Emerging Technologies and Terror Financing: A Case Study of Pakistan

NUST Journal of International Peace & Stability
2026 Vol. 9(2) Pages 39-51
njips.nust.edu.pk
DOI: http://doi.org/10.37540/njips.v9i2.221

***Adnan Aftab[1] & Haseeb Hussain[2]**

Abstract
This study investigates the existential threat facing Pakistan, specifically in the context of terrorist financing through the lens of emerging technologies. It provides a comprehensive analysis of cryptocurrencies, mobile money platforms, and artificial intelligence, examining how these technologies facilitate the generation, movement, and concealment of funds by terrorist organizations. Furthermore, the paper explores the typologies of terrorist organizations operating in Pakistan, with particular emphasis on those that actively exploit technology-driven financial channels. Employing a qualitative inductive methodology, the research evaluates Pakistan's existing Counter-Terrorism Financing (CTF) framework, including its regulatory measures, preventive strategies, and enforcement mechanisms, to assess its capacity to address these evolving technological challenges. The study identifies structural, legislative, and enforcement deficiencies that remain inadequate in the face of rapid technological advancements and offers recommendations for adaptive, technology-driven policy reforms aimed at strengthening Pakistan's CTF framework and mitigating emerging risks.

Keywords
Terror financing, emerging technologies, cryptocurrency, darknet, digital transformation

Introduction
In 2024, the Institute of Economics and Peace reported that Pakistan is the second-most-affected country globally by terrorism, with terrorist incidents rising from 513 in 2023 to 5397 (Institute of Economics and Peace, 2024). Pakistan, the country with the largest share, faced 2,635 terrorist attacks between 2001 and 2024 (Reynie, 2024). The attacks resulted in 24000 fatal civilian casualties and 9000 security forces personnel. A further 35,000 civilians and 10,000 security personnel were injured in this onslaught

[1] *Corresponding Author: *Adnan Aftab is* an MPhil Scholar at the National Defence University (NDU), Islamabad, Pakistan.
E-mail: diplomat7ir@gmail.com
[2] *Haseeb Hussain* is a Research Officer at Maverick Digital, Rawalpindi, Pakistan.

Received 14 August 2025; **Revised** 26 April 2026; **Accepted** 27 June 2026; **Published online** 30 June 2026

(Reynie, 2024). The backbone of these rapidly growing attacks is Terror Financing (TF), because without it, organisations cannot recruit, move, or sustain themselves. Now the question arises: how does this TF occur when there are already strict laws worldwide? The answer is that, over time, terror financing methodologies have changed, with new avenues emerging as technologies advance.

TF refers to the collection, storage, movement, and use of funds by terrorist organizations to facilitate, support, or execute terrorist activities (United Nations, 2019). Although the traditional mechanisms of terrorist financing have been extensively researched and documented, the role of emerging technologies in enabling and transforming these financial networks remains comparatively underexplored. The increasing digitalization of financial systems, including cryptocurrencies, encrypted communication platforms, the darknet, Artificial Intelligence (AI), and digital payment systems, has significantly complicated efforts to detect and monitor the cross-border movement of illicit funds. As terrorist financing mechanisms continue to evolve, Pakistan's existing counter-terrorism and counter-terror financing frameworks have struggled to keep pace with this rapidly changing operational environment. Consequently, there is an urgent need to reassess existing regulatory frameworks and policy responses to effectively address these emerging technological threats.

This research paper is structured around three main objectives that examine how terror financing in Pakistan has evolved in the context of emerging technologies. First, it studies the typological framework of Pakistan, which includes Neo-Jihadi, ethno-nationalist, sectarian, and religious nationalist groups. After clarifying the topographic landscape of Pakistan, this research paper explores the mechanisms of terror financing vis-à-vis these typological networks. Lastly, it critically examines the challenges associated with TF in Pakistan and juxtaposes them with the existing policy frameworks, potential, and expertise.

