated to inflame religious or caste tensions. In **September 2022**, the Ministry of Information and Broadcasting reported blocking 45 YouTube videos, citing fabricated and inflammatory content potentially disruptive of communal harmony.	Anger and retaliatory mobilisation can translate into threats, confrontations and disturbances.
Fear and displacement	In **August 2012**, rumours and threats contributed to the movement of thousands of people from north-eastern States back from southern Indian cities, as acknowledged in an official Ministry of Home Affairs statement.	Rumour-induced fear can disturb ordinary life and movement even without a sustained outbreak of violence.
Election-related disorder	False claims concerning polling, communal appeals or AI-generated impersonations can affect public confidence and tensions around voting. During **April 2026**, the ECI reported monitoring and action on more than 11,000 social-media posts or URLs across five election jurisdictions.	Public-order threats and electoral-integrity risks can overlap, although they are not identical.
Panic during emergencies	Fabricated warnings, incorrect location information, impersonated rescue instructions and misleading casualty claims may cause crowding, unnecessary travel or resistance to official directions.	Timely, trusted local communication becomes part of public-order management.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

Why disinformation travels rapidly in India

Amplification mechanism	How it works	The particular Indian vulnerability
Group forwarding	A claim passes repeatedly through private or semi-private messaging groups and gains apparent credibility through trusted acquaintances.	Family, neighbourhood, occupational and community networks; difficult public visibility of message circulation.
Algorithmic promotion	Engaging, sensational or divisive material may receive disproportionate exposure through recommendation and sharing systems.	Highly competitive political communication and emotionally charged identity issues.
Multilingual repackaging	The same narrative may be translated, revoiced or reformatted for different linguistic audiences.	Rapid verification requires relevant regional languages and local context.
Decontextualised evidence	Authentic older photographs, footage from another location or selectively edited recordings are presented as evidence of a new event.	Communal incidents, disasters, elections and security developments with strong emotional significance.
AI-enabled impersonation	Realistic synthetic voices, images or videos create the appearance that an authority or public figure has made a statement or taken an action.	Forged announcements, impersonated officials and persuasive local-language deepfakes.
Coordinated influence	Multiple accounts synchronise narratives to create a misleading impression of independent agreement or eyewitness corroboration.	Security-sensitive periods, organised propaganda and contested public events.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

The amendment chronology: what actually changed

Notification	Salient legal features	Connection with disinformation
2022 28 October G.S.R. 794(E)	**Rule 3(1)(b)(v):** intermediary rules and user communications cover misleading message origins and knowingly and intentionally communicated misinformation or patently false, untrue or misleading information. **Rule 3(1)(m) and (n):** intermediary accessibility, privacy, transparency and respect for constitutional rights. **Rule 3(2):** grievance handling, including an accelerated 72-hour category under the then-applicable provision. **Rule 3A:** online Grievance Appellate Committees; an aggrieved person may appeal within 30 days, and the committee should endeavour to decide within 30 calendar days.	Expands explicit user-facing due diligence concerning deceptive information while providing a route to challenge grievance decisions.
2023 6 April G.S.R. 275(E)	Amended Rule 3(1)(b)(v) to cover information concerning **any business of the Central Government** identified as fake, false or misleading by a government-specified fact-checking unit. The notification also included provisions concerning online gaming, separate from this question's principal subject. **Legal position:** the relevant government-business fact-checking amendment was struck down by the Bombay High Court on **26 September 2024**.	Illustrates the constitutional boundary of governmental authority over contested information. **Do not present the invalidated provision as an operative 2026 mechanism.**
2025 22 October G.S.R. 775(E) Effective 15 November	Substituted **Rule 3(1)(d)**. Legally relevant actual knowledge for removal arises through a competent court's order or a written, reasoned intimation from an authorised officer of the Appropriate Government or agency. The official intimation must specify the **legal basis, nature of unlawful conduct and identified electronic location**. General authorisation is subject to specified senior ranks; police intimations require a specially authorised officer not below **Deputy Inspector General of Police**. Government intimations are subject to **monthly review** by an officer not below Secretary rank for necessity, proportionality and statutory consistency. The removal deadline remained **36 hours**.	Clarifies the legal trigger and introduces safeguards against informal, vague or unreviewed official removal demands.
2026 10 February G.S.R. 120(E) Effective 20 February	**Rule 2:** defines synthetically generated information (SGI) and related audio-visual content, with exclusions for specified legitimate editing and other non-deceptive uses. **Rule 3(1)(d):** reduces the removal/disablement deadline following specified legal actual knowledge from 36 hours to **three hours**. **Rule 3(2)(a)(i):** reduces ordinary grievance disposal from 15 to **seven days**, and the specified expedited category from 72 to **36 hours**. **Rule 3(2)(b):** reduces the deadline from 24 to **two hours** for specified complaints concerning nudity, sexual acts, impersonation or morphed content. **New Rule 3(3):** due diligence concerning unlawful SGI, with appropriate technical measures and labelling, metadata and identifier obligations for permissible SGI. **Rule 4:** additional significant social media intermediary duties concerning user declarations, technical verification and prominent SGI labelling.	Addresses the speed and credibility of deepfakes and other realistic synthetic content; expands verification and provenance duties while accelerating legally specified responses.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

