PLUTUS IAS

CURRENT AFFAIRS

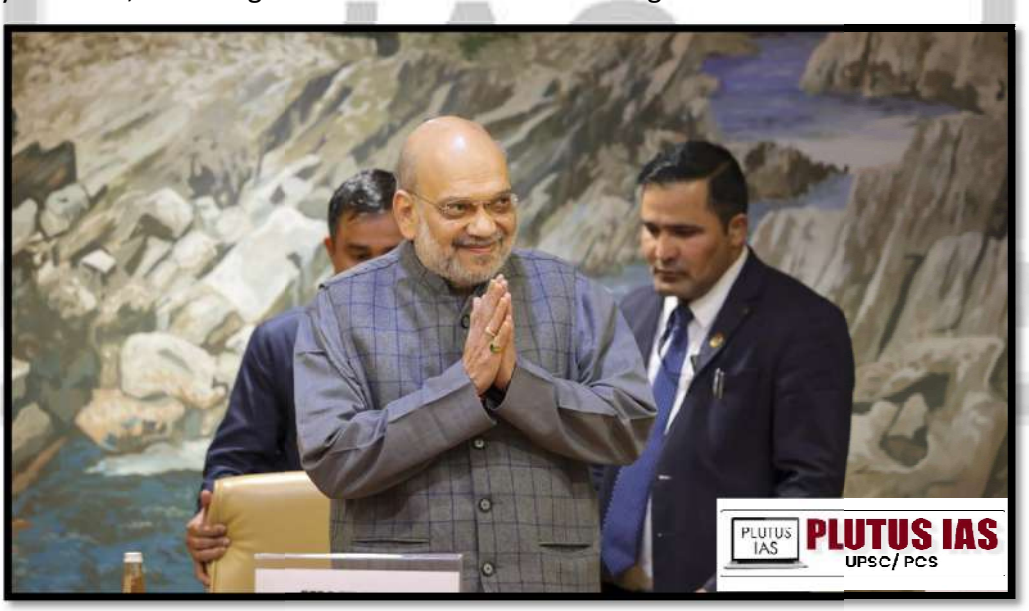
Argasia Education PVT. Ltd. (GST NO.-09AAPCAI478E1ZH)
Address: Basement C59 Noida, opposite to Priyagold Building gate, Sector 02,
Pocket I, Noida, Uttar Pradesh, 201301, CONTACT NO:-8448440231

Date –17- February 2025

NATIONAL SECURITY: SOCIAL MEDIA

WHY IN THE NEWS?

India's digital boom, while offering immense potential, is accompanied by a surge in cybercrime. Home Minister Amit Shah outlined the government's response, emphasizing a multi-faceted strategy. This includes blocking malicious online content, fostering inter-agency collaboration to combat cyber threats, and employing AI to detect financial fraud. Recognizing the borderless nature of cybercrime, the government stresses a holistic approach encompassing software security, service provider responsibility, and user awareness. The rising number of cybercrime cases underscores the urgent need for these measures to safeguard India's burgeoning digital economy and its citizens. The government's goal is a substantial reduction in cybercrime, reflecting its commitment to a secure digital future.



WHAT IS SOCIAL MEDIA?

Social media refers to online platforms and tools that enable users to create, share, and interact with content, as well as connect with others. It allows people to communicate, exchange ideas, and build communities through text, images, videos, and other forms of media. Social media platforms typically offer features like messaging, commenting, liking, sharing, and following, which help users engage with one another.

1. Facebook: A platform for sharing personal updates, photos, and videos and engaging with friends, family, and communities.
2. Instagram: Focused on sharing images and videos, often with artistic or personal branding purposes.
3. Twitter (now X): A microblogging platform for sharing brief thoughts, news updates, and trending topics.
4. TikTok: A video-sharing app that allows users to create short, creative videos, often paired with music or special effects.
5. LinkedIn: A professional network for connecting with colleagues, recruiters, and businesses, used for career networking and sharing industry-related content.

HOW HAS SOCIAL MEDIA BECOME A THREAT TO INTERNAL SECURITY?

1. Radicalization and Recruitment: Extremist groups use social media to spread propaganda and recruit individuals, particularly vulnerable youth, leading to potential violence.
2. Misinformation: False information spreads rapidly, causing confusion, distrust, and social unrest, often fueling protests or riots.
3. Cyberbullying and Harassment: Online abuse harms individuals psychologically and disrupts social cohesion, contributing to societal instability.
4. Organizing Protests and Riots: Social media enables the coordination of protests, which can escalate into violence, creating public safety risks.
5. Data Privacy Concerns: Personal information shared on social media can be exploited for malicious purposes like identity theft or targeted misinformation.
6. Foreign Interference: Social media is used by foreign actors to manipulate public opinion, interfere in elections, and create political divisions.