Concept of Terror Financing

TF refers to the processes through which funds are generated, collected, stored, invested, transferred, and ultimately utilised to finance terrorist activities or provide support for terrorism. These funds may be used to facilitate the planning and execution of terrorist attacks or to sustain related activities, including logistics, recruitment, propaganda, training, and publicity (Global AML/CFT, 2025). The domain of terrorist financing has become increasingly complex due to the forces of globalisation and the rapid advancement of emerging technologies, which have fundamentally transformed the methods through which terrorist organisations raise, move, and conceal financial resources (S. A. A. Bukhari, personal communication, 2026).

A terrorist organization requires operational resources to function effectively, including kinetic operations, the training of operatives, logistics, and communication networks. These operational components require financial resources to carry out their respective functions. As the size and complexity of a terrorist organization increase, so do its financial requirements to sustain its organizational and infrastructural operations (Tsvetovat & Carley, 2005). For greater clarity, these operational requirements can be classified into two categories: ‘tangible resources’, such as weapons, explosives, and basic sustenance for operatives, and ‘intangible resources’, such as leadership, intelligence, operational planning, and the communication of ideology (Wolfberg, 2025).

Traditionally, the versatility of TF means that both legal and illegal means are equally potent in obtaining funds, and both are used to generate funds. Legal means

range from businesses to welfare organisations/NGOs, whereas illegal means include criminal activities of all sorts, especially drug trafficking, arms smuggling, human trafficking, and extortion (Levi & Reuter, 2006).

What distinguishes contemporary TF from the traditional one is the radical transformation of the funding mechanisms. Traditional mechanisms – Hawala and Hundi, Layering, and front offshore companies — continue to be used. However, these traditional methods are now increasingly integrated with technologies that offer greater speed and anonymity, with detection remaining rare.

Terrorism in Pakistan: A Typological Overview

As per 82 Organizations Proscribed by the Ministry of Interior u/s 11-B-(1) r/w Schedule-I, ATA 1997, and to avoid analytical challenges, it is necessary to treat them as a monolithic phenomenon (NACTA, 2024). In this regard, the research paper 'Trends of contemporary Terrorism in Pakistan' has provided valuable insight by classifying terrorist organisations into Neo-Jihadi, Sectarian, Ethno-Nationalist, and Religious Nationalist categories (Global and the Local, 2020). Each category is crucial to this paper's purposes, financing, and the technological adoption by terrorists as elaborated below:

Neo-Jihadi

The term neo-Jihadi refers to an evolution of violent extremism, combining radical ideologies with criminal activities and typically employing digital tactics (Global and the Local, 2020). Drawing on the prescribed terrorist list by the National Anti-Terrorism Authority (NACTA), this category includes Tehreek-e-Taliban Pakistan (TTP), also known as Fitna-al-Khawarij, and its affiliates, such as Pashtun Taliban, Jamat-ul-Ahrar (JuA), Hizb-ul-Ahrar (HuA), and the most recent Afghan Taliban regime. The neo-Jihadi classification rejects the nation-state as non-Islamic. It is committed to global jihad, making it transactional in ideology and operational logistics, and this adaptation draws on global financial channels such as foreign donations, remittance exploitation, and cryptocurrency. According to the Habilian 2024 report, 50% of the economy in this category is regulated through digitised channels (Habilian, 2024).

Ethno-Nationalists

This classification divides nationalists in Pakistan by ethnicity, including Baloch separatist organisations. The most prominent is the Baloch Liberation Army (BLA), also known as Fitna-al-Hindustan, operating under the umbrella of Baloch Raaji Ajoi Sangar (Verma et al., 2025). These are radicalised ethno-nationalist insurgent groups led primarily by an educated middle-class leadership. They maintain a dedicated suicide unit, known as the Majeed Brigade, and utilise diaspora networks through social media platforms for fundraising, while relying on encrypted communication channels for operational coordination (Global and the Local, 2020). Furthermore, their deliberate targeting of Pakistan's strategic assets, including gas pipelines and the China–Pakistan Economic Corridor (CPEC), has introduced an international dimension to their financial requirements (Iqbal, 2026).