The timeline distinctions are substantive. The 2025 notification did not create the three-hour general Rule 3(1)(d) deadline; that change came into force on 20 February 2026. The 2026 three-hour deadline is triggered by the specified legally recognised notice or court order, not by every allegation that a post is false.

The operative 2026 framework, provision by provision

Provision	Practical obligation	Important limit
Rule 3(1)(b) User due diligence	Intermediaries must make reasonable efforts concerning listed categories of prohibited information and inform users of their rules, including restrictions on deceptive, impersonating or otherwise prohibited material.	The rule imposes intermediary due-diligence responsibilities. It does not itself make every incorrect statement a distinct criminal offence.
Rule 3(1)(d) Legal takedown	Remove or disable access to specified unlawful information within **three hours** after legally recognised actual knowledge from a competent court order or duly authorised reasoned government intimation.	Must be connected to applicable law and the required legal procedure; a random objection is not equivalent to statutory actual knowledge.
Rule 3(1)(c) User awareness	Users must be informed at least **once every three months** of applicable obligations and consequences; additional warnings apply to intermediaries facilitating SGI creation.	Awareness is preventive due diligence, not a substitute for a valid legal basis for content restriction.
Rule 3(2) Grievances	Ordinary complaints: seven-day resolution; certain expedited removal complaints: 36 hours; specified intimate-image, impersonation and morphed-content complaints: two-hour removal or disablement.	These are distinct complaint categories; the deadlines must not be conflated.
Rule 3(3) SGI due diligence	Requires reasonable and appropriate technical safeguards against unlawful synthetic content; permissible qualifying SGI must carry appropriate prominent labels and provenance-related metadata or identifiers.	Not every AI-assisted edit is SGI under the defined threshold; compliant synthetic media is not automatically prohibited.
Rule 4(1A) Significant platforms	Additional obligations for significant social media intermediaries, including declarations concerning synthetic content and reasonable technical verification before publication, with prominent identification where applicable.	Additional duties attach to the specified intermediary category, not indiscriminately to every small website or user.
Rule 3A Appeals	An online appeal may be filed against a Grievance Officer's decision within the prescribed 30-day period; committees aim to resolve appeals within 30 calendar days.	An administrative appeal does not exclude constitutional scrutiny or judicial remedies.
Rule 7 and Section 79 Compliance consequence	Failure to observe the applicable intermediary rules can affect the conditional legal protection available for third-party content under Section 79 of the IT Act.	Loss of safe harbour does not automatically establish every substantive offence; liability must still be assessed under applicable law.

