Discuss the evolving methods used by non-state actors, including terror outfits and transnational criminal networks, to exploit porous borders and digital platforms.

Question Understanding – Finding Information

- **Precise Syllabus Mapping:** Role of external state and non-state actors in creating challenges to internal security.

(GS Paper – III)

- **Marks and words limit:**
  - The marks-oriented approach to answering **(10-mark, 150-word)** questions in the question is to use **Bullet Points** (one idea per bullet point), **Brainstorming**, or a combination of both.
  - The way to score good marks in questions worth **(15 marks. 250 words)** is to use the **Heading** and **Subheading** method while writing your answers.

- **Directive words**
  - Discuss → Explain methods with breadth and examples, showing evolution and linkages

- **Focal points of the questions:**
  - Evolving methods of non-state actors
  - Exploitation of porous borders
  - Exploitation of digital platforms
  - Coverage of terror outfits and transnational criminal networks

Answer Writing Structure (Outline)

Introduction Paragraph

- Define non-state actors
- Mention convergence of physical and digital spaces

Body Paragraph

A. Evolving Methods Exploiting Porous Borders

➢ ***Dos & Don'ts: Focus on operational adaptation, not geography.***

- **Infiltration and Mobility Tactics**
  - Use of difficult terrain, riverine and coastal routes
  - Forged identities and document fraud
- **Smuggling and Logistics Networks**
  - Arms, narcotics, counterfeit currency
  - Use of local intermediaries and informal routes
- **Cross-Border Safe Havens**
  - Exploiting weak law enforcement zones
  - Frequent relocation to evade surveillance
- **Convergence of Terrorism and Crime**
  - Drug trafficking and extortion to fund terror activities
  - Shared logistics between criminal and terror networks

B. Evolving Methods Using Digital Platforms

- **Recruitment and Radicalisation**
  - Social media propaganda and encrypted messaging
  - Targeting vulnerable individuals online
- **Financing and Money Laundering**
  - Use of digital payments, cryptocurrencies
  - Hawala networks integrated with online tools
- **Operational Planning and Communication**
  - Encrypted platforms and dark web
  - Virtual coordination across borders

- **Cyber-Enabled Crimes**
  - Identity theft, online fraud and cyber-extortion
  - Use of cyber tools to support physical operations

C. Why These Methods Are Effective

- Low cost, anonymity, speed and deniability
- Jurisdictional and regulatory gaps
- Difficulty of real-time cross-border coordination

Conclusion (max. 40 Words)

- Synthesize information

Dos & Don'ts

- **Do for Maximum Marks**
  - ✓ Use Key terms: Hybrid threats, Non-traditional security challenges, Terror-crime nexus
  - ✓ You can use this Brainstorming idea: Border routes + Digital platforms → Operations → Impact
  - ✓ Show evolution and adaptation, not static methods
  - ✓ Balance physical border and digital domain aspects
  - ✓ Maintain analytical and objective tone
  - ✓ Link terrorism and organised crime where relevant

- **Don't do these Common Mistakes**
  - × Do not narrate specific terror incidents
  - × Avoid naming operational tactics in excessive detail
  - × Do not sensationalise violence
  - × Avoid GS-II diplomatic focus
  - × Don't ignore cyber and digital dimensions

Notes Oriented Content for Writing Answer

In the Indian context, non-state actors (NSAs) such as terror outfits (e.g., Lashkar-e-Taiba, ISIS modules) and transnational criminal networks have shifted from traditional infiltration to a hybrid warfare model. They leverage India's porous land and maritime borders alongside the anonymity of digital platforms to bypass conventional security.

Exploitation of Porous Borders

Non-state actors exploit geographical vulnerabilities to facilitate the "crime-terror nexus," where smuggling profits fund militant activities.

- **Drone-Based Logistics:** In 2025-2026, there has been a surge in the use of commercial drones to drop arms, ammunition, and narcotics across the Indo-Pak and Indo-Myanmar borders.
- **The Narco-Terror Corridor:** Criminal syndicates use under-policed stretches in Punjab and Jammu & Kashmir to smuggle high-value drugs (e.g., heroin). The proceeds are then funnelled into terror modules via illegal hawala channels.
- **Safe Havens in Neighbouring Regions:** Insurgent groups in the Northeast (e.g., ULFA, NSCN) exploit the hilly, unfenced terrain of the Indo-Myanmar border for training and tactical retreats.

Exploitation of Digital Platforms

The digital landscape has become a virtual "battlefield" where NSAs operate with minimal physical presence.

- **Online Radicalization and Recruitment:** Platforms like Telegram, Signal, and YouTube are used to target vulnerable youth through encrypted channels. **Example:** In January 2026, Punjab Police arrested a minor from Pathankot who was digitally groomed by ISI handlers via social media to leak defence-related information.
- **Digital Tradecraft & Financing:** Terrorists now use "unconventional apps" and private servers to exchange layouts and instructions while avoiding surveillance. **Example:** Investigators have uncovered ISIS-linked modules using cryptocurrency donations and payment services like PayPal to move funds globally while masking identities through VPNs.
- **E-commerce Weaponization:** Legitimate marketplaces are exploited to procure materials for IEDs. For instance, the Pulwama attack involved purchasing chemical precursors through common e-commerce sites.

- **The Dark Web:** This is increasingly used for the illegal trade of firearms and psychotropic substances, allowing sellers and buyers to remain anonymous while bypassing national customs.

Recent Strategic Responses (2025-2026)

India has countered these evolving threats with advanced technology and policy frameworks:

- **CIBMS & Smart Fencing:** Implementing the Comprehensive Integrated Border Management System, which uses thermal imagers, seismic sensors, and laser fencing to secure sensitive borders.
- **National Terror Databases:** The launch of the National Terror Database Fusion and Analysis Centre (NTDFAC) and the Organized Crime Network Database (OCND) in late 2025 to enable real-time data sharing between central and state agencies.
- **AI-Driven Surveillance:** Adoption of AI tools for predictive policing, facial recognition at transit hubs, and behaviour modelling to detect online radicalization.

In essence, non-state actors present a persistent and evolving challenge by blending physical cross-border activities with sophisticated digital strategies, requiring a multi-pronged counter-response from Indian security agencies.

***