The US Treasury's Office of Foreign Assets Control (OFAC) identified ZB's cryptocurrency exchange networks in 2022 and 2023, specifically identifying the use of Tether (USDT) on the TRON blockchain to circumvent sanctions — precisely the same instrument that TRM Labs (2025) identifies as accounting for 58% of illicit crypto volume globally (Chainalysis Team, 2026; TRM, 2025).

Sectarian Groups and Religious Nationalists

Sectarian groups, which are factions within a religion or political movement that adhere to rigid and separatist doctrines, such as Lashkar-e-Jhangvi (LeJ) and the Zainabiyyoon Brigade (ZB), primarily rely on external support, digital funding channels, and informal donations from sympathetic communities. In contrast, religious nationalist groups, which seek to merge religious identity with national identity, such as Jamaat-ud-Dawa (JuD) and Jaish-e-Muhammad (JeM), have historically depended on charity networks and foreign financial support rather than digital funding mechanisms (Verma et al., 2025).

Between 2020 and 2022, JuD was documented as adopting a decentralized digital fundraising model in which affiliated mosques and madrassas solicited contributions through WhatsApp-distributed QR codes linked to bank accounts registered in the names of peripheral associates rather than designated individuals (Andreopoulos, 2026). For example, in Lahore, Faisalabad, Muzaffarabad, and Mirpur, accounts registered using the identity documents of non-designated individuals enabled a financing network that generated an estimated PKR 180 million annually through digital channels (AAJ News, 2026). Similarly, in 2026, investigations by the Federal Investigation Agency (FIA) concluded that LeJ-linked fundraisers based in the Gulf were using hawala networks operating through the UAE and connected to EasyPaisa and UBL Omni accounts in Lahore and Multan to transfer operational funds to identified personnel via multiple low-value transactions (Bilal, 2026). This systematic use of numerous small-value transfers is consistent with the Financial Action Task Force (FATF) concept of 'smurfing' in a digital context, illustrating LeJ's adaptation of technology for financial operations.

Pakistan Geographical Location vis-à-vis Threat Spectrum

Pakistan has remained one of the primary targets of terrorism since the events of 9/11. The United States' invasion of Afghanistan resulted in significant casualties, widespread damage to infrastructure, increased pressure on state institutions, and the erosion of Pakistan's social fabric (Center for Preventive Action, 2025). Furthermore, Pakistan's complex socio-political landscape, coupled with its historical entanglements with militant groups following the Soviet-Afghan War, has created conditions that provide greater space for the persistence and evolution of terrorism (Center for Preventive Action, 2025). Pakistan's geographical location further compounds these challenges. Sharing borders with South, Central, and Western Asia, along with an extensive coastline on the Arabian Sea, the country faces considerable difficulties in securing its porous borders. This has facilitated the infiltration of terrorists and the cross-border smuggling of illicit goods. According to official reports by the United Nations Office on Drugs and Crime (UNODC), approximately 43% of drugs entering Pakistan originate from Afghanistan, representing an estimated illicit trade valued at USD 30 billion (Pietschmann, 2011). These interconnected challenges further exacerbate terrorism and, consequently, contribute to the financing of terrorist activities through illicit cross-border networks.

According to the South Asia Terrorism Portal (SATP) 2024 report, 12 domestic groups, 32 transnational terrorist organisations, and 4 extremist groups were operating in Pakistan (SATP, 2024). The TF from emerging technologies has now made Pakistan an ideal breeding ground for terrorism. According to the Global Terrorism Index 2025 (Institute for Economics and Peace, 2024), Pakistan ranked second globally

among terrorism-affected countries in 2024, behind Burkina Faso. These terrorists receive financing through the following means:

Drug Trafficking, Arms Smuggling, and Technology-Enhanced Criminality

Drug trafficking, arms smuggling, kidnapping for ransom (KFR), and extortion remain central to TF revenue generation for territorially operating groups. However, these traditional criminal revenue streams are increasingly mediated by technology, creating hybrid TF schemes that combine physical criminality with digital financial infrastructure. For example, 30% of TTP's income is increasingly settled through digital means, including mobile wallets and cryptocurrencies (Habilian, 2024). Moreover, terrorist organizations, along with emerging tactics of TF, share smuggling routes with organized criminal groups, which are ideal for obscuring the origins and destinations of funds.