How the amendments address distinct threats

Disinformation problem	Relevant provision	Intended effect	Remaining challenge
Fabricated message origin	2022 Rule 3(1)(b)(v)	Due diligence against deceptive or misleading communications.	Reliable proof and lawful expression.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

Disinformation problem	Relevant provision	Intended effect	Remaining challenge
Rapid circulation of unlawful material	2025 and 2026 Rule 3(1)(d)	Authorised removal directions and faster compliance.	Due process under very short deadlines.
Convincing synthetic audio or video	2026 Rule 3(3), Rule 4	Prevention of unlawful SGI; visible labels and provenance identifiers for permissible SGI.	Detection errors, stripped metadata and cross-platform forwarding.
Incorrect moderation decision	2022 Rule 3A	Additional grievance appeal mechanism.	Meaningful independence and effective restoration.
Unclear official takedown demands	2025 Rule 3(1)(d)	Reasoned, authorised, reviewable government intimations.	Whether review and disclosure are sufficient in practice.
Election-related false narratives	IT Rules plus ECI directions	Platform response combined with election-specific monitoring and corrective communication.	Credible verification, impartiality and avoiding suppression of legitimate political speech.

The legal distinction that secures marks. Section 69A of the IT Act concerns government blocking powers, subject to its own statutory framework. **Rule 3(1)(d)** concerns intermediary action after legally recognised actual knowledge. **Rule 3A** concerns grievance appeals. They are related instruments, but they are not interchangeable.

The 2023 fact-checking distinction. The Bombay High Court invalidated the specific government-business fact-checking amendment. That does **not** mean the entire IT Rules framework was struck down, or that public authorities are barred from publishing factual corrections. The PIB's fact-checking activity and the invalidated special regulatory power must be distinguished.

TIER 2 · EXTENDED UNDERSTANDING: THE WHOLE TOPIC AROUND IT

Institutional responses beyond takedown

1. **PIB Fact Check Unit:** publicly verifies claims relating to the Central Government and publishes corrections. During Operation Sindoor, it issued rebuttals to circulating false claims, according to the Government's July 2025 account.
2. **Election Commission:** Myth vs Reality Register, launched 2 April 2024, and specific directions on AI-generated campaign content, including prominent labelling and action against unlawful misinformation.
3. **Ministry of Information and Broadcasting:** supervises relevant digital-media publisher mechanisms under Part III of the IT Rules; also operates within other statutory media frameworks.
4. **State police and cybercrime units:** investigate offences and manage local threats to public order under applicable criminal law. The Union Government's August 2026 statement confirmed that police and public order are primarily State subjects.

Where regulation can fall short

1. **Propagation outruns response:** a false narrative may spread widely before detection, reporting and a legal removal direction.
2. **Private or encrypted channels:** public debunking and platform moderation may not reach every closed messaging group or copied message.
3. **Language and context:** sarcasm, local idiom and political context can generate erroneous automated classifications.
4. **Synthetic-media provenance:** labels or metadata can be detached when material is re-recorded, reformatted or redistributed.
5. **Over-removal:** very short deadlines can create incentives to remove disputed material before detailed assessment, particularly when safe-harbour protection is at stake.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

5. **National Cyber Crime Reporting Portal:** provides reporting channels for cybercrime; its role differs from general truth verification or ordinary complaints to social-media platforms.
6. **Independent fact-checking and journalism:** corroboration, geolocation, reverse-image checking, original-source verification and transparent corrections can reduce reliance on official takedowns alone.
6. **Trust deficit:** a correction may be ineffective if its source lacks public credibility or if competing groups reject common evidence.

The constitutional architecture of information control

Constitutional or judicial principle	What it means	Why it matters here
Article 19(1)(a)	Protects freedom of speech and expression, including political criticism, discussion and disagreement.	Incorrect or unpopular expression does not automatically lose constitutional protection.
Article 19(2)	Permits reasonable restrictions on specified grounds, including security of the State, public order, sovereignty and integrity of India, and incitement to an offence.	A restrictive measure needs a constitutionally permissible basis and must meet applicable standards.
Article 14	Requires equality before the law and guards against arbitrary State action.	Vague, selectively applied or unguided truth-determination powers raise constitutional concerns.
Article 21	Protects life and personal liberty, including privacy as recognised by the Supreme Court.	Investigations and content controls must account for privacy and procedural fairness.
Shreya Singhal, 2015	The Supreme Court invalidated Section 66A and addressed the legal basis for intermediary takedown obligations.	Vagueness and overbreadth are constitutional problems, not technical drafting details.
Kunal Kamra, 2024	Bombay High Court majority invalidated the 2023 government-business fact-checking amendment.	The Government cannot assume unlimited power to define falsehood through subordinate legislation.
Proportionality	Restrictions should pursue a legitimate purpose through lawful, necessary and appropriately limited means.	Targeted, reasoned intervention is preferable to indiscriminate or unreviewable suppression.

