Mains Practice Question

Q. The weaponization of social media for propaganda and recruitment by extremist groups poses a significant threat to internal security. How can India develop a robust strategy to combat digital extremism without compromising democratic values? **(250 words)**

11 Sep, 2024 GS Paper 3 Internal Security

Approach

- Introduce the answer by highlighting the proliferation of digital extremism
- Delve into the Challenges Posed by Digital Extremism
- Give Strategies to Combat Digital Extremism
- Highlight ways to Striking a Balance Between Combating Digital Extremism and Upholding Democratic Values
- Conclude suitably.

Introduction

The digital age has brought **unprecedented connectivity and access to information,** but it has also created **new avenues for extremist groups to spread propaganda and recruit followers.**

- India, as the world's largest democracy and a rapidly digitizing nation, faces a unique challenge in combating **digital extremism** while upholding its democratic values.

Body

Challenges Posed by Digital Extremism:

- **Rapid Dissemination of Hate Speech**: Social media platforms allow extremist groups to disseminate hateful content at lightning speed, reaching a wide audience and fostering division within society.
  - **Example:** The **Christchurch mosque attacks in 2019,** where the perpetrator live-streamed his heinous acts on Facebook, demonstrating the rapid spread of extremist content online.
- **Recruitment and Radicalizati**on: Online platforms provide a **fertile ground for extremist groups to recruit vulnerable individuals** and groom them into radicalized followers.
  - **Example**: ISIS used Telegram and other messaging apps to recruit and spread propaganda.
- **Deepfakes and Misinformation:** The **proliferation of deepfakes** and other forms of misinformation can be used to manipulate public opinion and undermine trust in democratic institutions.
  - The **Indian general election of 2024** saw a surge in the deployment of AI-based technologies, particularly deep fakes and disinformation campaigns.
- **Honey Trapping**: Extremist groups may employ honey trapping tactics through social media to compromise individuals working in sensitive positions, such as defense or government agencies.
  - In 2023, a **DRDO scientist was arrested** for allegedly sharing sensitive information with

a Pakistani intelligence operative who had lured him into a romantic relationship.

Strategies to Combat Digital Extremism:

- **Multi-Stakeholder Collaboration:** A collaborative approach involving government agencies, technology companies, civil society organizations, and academic institutions is essential to combat digital extremism.
- **Content Moderation and Fact-Checking**: Technology companies should implement **robust content moderation policies and invest in fact-checking initiatives** to reduce the spread of harmful content.
    - **Indian Government** issues advisory to social media intermediaries to identify misinformation and deep fakes and remove any such content when reported within 36 hours of reporting, is a significant step in this direction.
- **Counter-Narratives and Positive Messaging:** Government and civil society organizations should develop counter-narratives and promote positive messaging to challenge the extremist ideology.
- **Cybersecurity and Digital Literacy**: Strengthening **cybersecurity measures and enhancing law enforcement capabilities** can help disrupt the activities of extremist groups online.
    - Also, promoting digital literacy among the population can help individuals identify and counter extremist propaganda.

Striking a Balance Between Combating Digital Extremism and Upholding Democratic Values:

While combating digital extremism is crucial, it is equally important to safeguard democratic values such as freedom of speech and expression. Here are some key considerations:

- **Proportionality:** Any measures taken to restrict online content should be proportionate to the threat posed.
- **Clarity and Transparency:** Laws and regulations governing online content should be clear and transparent to avoid arbitrary censorship.
- **Independent Oversight**: An independent body should be established to monitor and review government actions related to online content moderation.
- **International Cooperation**: International cooperation is essential to address the global nature of digital extremism while respecting national sovereignty.

Conclusion

Combating digital extremism in India requires a multifaceted approach that balances the need to **protect national security with the preservation of democratic values.** By fostering collaboration, promoting digital literacy, strengthening cybersecurity measures, and developing effective counter-narratives, India can mitigate the threat posed by extremist groups operating online.