However, KFR operations by TTP, BLA, and allied groups also benefit from digital financing methods. Ransom payments are now made digitally via cryptocurrency, reducing the need for collectors to be physically present. The BLA's extortion of the Baluchistan mining industry, which earns 4 million rupees per day, is increasingly channelled through mobile wallets and electronic payment systems. This methodology falls outside the current monitoring architecture in Pakistan (Shahid, 2025). Moreover, Jaish-e-Mohammed (JeM) is transitioning to Pakistani mobile payment systems such as Easy Paisa and SadaPay. Following disruptions to their normal funding channels, JeM operatives have used wallets linked to their leadership to make wallet-to-wallet transfers.

Emerging Technologies and Terror Financing in Pakistan

In 2026, while technology has provided a significant edge and reliable work speed, it has also posed serious challenges in Pakistan. Financial Technologies (Fintechs) have introduced significant transformation in the TF domain. In this regard, the FATF has explicitly recognised that digital media wallets, online banking, cryptocurrency, and other digital means pose risks that were not covered by existing regulatory frameworks, such as the Recovery of Finance Ordinance 2001, Anti-money laundering (AML), combating the financing of terrorism (CFT) & Countering Proliferation Financing (CPF) regulations, etc. (FATF, 2025). The subsequent analysis relies extensively on this taxonomy to provide the most recent delineation of global and Pakistani TF practices. Accordingly, the following analysis draws extensively on the FATF taxonomy to provide an up-to-date examination of global and Pakistani terrorist financing practices.

Driver 1: Globalization and Erosion of Financial Borders

Globalisation, the integration of financial markets, the growth of international remittances, and the emergence of new digital money transfer methods have reduced the geographical barriers to TF. Although these developments have made financial transactions faster and more convenient, they have also created new opportunities for terrorist organisations to raise, transfer, and conceal funds. Terrorist groups exploit free trade zones, offshore financial centres, and weak regulatory systems to move money with limited oversight. Prominent examples include the 2004 Madrid bombings, which cost approximately USD 10,000, and the 9/11 attacks, which were estimated to have cost around USD 500,000 (Messenger, 2026). Similarly, the 2021 TTP vehicle-borne improvised explosive device (VBIED) attack was financed through reactivated dormant bank accounts (Ahmed, 2024). Investigations by the Financial Monitoring

Unit (FMU) later revealed that the financier had received remittances totalling PKR 250,000 (Financial Monitoring Unit, 2021). Because these were small-value transactions, they remained undetected under the existing regulatory framework. To address such vulnerabilities, the United Nations Office on Drugs and Crime (UNODC) conducted training for Pakistan's real estate sector in 2026 to improve the reporting of Suspicious Transaction Reports (STRs) and strengthen the detection of illicit financial activities (UNODC, 2026).

Driver 2: Cryptocurrency and Decentralized Finance

Cryptocurrency and Decentralised Finance (DeFi) pose a serious threat to traditional methods of TF, offering blockchain-based solutions that provide pseudo-anonymity and irreversible transactions, as seen with Bitcoin, Ether, Zcash, and Monero. Market science and GNet reports highlight several TF-specific misuse patterns, including the use of privacy coins to obscure transaction trails, the exploitation of peer-to-peer exchanges that lack Know Your Customer (KYC) protocols, and the exploitation of Non-Fungible Tokens (NFTs), such as Treasure NFT, which was initially used by ISIS (Spyra et al., 2025).

During 2014-2015, IS/Daesh was among the first terrorist organisations to use Bitcoin donations in documented campaigns. In 2021, the US Department of Justice seized over 1 billion dollars in cryptocurrencies linked to TF (Movchan et al., 2023). Moreover, amid increasing transaction complexities, terrorist actors are migrating to privacy-focused coins such as Monero and to DeFi platforms, which enable financial transactions without intermediaries.