Governance: removal is only one response

An effective disinformation strategy works at **three stages**. Before dissemination, credible public information, digital literacy, verified official channels and clearer synthetic-media labelling help prevent deception. During dissemination, detection, independent verification, targeted lawful moderation and timely public correction can reduce amplification. After harm, police investigation where offences are established, grievance appeals, evidence preservation and public review of enforcement decisions support accountability.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

This distinction is particularly important for **State and district administrations**. When a fabricated communal allegation circulates, a police or district administration may need to verify the facts locally, communicate promptly in relevant languages, protect vulnerable communities and initiate action against unlawful incitement. Broad internet restrictions or blanket removal requests should not replace the assessment of the specific threat and the legal authority available.

Two debates worth knowing

Should the Government decide what counts as fake news?

The case for: national-security agencies may possess verified operational information unavailable to private platforms, especially during conflict or emergencies. Rapid authoritative rebuttals can prevent panic. **The concern:** the Government is also a participant in public debate and may have an interest in suppressing embarrassing but lawful criticism. The Bombay High Court's 2024 judgement demonstrates why broad official truth-determination powers are constitutionally contested. **The balanced position:** distinguish public factual correction from coercive removal; require a lawful basis, independent scrutiny, reasoned decisions and accessible remedies.

Does faster takedown automatically produce greater security?

The case for: convincing deepfakes, impersonated instructions and communal incitement can spread faster than older moderation procedures, making prompt action necessary. **The concern:** a three-hour deadline may encourage precautionary over-removal when difficult factual and legal questions require careful assessment. **The balanced position:** retain rapid action against clearly unlawful material while improving precise legal notices, transparent review, verified provenance, appeal mechanisms and subsequent restoration of content wrongly removed.

4 Pitfalls and variations

The six mistakes that weaken this answer, the claims that must never appear, and how the answer changes when the directive or focus changes.

4.1 Six pitfalls, each with its correction

Confusing security with public order

~~Fake news creates panic, so it is a threat to national security.~~

Separate hostile propaganda, radicalisation and institutional disruption from communal mobilisation, crowd panic and disturbances of local peace.

All threats, no regulatory detail

~~False news spreads hatred, causes violence and creates tension. We need strict laws.~~

Reserve about two-fifths of the body for the actual amendments, specifying the year, rule and obligation.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

Chronological confusion

~~The 2021 Rules introduced the three-hour takedown rule and AI labelling requirements.~~

The 2021 Rules created the parent framework; the three-hour Rule 3(1)(d) deadline and dedicated SGI provisions came into force on 20 February 2026.

Ignoring the 2024 judgement

~~The Central Government's Fact Check Unit can order removal of all fake news about government affairs under the 2023 amendment.~~

The contested 2023 government-business fact-checking provision was struck down by the Bombay High Court in September 2024. Separate lawful takedown powers and public fact-checking activity remain distinct.

Conflating the deadlines

~~All fake news must be removed within three hours of a complaint.~~

Rule 3(1)(d) provides three hours after specified legal actual knowledge; certain grievances have a 36-hour timeline, and the designated intimate-content category has a two-hour removal deadline.

No constitutional judgement

~~Strict censorship is the only way to protect internal security.~~

Target unlawful disinformation through proportionate, reasoned and reviewable procedures; combine moderation with reliable information and independent fact-checking.