WHAT ARE THE GOVT ACTION TO TACKLE THE THREAT OF SOCIAL MEDIA?

1. Advisories: MeitY has advised social media platforms to quickly remove misinformation and hoax bomb threats. Social media platforms are urged to report activities that threaten India's unity, integrity, sovereignty, security, or economic stability.
2. Financial Assistance: The central government provides financial assistance to law enforcement agencies in states and union territories to enhance their cybersecurity infrastructure and capabilities.
3. Partnerships: The government collaborates with academic institutions and R&D centres to build the cybersecurity workforce.
4. Legal Action: Social media platforms that fail to comply with the IT Rules and Bharatiya Nyay Sanhita (BNS) may face legal action.
5. Reporting: Social media threats can be reported to the Internet Crime Complaint Center (IC3).
6. Other Actions: The government has strengthened mechanisms to address and combat cybercrime.

CHALLENGES IN CONTROLLING THREATS FROM SOCIAL MEDIA:

1. Misinformation and Fake News: False information spreads rapidly on social media, causing confusion, inciting violence, or triggering harmful actions.
2. Hate Speech and Cyberbullying: Identifying and moderating harmful content like hate speech and bullying is difficult, especially when it's subtle or disguised.
3. Privacy Concerns: Balancing user privacy with the need to monitor for malicious activity is complex due to the large amount of personal data collected on platforms.
4. Anonymity: Online anonymity allows harmful behaviours to thrive without accountability, making it hard to trace perpetrators.

5. Platform Complexity: The vast number of social media platforms and their constantly evolving features make it hard to monitor and enforce rules consistently.
6. Global Reach: Social media threats can quickly cross international borders, requiring cooperation between multiple legal systems and jurisdictions to address them.
7. Algorithmic Manipulation: Algorithms that prioritize engagement can unintentionally amplify harmful content, making it more likely to spread.
8. Social Engineering Attacks: Cybercriminals exploit social media to manipulate users through scams like phishing, aiming to steal sensitive information.
9. Resource Limitations: Effective policing of social media requires significant human resources to review flagged content and take appropriate action.

WHAT ARE WAYS TO REGULATE SOCIAL MEDIA?

1. Content Moderation: Use AI and human moderators to detect and remove harmful content like hate speech and misinformation. Platforms should have clear guidelines and enforce them consistently.
2. Platform Accountability: Hold platforms accountable for harmful content and impose penalties for non-compliance with regulations.
3. Transparency: Require platforms to publish transparency reports on content moderation and disclose political ads to prevent manipulation.
4. Data Privacy: Strengthen user data protection with stricter privacy laws and ensure platforms get explicit consent before collecting data.
5. Combating Misinformation: Partner with fact-checkers, label false content, and provide context to reduce misinformation spread.
6. Protect Vulnerable Groups: Implement stronger protections against cyberbullying harassment and create safe spaces for users, especially minors.
7. Media Literacy: Promote digital literacy campaigns to help users identify misinformation and navigate social media safely.
8. Cross-Border Cooperation: Establish international regulations and cooperation between countries to tackle global issues like hate speech and cybercrime.
9. Algorithm Transparency: Regulate algorithms to prevent the amplification of harmful content and ensure user well-being is prioritized.

CONCLUSION

Social media has become an integral part of modern life, providing significant benefits in communication, networking, and content sharing. However, its widespread use also presents critical threats to internal security, such as radicalization, misinformation, cyberbullying, and privacy concerns. To address these threats, governments are taking multi-faceted actions, including advisories, financial assistance to law enforcement, partnerships with academic institutions, and legal measures to enforce compliance with regulations.

PRELIMS QUESTIONS:

Q. Which of the following statements are correct regarding the challenges posed by social media to internal security?
1. Misinformation on social media can lead to public confusion and unrest.
2. Cyberbullying and online harassment do not significantly affect social cohesion.
3. Anonymity on social media can protect harmful individuals from accountability.
Select the correct answer using the code given below:

A. 1 and 2 only
B. 2 and 3 only
C. 1 and 3 only
D. 1, 2 and 3
Answer: C

MAINS QUESTIONS:

Q. Critically examine the government's approach to tackling the threats posed by social media to internal security, focusing on measures such as content moderation, legal action, and international cooperation. (250 words, 15 marks)

Munde Dhananjay Navnath