In Pakistan, the TTP has also incorporated cryptocurrency into its online operations vis-à-vis Bitcoin wallet addresses on Telegram and other social media platforms (Zia Khan Dawar & Afridi, 2021). These currencies are typically exchanged into Pakistani Rupees through dark web exchanges and Peer-to-peer (P2P) exchanges on online exchanges such as Binance.

Driver 3: Digital Wallets and Fintech Platforms

TF has found Digital Wallets and Fintech Platforms appealing because they are fast and easily accessible across borders. For example, to collect extortion in Somalia, Al-Shabaab has organized the exploitation of mobile money services in Kenya, such as M-Pesa, EVC-Plus, Sahal, and Zaad (Mohamed, 2023). Then funnelling millions of dollars each year to fund terror-related activities. In response, the 2023 crackdown is one of the most notorious examples, as the Somali government froze 70 associated mobile money accounts, but others remain unidentified (Feyissa & Gebresenbet, 2026).

As far as Pakistan is concerned, by the end of fiscal year 2023-24, the State Bank of Pakistan's (SBP) Payment Systems Review recorded about 130 million mobile wallet accounts registered across various platforms, with quarterly transaction volume exceeding 2.1 trillion rupees (State Bank of Pakistan, 2024). These platforms are powered by Jazz Cash, Easy Paisa, and Sada Pay. In 2021, Pakistan launched the RAAST instant payment system to secure person-to-person and bulk transactions, but even with Level 1 RAAST accounts proliferating, TF remains ongoing (Shah & Zaidi, 2025). Moreover, in the ethno-nationalist sphere, the Counter Terrorism Department (CTD) also finds that financing for the BLA is now being channelled through digital means. Hence, 4 million rupees per day in extortion income derived from the mining and construction businesses in Baluchistan is now being channelled through Jazz Cash and informal mobile money wallets.

Driver 4: Virtual Assets (VA)

The use of virtual assets (VA) in TF is not easily measurable. The FATF affirms that VA use by terrorist organisations is growing worldwide. Meanwhile, Bitcoin is the leading VA in TF fundraising campaigns. Terrorist groups are systematically using stablecoins (especially USDT/Tether) because of their price stability, lower fees, and perceived difficulty of tracking. Another VA, Monero, with a cryptographic architecture that offers strong transaction obfuscation, is commonly used in TF. TRM Labs (2025) found that 58% of illegal crypto volume in 2025 was in TRON-based stablecoins (USDT) (TRM, 2025). The al-Siddiq wing of ISKP specifically requests Monero (XMR) because of its privacy-focused, untraceable nature in TF in Pakistan, Afghanistan, India, Bangladesh, and the Philippines (TRM, 2025).

Moreover, the FIA and NACTA have identified a trend in TF called 'hybrid financing' (Virk, 2023). In this emerging trend, legitimate DeFi activities are being exploited to conceal the rise of automated TF enabled by AI tools. This makes suspicious financial flows appear like normal high-frequency trading, thereby complicating the pattern-detection methods used by current AML systems.

Emerging Technologies and the Evolving Landscape of TF in Pakistan

Pakistan's approach to TF has traditionally focused on conventional financial measures, including cash surveillance, the disruption of hawala networks, and the prosecution of financing-related offences. At the same time, Pakistan's successful removal from the FATF Grey List in October 2022 demonstrates the country's sustained legislative and institutional reforms. However, the emergence of financial technologies (FinTech) has introduced new challenges that extend beyond compliance with existing regulatory standards. In Pakistan, a significant gap remains between the progress achieved during the post-FATF Grey List period, particularly in strengthening the AML and CFT framework, and the evolving risks posed by emerging technologies. This gap presents a major challenge for Pakistan's counter-terrorist CTF policy. Accordingly, the following discussion examines these challenges at three levels: legislative, institutional capacity, and international:

Legislative Level

At the legislative level, the primary issue is the lack of clear legal guidelines for VA. For example, SBP warned about loopholes that could mitigate the risks of digital TF but did not fully ban or regulate cryptocurrency activities, which has resulted in an increase in terrorism. The SBP's current prohibition-leaning approach has unintentionally created a regulatory gap, and although Pakistan has legalised VA, this gap continues to persist (Iqbal, 2026). As a result, detecting VA-related transactions has become more difficult than monitoring transactions on supervised exchanges that follow standardised KYC procedures. Furthermore, the absence of a formal licensing and KYC framework for VA service providers has pushed cryptocurrency activity towards unregulated peer-to-peer networks, which are considerably less transparent than supervised exchanges. Consequently, the rapid growth of cryptocurrency uses in Pakistan, India, and Bangladesh, combined with weak AML/CFT requirements, has created a threat environment in which terrorist groups can exploit cross-border digital transactions with a relatively low risk of detection (Dave, 2025).

Pakistan's current legal framework also falls short across the broader landscape of technology-enabled TF. According to the Islamabad Policy Research Institute (IPRI) policy brief on Terrorism and Evolving Technologies, there are

significant gaps in Pakistan's Anti-Terrorism Act (Khanum, 2026). This includes: a lack of recognition of AI-generated propaganda as criminal, the misuse of encrypted communications for financial coordination, and the use of anonymous digital financing tools. This legislative gap is crucial because groups like TTP and BLA are already utilizing drones for reconnaissance, and the increasing use of AI-generated propaganda in languages such as Urdu and Pashto is lowering the barrier for recruitment and financial campaigns targeting Pakistani audiences.

Institutional Capacity

Institutional capacity is equally crucial for addressing the counter-strategy challenge. Rousselle (2025) highlights an enforcement gap in counter-TF and outlines a three-tier illicit liquidity framework. Tier 2 comprises over-the-counter brokers, poorly regulated digital exchanges, and crypto-enabled shadow banking networks, which link elite capital flows to terrorist financing at the operational level (Rousselle, 2025).

Moreover, Pakistan's FMU lacks the blockchain analytics capabilities necessary to understand these connections. Neither FIA's cybercrime division nor NACTA has publicly shown a dedicated digital TF intelligence function. So, implementing AI-powered investigative tools, such as wallet clustering, transaction graph analysis, and automated laundering pattern detection, is now an urgent operational need rather than a future goal. For example, groups within the ISKP's al-Siddiq financial network have been actively financing operations across Pakistan through these Tier 2 intermediary channels. (FATF, 2025; Rousselle, 2025).

Additionally, micropayment and creator-economy features on encrypted messaging apps pose a serious threat. Bindner and Gluck (2026) describe how, in the Middle East, terrorists have used Telegram channels and Telegram Stars – the platform's in-app currency – as a fundraising tool. Users earn Stars through interactions, which are then converted into Toncoin and cashed out via the TON ecosystem's privacy features (Bindner & Gluck, 2026). This process effectively obscures the financial trail from both law enforcement and the platform after the Stars are redeemed off-platform.

This typology is also highly pertinent to Pakistan's threat landscape: Telegram has been well documented as the main platform for communication and fundraising for both TTP and BLA propaganda efforts aimed at Pakistani-language audiences. Consequently, using these channels for micropayment exploitation is a plausible and insufficiently monitored method of terrorist financing (Bindner & Gluck, 2026).

International Level

At the international level, Pakistan's counterstrategy lacks a multilateral framework. Pakistan should more assertively engage with the multilateral framework of technology-specific counter-TF obligations. UNSCR 1373 requires all countries to criminalise financing and support for terrorism (United Nations Security Council, 2001), including online fundraising and digital payments. Meanwhile, UNSCR 2462 urges countries to enhance oversight of virtual assets and emerging financial technologies (United Nations Security Council, 2019; IPRI, 2026). Pakistan's National Action Plan 2021-2026 (NAP) is comprehensive, but still lacks a specific framework for implementing these obligations through technology.

Hence, Pakistan's CTF strategy has bolstered traditional institutions but still lacks a digital dimension. The aim is not to replace existing systems but to strengthen them by implementing virtual asset regulations, AI-based financial intelligence, platform-specific agreements, and revised laws to prevent terrorists from exploiting new digital technologies, where opponents can operate with little restriction.

