

Digital Platforms and Terror Financing

Posted at: 09/07/2025

Digital Platforms and Terror Financing: FATF's Latest Warning

Context

The Financial Action Task Force (FATF), in its recent report titled 'Comprehensive Update on Terrorist Financing Risks', has flagged the rising misuse of digital platforms such as ecommerce, VPNs, online payment systems, and social media in terrorist financing. The report draws attention to major incidents like the Pulwama terror attack (2019) and the Gorakhnath Temple attack (2022), both of which involved the exploitation of such platforms.

About FATF

- Established: 1989, at the G7 Summit in Paris
- Nature: An intergovernmental policy-making body
- Objective: To combat money laundering (ML), terrorist financing (TF), and related threats to the global financial system
- Headquarters: Paris, France, operating under the OECD
- Members: 39 members (including 37 jurisdictions and 2 regional organisations European Commission and Gulf Cooperation Council)
- India's membership: Became a full member in 2010, enhancing its global credibility

Key Functions of FATF:

- Develops 40 International Recommendations on ML and TF
- Conducts **Mutual Evaluations** of member countries

Maintains Grey List (watch list) and Black List (high-risk jurisdictions)
Issues public statements and alerts

• Promotes legal, regulatory, and institutional reforms

Key Highlights of the Report

1. Misuse of Digital Platforms

- Terrorists exploited online payment services, VPNs, and e-commerce platforms
- In the Pulwama attack (2019), aluminum powder (used in IED) was purchased via Amazon
- In the Gorakhnath Temple attack (2022):
 - The attacker used **VPNs** to hide identity
 - Transferred ₹6.69 lakh (approx. \$7,736) internationally via PayPal
 - Received and sent funds to ISIL-linked foreign accounts

2. Social Media and Messaging Apps

• Social media platforms, messaging services, and crowdfunding websites are increasingly being exploited to raise and move terror funds

3. State-Sponsored Terror Financing

- The report notes that **some national governments** (unnamed) provide:
 - Direct funding

- Logistical support
- Training to terrorist groups
- Use **trade routes and smuggling** to bypass sanctions

4. Complex Financial Schemes

- Usage of commodity-based laundering models like:
 - ∘ Oil → Gold → Cash routes
 - Transactions spread across multiple jurisdictions to avoid detection

5. Decentralisation of Terror Networks

- Shift from centralised to local, self-financed terror cells
- These cells operate with:
 - Criminal proceeds
 - Small business investments
 - Local financial resources
- Example: Al-Qaeda in the Indian Subcontinent (AQIS) operates independently in India

6. Trade and Storage-Based Financing

- Use of gold and jewellery by groups like ISIL and Al-Qaeda in India to store small funds
- Growing reliance on **trade-based schemes** for laundering and financing operations

7. Additional Channels of Terror Funding

The report flags several other methods:

- · Human trafficking, wildlife smuggling, drug trade
- Virtual assets, crowdfunding, hawala, and mobile apps
- Shell entities, donation drives, and extortion
- Misuse of NGOs and non-profits

FATF's Earlier Warning: Pahalgam Attack

- Following the **Pahalgam terror attack (April 22, 2022)**, FATF emphasized:
 - Terror attacks are not possible without financial infrastructure
 - Announced a **detailed investigation** into emerging terror financing trends

Conclusion: Need for Global and Domestic Oversight

- The report highlights an **urgent global concern** over the **digitalisation of terror financing**
- Calls for:
 - Stricter regulations on digital payments and e-commerce
 - **Real-time monitoring** of financial transactions
 - **Global cooperation** for intelligence sharing and countermeasures