4.2 Never write these

- "The IT Rules make all fake news a criminal offence."
  The Rules impose duties on intermediaries and interact with existing laws; criminal liability depends on the elements of an applicable offence.
- "The 2026 amendment bans all AI-generated material."
  It addresses defined synthetically generated information, prohibits specified unlawful uses and establishes labelling and related duties for permissible content; legitimate uses are not all prohibited.
- "The three-hour takedown deadline began in October 2025."
  G.S.R. 775(E), notified on 22 October 2025, retained 36 hours; G.S.R. 120(E), effective 20 February 2026, reduced the period to three hours.
- "The 2023 Government Fact Check Unit rule is fully operational."
  The relevant amendment to Rule 3(1)(b)(v) was struck down by the Bombay High Court on 26 September 2024.
- "The PIB's Fact Check Unit was abolished by the Bombay High Court."
  The judgement concerned the disputed regulatory provision; PIB's public verification and rebuttal functions are distinct.
- "All social media platforms must identify the first originator of every message."
  Originator identification under the original Rule 4(2) concerns specified significant messaging services and limited categories of lawful orders, with statutory qualifications; it is not a universal message-tracing obligation.
- "Section 69A and Rule 3A provide the same remedy."
  Section 69A relates to blocking powers; Rule 3A establishes Grievance Appellate Committees.
- "The ECI removed 11,000 fake posts during the 2026 Assembly elections."
  Its 19 April 2026 statement reported that more than 11,000 items had been identified and acted upon, using various forms of action, not exclusively removal.
- "Every mistaken online claim is disinformation."
  Disinformation involves deliberate deception; misinformation can spread without that intent.
- "National security permits unrestricted censorship."
  Article 19(2) permits specified reasonable restrictions; statutory authority, necessity, proportionality and procedural safeguards still matter.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

4.3 If the question changes

If it asks	The structure becomes	What must change
Critically examine the IT Rules and freedom of expression	Regulatory objectives; due-diligence benefits; risks of over-removal; Shreya Singhal and Kunal Kamra; procedural reforms; judgement.	Constitutional scrutiny becomes the main body, not a short final part.
How **deepfakes** threaten elections	Types of synthetic media; electoral harms; ECI directions; 2026 SGI amendments; labelling, authentication and enforcement gaps.	Focus on AI-enabled deception rather than the full misinformation landscape.
Evaluate the **2026 IT Rules amendment**	SGI definition; Rule 3(3); Rule 4 duties; revised takedown and grievance deadlines; advantages; rights and compliance challenges.	Concentrate on G.S.R. 120(E) and its actual commencement date.
Role of **social media in communal violence**	Rumour creation; amplification; mobilisation; Indian cases; police response; legal intervention; local trust-building.	Public Order becomes dominant; intermediary law becomes one remedy.
Assess **cross-border information warfare**	Threat actors; false narratives; conflict-time manipulation; Operation Sindoor; institutional coordination; verification and countermeasures.	National-security operations and hostile influence become the focus.
The same question for **15 marks**	Both explicit demands at greater depth, a provision-by-provision amendment table, examples, constitutional case law and a balanced judgement.	Use additional evidence and explicit legal distinctions without turning the answer into a history of every IT provision.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

5

The model answer

One model answer, written to the UPSC Gurus house range of 150 to 153 words (**152 words exactly**, counting every whitespace-separated token in the answer sheet, including section numerals, headings and point labels; UPSC's printed limit is 150 words). The form is three headed parts: the security and public-order mechanisms, the four amendment stages, and a short constitutional qualification. The introduction addresses both demands; the conclusion reconciles effective regulation with constitutional freedoms.

Model answer ## Threats, amendments and safeguards **152 words**

Disinformation exploits India's divisions, threatening security and public order; amended IT Rules seek faster, accountable responses.

1. Threats to security and public order

- **Security:** Fabricated military claims during Operation Sindoor (2025) fuelled confusion; hostile propaganda undermines institutions and can facilitate radicalisation.
- **Public order:** Local communal rumours and manipulated videos can provoke panic, retaliation and violence.
- **Amplification:** Messaging forwards, multilingual networks and convincing deepfakes speed mobilisation.

