

Q.1) How can social media influencers become a threat to India's national security? What laws and rules help the government deal with these risks? (150 words, 10 marks)

Introduction

With their vast online reach, social media influencers can significantly **shape public opinion**. In 2023, an influencer from Punjab used Instagram and YouTube to promote pro-Khalistan views, highlighting the potential threats influencers pose to national security.

Body

How Influencers Can Threaten National Security

- 1. Spreading Misinformation:** Fake news about communal issues, military operations, or natural disasters can trigger panic or violence. Example: During **COVID-19**, some promoted fake cures, causing panic buying.
- 2. Propaganda and Radicalization:** Foreign-sponsored influencers may promote anti-India narratives or extremist ideologies. Example: Pro-Khalistan accounts incited unrest during the **Amritpal Singh** crackdown.
- 3. Cyber Espionage:** Influencers sharing sensitive geolocation or troop data can compromise secrecy. Example: In 2020, some YouTubers shared troop movements during the **Galwan** standoff.
- 4. Economic Disruption:** Promoting scams or crypto schemes can destabilize trust. Example: The '**Morris Coin**' scam duped many investors.
- 5. Undermining Democratic Institutions:** Fake election-related content can erode trust in democratic processes.
- 6. Deepfake Technology:** Influencers using AI impersonations can mislead the public and authorities.



Legal and Regulatory Measures

- 1. Information Technology (IT) Rules, 2021:** Mandates due diligence for social media platforms and empowers flagging of fake or harmful content.
- 2. Bharatiya Nyaya Sanhita (BNS):** Sections on sedition, promoting enmity, and public mischief apply to harmful online acts.
- 3. Unlawful Activities (Prevention) Act (UAPA):** Allows action against influencers promoting terrorism or anti-national content.
- 4. Broadcasting Services (Regulation) Bill (proposed):** Aims to regulate OTT and digital content, including influencers.

5. **Digital Personal Data Protection Act, 2023:** Prevents misuse of personal data by influencers and platforms.
6. **FEMA & FCRA:** Used to monitor foreign funding or business deals that may affect national interests.

Way Forward

1. **Stronger Vetting and Monitoring:** Set up AI-driven monitoring cells to detect coordinated harmful content early, especially during sensitive events like elections or crises.
2. **Influencer Code of Conduct:** Introduce mandatory training and certification for influencers on responsible content creation and national security awareness.
3. **Collaborative Fact-Checking Framework:** Encourage collaboration between government, civil society, and platforms to flag and counter disinformation rapidly.

Conclusion

India must strengthen enforcement and digital literacy. Adopting global models like the EU's **Digital Services Act** can help build accountability while ensuring free expression remains protected and national security safeguarded.

Q.2) The UN Convention on Cybercrime marks a major step in global efforts to combat cyber threats. Highlight its key provisions and analyze its significance for India in addressing cross-border cybercrime challenges. (150 words, 10 marks)

Introduction

The UN Convention on Cybercrime, adopted by the UN General Assembly in **2024**, provides the first legally binding global framework to address cybercrime through cooperation, jurisdiction, and procedural tools—vital for digitally expanding nations like India.

Body

Key Provisions of the Convention

1. **Criminalisation of Core Cyber-Offences:** Establishes offences such as hacking, identity theft, fraud, child exploitation and ransomware as crimes.
2. **Procedural Tools for Investigation:** Enables preservation of electronic evidence, real-time data interception orders, and expedited search and seizure.
3. **International Cooperation Mechanisms:** Mandates mutual legal assistance, designation of 24/7 contact points, data sharing, and joint cross-border investigations.
4. **Human Rights Safeguards:** Includes privacy protections, respect for due process, and limits on surveillance powers.
5. **Capacity Building for Developing States:** Promotes technical assistance, training, and resource sharing, especially for developing countries.

