FATF Highlights Digital Platforms in Terror Financing: Pulwama & Gorakhnath Attacks

July 9, 2025 • vajiramandravi.com

FATF Terror Financing Report Latest News

- The Financial Action Task Force (FATF), in a report, highlighted that digital platforms—including online payments, VPNs, social media, and e-commerce—were misused in the Pulwama (2019) and Gorakhnath Temple (2022) terror attacks.
- The report, titled *'Comprehensive Update on Terrorist Financing Risks'*, serves as a global alert on the evolving and increasingly complex methods of terrorist financing.
- It warned that such platforms are increasingly being exploited for terror financing.

Financial Action Task Force (FATF)

- FATF is an intergovernmental policy-making body established in 1989 at the G7 Summit in Paris.
- Its primary objective is to develop policies to combat money laundering (ML), terrorist financing (TF), and other related threats to the integrity of the international financial system.

- **Headquarters –** FATF is headquartered in Paris, France, and functions out of the Organisation for Economic Co-operation and Development (OECD) headquarters.
- **Members**
    - FATF comprises 39 members, including 37 jurisdictions and 2 regional organizations (European Commission and Gulf Cooperation Council).
    - India became a full member of the FATF in 2010, which enhanced its global financial credibility.
- **Key Functions & Roles**
    - Setting International Standards for combating Money Laundering and Terror Financing through its famous 40 Recommendations.
    - Monitoring Compliance of member and non-member countries with those standards.
    - Conducting Mutual Evaluations to assess effectiveness of anti-money laundering and counter-terrorist financing measures.
    - Issuing Public Statements to identify high-risk and non-cooperative jurisdictions (also known as the FATF Grey List and Black List).
    - Encouraging Legal, Regulatory, and Operational Reforms in financial systems globally.

FATF Flags Rising Misuse of Digital Platforms for Terror Financing

- The FATF report highlights how terrorists involved in the Pulwama (2019) and Gorakhnath Temple (2022) attacks used online payment services, VPNs, and e-commerce platforms.
- It warns that social media, messaging apps, and crowdfunding sites are increasingly being exploited for financing terrorism.

State-Sponsored Terror Financing

- Without naming countries, the report notes that some national governments continue to financially and materially support terrorist organisations.
- This includes direct funding, logistical support, training, and sanctions circumvention via trade and smuggling.

Complex Financial Schemes

- The FATF also points to commodity-based schemes, such as oil-to-gold-to-cash transactions involving multiple jurisdictions, used to move terror funds while evading detection.

Decentralisation of Terror Networks

- The FATF report flags a global shift in terror operations towards decentralised structures, with regional financial hubs and self-financed cells adapting to local contexts.
- These cells use criminal proceeds, business investments, and local resources to sustain activities.

Pahalgam Attack and FATF’s Prior Warning

- The FATF condemned the April 22 Pahalgam attack, stating that such terror acts are not possible without financial support and money transfer mechanisms.
- It had announced plans for a detailed analysis on terrorist financing.

Storage and Trade-Based Terror Financing

- FATF also noted gold and jewellery being used for storing small funds by ISIL or Al-Qaeda-inspired individuals in India.
- Trade-based financing schemes and decentralised decision-making—like Al-Qaeda in the Indian subcontinent (AQIS) managing operations independently—reflect an evolving strategy in terror financing globally.

Other Channels of Terror Financing

- The report identified various other funding methods:
  - Human trafficking, wildlife smuggling, drugs, and virtual assets.
  - Donations, shell entities, shell accounts, and mobile apps.
  - Hawala routes, crowdfunding, extortion, and ransom collection.
  - Misuse of non-profit organisations.

Pulwama Attack: E-Commerce Misuse

- In the 2019 Pulwama attack, aluminum powder—a key component of the IED—was procured via Amazon, revealing how e-commerce platforms can be exploited for acquiring materials used in terror attacks.
- Authorities attributed the attack to Jaish-i-Mohammed, with evidence of cross-border movement of explosives.

Gorakhnath Attack: VPNs and Online Payments

- The 2022 Gorakhnath Temple attacker, influenced by ISIL ideology, used VPNs to hide his identity and PayPal to transfer ₹6.69 lakh ($7,736) internationally.
- He also received foreign funds and sent money to ISIL-linked individuals abroad. PayPal later suspended the account due to suspicious activity.

Conclusion: Exploitation of Digital Infrastructure

- The report underscores a growing trend of misusing digital tools—e-commerce, VPNs, and online payment systems—for planning, funding, and executing terrorist acts.
- This highlights the urgent need for regulatory oversight and monitoring.

Source: IE | TH | HT