2. Amendments to IT Rules, 2021

- **2022:** Rule 3(1)(b)(v) covers intentionally misleading information; Rule 3A enables grievance appeals.
- **2023:** Government-business fact-checking provision struck down by Bombay High Court (2024).
- **2025:** Rule 3(1)(d) requires reasoned, authorised takedown intimations and review.
- **2026:** Three-hour removal after valid notice; synthetic-media labelling, provenance, verification and faster grievance redressal.

3. Constitutional safeguards

Restrictions require legality, proportionality and review, protecting Articles 14, 19 and 21; lawful criticism must survive moderation.

Security improves when prompt corrections and transparent enforcement protect social peace and free expression.

DEMAND
Explain how disinformation threatens Internal Security and Public Order in India, then discuss the salient provisions, duties and significance of amendments to the IT Rules, 2021

HIDDEN DEMAND
Disinformation control must remain compatible with freedom of expression, due process, independent information and proportionate, reviewable State action

STRUCTURE
About two-fifths on security and public-order threats, two-fifths on the amended IT Rules, and a short final part on constitutional freedoms and safeguards

BALANCE
Introduction 16 words, conclusion 14 words; 152 words in all

Why it works: The introduction links disinformation's security harms to the regulatory response without spending words on a definition. Part 1 differentiates security from public order, includes the Indian example of Operation Sindoor (2025), and identifies amplification mechanisms. Part 2, the largest component, follows the amendment chronology: the 2022 due-diligence and appeal changes, the 2023 provision invalidated in 2024, the 2025 safeguards and the 2026 accelerated deadlines and synthetic-media duties. Part 3 answers the hidden demand through constitutional rights and proportionality. The conclusion treats effective security and lawful expression as compatible objectives. **The answer contains exactly 152 whitespace-separated words, including all numbered headings and labels.**

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

6 Other ways to write it

The model answer above remains the answer. These alternative outlines show how the same demand could be answered without losing either the threat mechanisms or the amended regulatory framework.

Approach	How it is built	When it works
Threat-to-regulation matrix	A compact table matching hostile propaganda, communal rumours and deepfakes with intermediary duties, takedown procedures and synthetic-media safeguards. End with constitutional limits.	When you want each regulatory instrument explicitly connected to a security problem.
Chronological regulatory answer	Brief security and public-order threats; then 2022, 2023, 2025 and 2026 amendments, naming the relevant rule and significance of each; conclude with judicial safeguards.	When the distinctive feature of the question is the word **amendments**.
Open with an Indian example	Introduction: Operation Sindoor's misinformation environment or the 2022 blocking of inflammatory YouTube videos; explain the causal mechanisms, then discuss the amended Rules.	When you want a concrete opening, provided the example does not consume the answer's limited space.
Constitutional-first answer	Begin with the security need and Article 19(2); show why the amendments are necessary, then test them against the Kunal Kamra judgement, proportionality and appeals.	When the directive changes to **critically evaluate** the regulatory framework.
For 15 marks	Add a threat-amplification flow, a provision-wise table, election and conflict examples, a distinction between Section 69A and Rule 3(1)(d), and a fuller constitutional judgement.	When more space is available to explain legal mechanisms and their limitations.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

7 Quick recall and Prelims crossover

Sixteen verifiable facts connecting India's intermediary framework, amendment dates, institutional mechanisms and concrete misinformation responses.