Significance for India

1. **Bridging Jurisdictional Gaps:** Facilitates action against cybercrimes originating abroad, including phishing and ransomware affecting Indian users.
2. **Strengthening Law Enforcement Agencies :** Supports Indian agencies like **CERT-In**, **NCIIPC**, and **NIA** in gathering and sharing digital evidence internationally.
3. **Legal Harmonisation:** Pushes reform of the **IT Act, 2000** and aligned laws to meet global standards and obligations under the convention.
4. **Enhancing Citizen Trust:** Strengthens protections for digital payments, personal data, and public infrastructure security.
5. **Global Leadership Role:** Shows India's willingness to lead in crafting a trusted, secure global digital order.

Way Forward

1. **Amend Domestic Laws:** Revise the IT Act and allied legislation to reflect provisions of the Convention.
2. **Build Institutional Capacity:** Train law enforcement, judiciary, and cyber investigators in new cross-border procedures.
3. **Deepen International Links:** Participate in bilateral and multilateral initiatives, including with **CBI's Bharatpol** and **I4C** under MHA.
4. **Public Awareness and Collaboration:** Raise citizen awareness on cyber hygiene and encourage reporting of cybercrime.

Conclusion

India's involvement in the **UN Cybercrime Convention** enables it to close jurisdictional gaps, enhance LEA capacities, and modernise cyber laws. Effective ratification and coordination will be critical to combat global cyber threats.

Q.3) What is the Integrated Theatre Command (ITC) system? Critically evaluate its need and challenges in the Indian context. (150 words, 10 marks)

Introduction

Recommended by the **Shekatkar Committee**, the Integrated Theatre Command (ITC) aims to integrate the Army, Navy, and Air Force under a **unified command structure** for better synergy in planning and execution of operations.

Body

Need for ITC in the Indian Context

1. **Operational Efficiency:** Helps in joint planning and resource optimization, especially crucial in a two-front war scenario.
2. **Cost-effectiveness:** Avoids duplication of assets across services, ensuring optimal use of budget and resources.

3. **Quicker Decision-making:** A unified command facilitates faster response to emerging threats.
4. **Global Practice:** Countries like the **USA and China** have adopted integrated commands, showcasing its strategic relevance.

Challenges in Implementation

1. **Inter-service Rivalry:** Lack of consensus among services regarding structure and command hierarchy.
2. **Theatre Demarcation:** Geographical and functional boundaries for theatres remain contentious.
3. **Human Resource Integration:** Aligning training, culture, and promotional pathways is a complex task.
4. **Lack of Doctrine:** Absence of a comprehensive joint doctrine for integrated operations.

Way Forward

1. **Clear Legislative Mandate:** Define the roles and responsibilities of ITC through proper legislative backing.
2. **Capacity Building:** Invest in joint training and shared infrastructure to facilitate integration.
3. **Consensus Building:** Encourage dialogue among services to resolve disagreements.
4. **Phased Implementation:** Start with pilot commands and scale gradually based on learnings.

Conclusion

With 2025 declared the “**Year of Reforms**,” empowering the **CDS to issue joint orders** marks a pivotal step toward integration and strengthens India’s path to establishing functional Integrated Theatre Commands (ITCs).

Q.4) What are the new methods used for money laundering and terrorist financing as highlighted in FATF’s 2025 update? How can India improve its efforts to tackle these threats at both national and global levels? (250 words, 15 marks)

Introduction

Money laundering is the process of **making illegal proceeds appear legal**. As per FATF’s 2025 update, evolving technologies and globalized finance are enabling new laundering and terrorist financing methods, challenging India’s national and international enforcement systems.

Body

New Methods Identified by FATF (2025)

1. **Use of Cryptocurrencies and Virtual Assets:** Terror groups use virtual currencies for anonymous cross-border transfers.

2. **Trade-Based Money Laundering (TBML):** Mis-invoicing and over/under-invoicing in international trade hide illicit funds.
3. **Crowdfunding Platforms:** Misused for raising funds under humanitarian pretexts.
4. **Shell Companies and Complex Ownership Structures:** Layering ownership across jurisdictions to obscure sources.
5. **Smurfing via Digital Wallets:** Splitting transactions into small amounts through mobile wallets or prepaid cards.

