# Defence & Security · GS - III

**Information warfare increasingly exploits artificial intelligence and social divisions to create internal security challenges. Analyse India's vulnerabilities and the institutional response required.**

| EXAM YEAR | PAPER | SUBJECT |
|---|---|---|
| DAILY PRACTICE 27/11/2026 | GS - III | Defence & Security |

| MARKS | WORD LIMIT |
|---|---|
| 15 | ~250 words |

## Answer Hint

**Deepfakes, disinformation, bot networks, social polarisation, cyber security, digital literacy, platform accountability, intelligence coordination**

## Model Answer

Information warfare uses digital platforms and manipulated narratives to influence public opinion, weaken institutional trust and exploit social divisions. The reported use of fake identities, coordinated accounts and AI-generated deepfakes against India illustrates the growing intersection of technology and internal security.

**Major vulnerabilities**

1. **Rapid information circulation:** Social media and encrypted messaging platforms enable misleading content to spread before verification.
2. **Deepfake manipulation:** Synthetic videos and audio can impersonate public figures, distort events and provoke public reactions.
3. **Social fault lines:** Disinformation targeting religious, regional or political identities can intensify mistrust and communal tensions.

4. **Coordinated amplification:** Bot networks and fake profiles can create artificial trends and make fabricated narratives appear credible.
5. **Attribution difficulties:** Identifying the origin, coordination and sponsorship of online campaigns requires specialised technical and intelligence capabilities.

**Institutional response**

1. **Cyber intelligence:** Strengthen coordination between intelligence agencies, cybercrime units and digital forensic institutions.
2. **Fact-checking:** Develop rapid verification mechanisms and communicate corrections in multiple Indian languages.
3. **Platform accountability:** Encourage transparent content moderation, detection of coordinated inauthentic behaviour and timely preservation of digital evidence.
4. **Legal safeguards:** Apply relevant provisions of the Information Technology Act, 2000, and other applicable laws while protecting freedom of speech and expression.
5. **Public resilience:** Promote media literacy so citizens can identify manipulated content and verify information before sharing it.

**Strategic priority**

India needs a whole-of-society approach combining technological preparedness, credible public communication, democratic safeguards and international cooperation.

**Conclusion:** National security in the digital age depends not only on protecting networks but also on strengthening citizens' ability to distinguish authentic information from deliberate manipulation.

BECOME IAS
AI POWERED UPSC PREP