1. **IT Rules, 2021**: notified **25 February 2021**, G.S.R. **139(E)**, under the IT Act, 2000.
2. **2022 amendment**: G.S.R. **794(E)**, **28 October 2022**; revised Rule 3(1)(b) and inserted Rule 3A.
3. **Rule 3A**: Grievance Appellate Committees; appeal generally within **30 days**, with a **30-calendar-day** disposal endeavour.
4. **2023 amendment**: G.S.R. **275(E)**, **6 April 2023**; included the contested Central Government fact-checking provision.
5. **Kunal Kamra v. Union of India**: Bombay High Court struck down the 2023 government-business fact-checking amendment on **26 September 2024**.
6. **2025 amendment**: G.S.R. **775(E)**, dated **22 October 2025**; effective **15 November 2025**; reasoned official intimations and monthly review.
7. **2026 amendment**: G.S.R. **120(E)**, **10 February 2026**; effective **20 February 2026**.
8. **Section 79, IT Act**: qualified intermediary protection for third-party information, subject to legal conditions and due diligence.
9. **Unlawful-content removal**: Rule 3(1)(d), **three hours** after specified legal actual knowledge, effective **20 February 2026**.
10. **Ordinary grievances**: resolution period reduced from **15 to seven days** by the 2026 amendment.
11. **Specified intimate or morphed-content complaints**: removal or disablement deadline reduced from **24 to two hours** in 2026.
12. **SGI definition**: Rule **2(1)(wa)**; realistic synthetic audio, visual or audio-visual information, subject to specified exclusions.
13. **Rule 3(3)**, inserted in 2026: due diligence against unlawful SGI and labelling, metadata and identifiers for permissible SGI.
14. **Rule 4(1A)**: significant social media intermediaries must seek SGI declarations, undertake appropriate verification and label confirmed SGI.
15. **September 2022**: MIB directed blocking of **45 YouTube videos** from **10 channels**, reporting over **1.3 crore views**.
16. **ECI, 19 April 2026**: over **11,000 posts/URLs** identified and acted upon in Assembly elections through removals, FIRs, clarifications or rebuttals.

THE ONE SENTENCE TO CARRY OUT OF THIS DOCUMENT

India must prevent falsehood from becoming violence without allowing the fight against disinformation to become a licence to suppress lawful expression.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

8 Write it yourself

Write the answer in 150 words without looking back, then check whether it explains both the threats and the amendments, and whether its constitutional judgement is supported by the law.

	Check	Yes / No
1	Does the introduction connect **digital disinformation, security harms and the need for regulatory responses**?	
2	Does Part 1 distinguish **Internal Security from Public Order** and explain how disinformation causes each threat?	
3	Have I included **amplification mechanisms, an Indian example and the specific vulnerabilities** that make misinformation dangerous?	
4	Does Part 2 correctly identify the **2022, 2023, 2025 and 2026 amendments**, naming operative provisions and recognising the 2024 judgement?	
5	Have I distinguished **intermediary due diligence, lawful takedown, grievance appeals and synthetic-media obligations**, without confusing their deadlines?	
6	Does the short final part address **freedom of expression, proportionality, reasoned decisions and review**, with a conclusion approximately matching the introduction's length?	
7	Is the answer **150 words or a little over**, counting all headings and labels, and free of every incorrect claim listed in section 4.2?	

Sources

- **Ministry of Electronics and Information Technology:** Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended to February 2026, with rule-by-rule legislative footnotes, consolidated as at 10 February 2026. Read with corrigendum G.S.R. 148(E), dated 26 February 2026. meity.gov.in.
- **MeitY, 28 October 2022:** consolidated IT Rules reflecting G.S.R. 794(E), including amendments to Rule 3(1)(b), intermediary duties, grievance redressal and Rule 3A. meity.gov.in.
- **MeitY, 6 April 2023:** updated IT Rules incorporating G.S.R. 275(E), including the government-business fact-checking amendment that was subsequently invalidated. meity.gov.in.
- **Bombay High Court:** Kunal Kamra v. Union of India and connected matters, final judgement dated 26 September 2024, declaring the 6 April 2023 amendment to Rule 3(1)(b)(v) unconstitutional and striking it down. Judgement text: indiankanoon.org. Contemporary judgement reporting: indianexpress.com.
- **MeitY, Gazette of India, 22 October 2025:** G.S.R. 775(E), Information Technology Amendment Rules, 2025; substituted Rule 3(1)(d), commenced 15 November 2025, specifying reasoned, authorised intimations and monthly review. meity.gov.in. Official explanatory release dated 23 October 2025: pib.gov.in.
- **MeitY, Gazette of India, 10 February 2026:** G.S.R. 120(E), Information Technology Amendment Rules, 2026, effective 20 February 2026. Primary notification covering SGI definitions, Rule 3(3), Rule 4(1A), three-hour takedown and grievance timelines: meity.gov.in. Official explanatory FAQs, including the distinctions between lawful and unlawful synthetic information: meity.gov.in.
- **Supreme Court of India:** Shreya Singhal v. Union of India, judgement of 24 March 2015, concerning Section 66A, freedom of expression and intermediary actual knowledge. Judgement text: indiankanoon.org.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