India's National Efforts to Tackle These Threats

1. **Strengthening Enforcement Directorate under PMLA:** Empowering the ED to track, seize and prosecute laundered assets.
2. **FIU-IND Monitoring:** Financial Intelligence Unit analyses suspicious transaction reports from banks and financial institutions.
3. **Digital KYC and Aadhaar Integration:** Ensures customer due diligence across platforms.
4. **Crackdown on Illicit Crypto Exchanges:** Recent ED actions against unregulated exchanges show rising vigilance.
5. **Amendments to Unlawful Activities (Prevention) Act (UAPA):** Enables designation of individuals and freezing of assets linked to terrorism.

India's Global Engagements and Cooperation

1. **Active FATF Participation:** India supports global standards and regularly updates compliance frameworks.
2. **Bilateral Treaties and Information Exchange:** Agreements with nations to trace and repatriate black money.
3. **Membership in Egmont Group:** Enhances global cooperation among FIUs for intelligence sharing.

Conclusion

India must combine strict laws like **PMLA** with global coordination and technological surveillance. As global norms evolve, India's proactive participation and adaptive enforcement will be key to countering financial crimes.



Q.5) What is hybrid warfare? Discuss the emerging threats it poses to India's national security and suggest measures to strengthen India's preparedness against such challenges. (250 words, 15 marks)

Introduction

Hybrid warfare refers to a blend of conventional warfare, irregular tactics, cyber operations, disinformation campaigns, and economic coercion. It exploits a nation's vulnerabilities across **multiple domains**, posing **new-age threats** to India's national security.

Body

Emerging Hybrid Warfare Threats to India

- 1. Cyber Attacks on Critical Infrastructure:** Attacks have targeted power grids and health systems.
Example: Malware attack on Maharashtra's grid (2020); AIIMS cyber breach (2022).
- 2. Disinformation & Influence Operations:** Social media used to polarize and spread fake narratives.
Example: Disinformation during Delhi riots (2020); Manipur unrest (2023).
- 3. Terrorism and Insurgency with Cross-Border Support:** Drones used to smuggle arms and aid terror groups. Example: Drone arms drops in Punjab (2022); Reasi attack on pilgrims (2024).
- 4. Economic and Trade-Based Pressure:** Disrupting supply chains to create dependence. Example: API supply shocks during COVID; EV disruptions due to lithium issues (2024).
- 5. Maritime and Grey-Zone Tactics:** Civilian vessels used for surveillance in Indian waters. Example: Chinese ships near Andamans (2022).

Measures to Strengthen India's Preparedness

- 1. Integrated Cyber Defence Framework:** Strengthen CERT-In, military-civilian coordination, and real-time threat sharing.
- 2. Strategic Communication Units:** Establish agencies to counter disinformation and fake news.
- 3. Modernization of Armed Forces with Jointness:** Roll out Theatre Commands and invest in AI, drones, EW.
- 4. Public Awareness and Digital Literacy:** Educate citizens on digital hygiene and misinformation.
- 5. Multi-Domain Task Forces:** Civil-military teams for hybrid threat response.
- 6. Enhanced Maritime Surveillance:** Expand radar networks and ship tracking capabilities.

Steps Already Taken by India

- 1. Creation of Defence Cyber Agency:** Protects military assets from cyber threats.
- 2. Banning of Hostile-Origin Apps:** Chinese-origin apps banned over data and influence risks.
- 3. New IT Rules and Fact-Check Units:** Counter misinformation online.
- 4. Induction of Advanced Technologies:** Use of **AI and drones** on sensitive borders.

Way Forward

1. **Formulate a National Hybrid Warfare Strategy:** Define roles for civil, military, and intelligence agencies.
2. **Strengthen Global Partnerships:** Collaborate with like-minded countries on cyber norms and maritime security.
3. **Capacity Building and Red-Teaming:** Regular drills **simulating hybrid attacks** across sectors.

Conclusion

Hybrid warfare demands proactive defence. India must adopt a **whole-of-nation approach**—blending **technology, coordination, and foresight**—to protect its sovereignty and democratic institutions from emerging multi-domain threats.