- **Ministry of Electronics and Information Technology:** Government announcement of three Grievance Appellate Committees, published by PIB on 28 January 2023, covering their constitution, appeal purpose and digital functioning. pib.gov.in. Government parliamentary response dated 2 August 2024 reporting 1,065 appeals filed and 937 disposed of up to 30 June 2024: pib.gov.in.
- **Ministry of Information and Broadcasting, 26 September 2022:** official report of blocking orders dated 23 September against 45 YouTube videos from 10 channels, citing fake news, morphed content and potential communal disharmony. pib.gov.in.
- **Ministry of Home Affairs:** National Integration Council proceedings (2013), including the account of the 2012 north-eastern exodus, rumours, social-networking messages and social tensions. mha.gov.in.
- **Election Commission of India:** press note dated 2 April 2024 introducing the Myth vs Reality Register for election misinformation: eci.gov.in. Press note dated 6 May 2024 directing responsible use of social media and action on political-party deepfakes and misinformation: eci.gov.in.
- **Election Commission of India, 19 April 2026:** press note on action against more than 11,000 social-media posts and URLs during Assembly elections in Assam, Kerala, Tamil Nadu, Puducherry and West Bengal, distinguishing removal, FIRs, clarifications and rebuttals. Official release reproduced by PIB: pib.gov.in.
- **Ministry of Information and Broadcasting, 30 July 2025:** official account of misinformation and hostile narratives during Operation Sindoor, including PIB Fact Check Unit rebuttals, official security communication and blocking directions covering more than 1,400 URLs. pib.gov.in.
- **Ministry of Information and Broadcasting, 1 to 2 April 2026:** parliamentary response and PIB release explaining the continuing public fact-checking activities of the PIB Fact Check Unit, including 2,913 published fact checks, distinct from the invalidated 2023 regulatory provision. pib.gov.in.
- **Union Public Service Commission:** official Civil Services (Main) Examination question-paper archive for GS Paper III, 2013 to 2026, including the verbatim PYQs identified by examination year, paper and question number in section 2.2. upsc.gov.in. Earlier archived question papers: upsc.gov.in.

Explain how fake news and disinformation pose threat to Internal Security and Public Order in Indian context ? In this regard, discuss salient features of amendments in respect of Information Technology (Intermediatory Guidelines and Digital Media Ethics Code) Rules 2021.

YOUR NEXT STEP

Now write GS Paper III 2026 again.

You now know what this question asked, what it expected without saying so, and how its answer is built. Write the whole paper under the clock, have it evaluated, and read the feedback against this document.



1 Write the full paper in three hours

2 Self-check this answer with section 8

3 Have the paper evaluated

4 Read the feedback against this document

FREE

Mains Replay

170 UPSC Mains papers from 2017 to 2026 (GS I to IV, Essay and six optionals), with a built-in three-hour exam clock. Write GS Paper III 2026 exactly as you would in the hall.

upscgurus.in/mains-pyq

₹1,499 PER PAPER, INCL. GST

Paper Evaluation

A written evaluation of every answer and a personal feedback session, through Mains Mastery.

upscgurus.in/mains-mastery

FREE

UG Handout 01

Where did my Mains 2026 marks go? All 79 GS questions and parts decoded: demand, hidden demand, structure.

upscgurus.in/open-library

FREE

GS Mains PYQ Deep Decode

Previous year questions taught on YouTube: the reasoning, the structure and what a strong answer holds.

UPSC Gurus on YouTube

PROGRAMME

Mains Mastery

The UPSC Gurus GS Mains programme: every question read for its demand, hidden demand and structure, and answers written and evaluated to that standard.

upscgurus.in/mains-mastery

UPSC Gurus is an inclusive platform. This PDF is tagged, with headings, reading order and selectable text, for use with screen readers.

Guranchal Ma'am

Founder, UPSC Gurus