Towards a Resilient CTF Framework

The way forward is divided into 3 parts: the legislative level, Institutional capacity, and the regional and international level.

Legislative Level: From Prohibition to Supervised Integration

At the legislative level, one of the best examples is the digital financing regulatory model of the United Arab Emirates (UAE) and the European Union (EU). Following the FATF and the Middle East and North Africa Financial Action Task Force (MENAFATF) recommendations, the UAE established the Virtual Assets Regulatory Authority (VARA) network. The VARA is a tiered licensing system that allows exchanges to operate under different compliance levels depending on their risk profiles. As a result, UAE authorities observed and then halted a 47% rise in suspicious transaction disclosures from the virtual asset sector. This increase was not due to a rise in illegal activities but to the regulation requiring entities. In contrast, the EU has established the Crypto-Assets (MiCA) regulation, which, in cooperation with the EBA, EIOPA, and the ECB, requires Travel Rule compliance for all crypto-service providers (CASPs). This rule requires the transmission of originator and beneficiary details for transfers over €1,000.

Given Pakistan's geographical and economic conditions, it does not need to fully adopt either the UAE or the EU model for its financial regulatory system. Pakistan's political economy differs significantly from those of the UAE and the EU. However, the key takeaway from the comparative analysis is as follows:

- Pakistan should adopt a formal supervisory framework to help VA service providers generate more practical financial intelligence rather than resorting to outright exclusion.
- Pakistan's threat vectors are different from those of any other country in the world. Therefore, its licensing regime should be tailored to Pakistan's specific needs, including the exploitation of P2P exchanges, stablecoin transfers, and crypto-to-mobile money conversions.

Institutional Level: Blockchain Analytics and Dedicated Digital TF Intelligence

At the institutional level, the UK's Financial Intelligence Unit is known to use Chainalysis Reactor, a US-sourced blockchain analysis tool, and Elliptic Enterprise, a similar British tool. These tools have proven useful for monitoring cryptocurrency transactions across wallet clusters and exchange-level conversion points. From Pakistan's perspective, they can be used to monitor fund transfers, including those converted from cryptocurrency to Pakistani rupees, by the TTP and BLA (U. Pervaiz, personal communication, 2026).

In line with the recommendations, a designated Digital Terror Financing Intelligence Cell (DTFIC) should be established within NACTA, comprising FMU analysts, SP examiners, and the FIA Cybercrime wing. For inspiration, an operational model can be based on the UK's Joint Money Laundering Intelligence Taskforce (JMLIT). This will facilitate real-time intelligence coordination between law enforcement and financial institutions to understand and analyse emerging TF methods. This will also curb vulnerabilities that result from the use of banned payment networks, including Jazzcash, Easypaisa, and Telegram, by preventing exploitation of loopholes.

Regional and International Level

Internationally, Pakistan's core security concerns, exposure to TTP, BLA, and similar terrorist networks, demand multilateral CFT coordination rather than symbolic discussions. One such example is the FATF's Operational Network, established in 2023. It goes beyond strategic policy discussions to foster direct operational collaboration between FIUs on TF cases. Such initiatives are crucial in enabling Pakistan's access to Blockchain tracing and virtual assets intelligence capabilities from FIU groups such as FinCEN, the UK's NCA, and Germany's FIU, specifically focused on terrorist network nodes. It is recommended that, in order to enhance operational intelligence coordination, cases featuring virtual assets should be formally categorized. A classification that enables eligibility for Egmont Ground Emergency Exchanges should be utilized.

SCO's Regional Anti-Terrorist Structure (RATS) could also be leveraged at the regional level to encourage crypto-specific intelligence coordination through multilateral negotiations. This protocol would draw attention to the Afghan-Pakistan-Central Asia Corridor, a route exploited by terrorist groups, including the TTP, for cross-border terrorism. Similarly, the Association of Southeast Asian Nations (ASEAN) is an effective platform for assessing financial crime. For example, ASEAN's working group on Financial Crime concluded in 2022 that mobile money monitoring protocols can deliver operational results within 2 to 3 years. Finally, government-to-platform agreements with major corporations such as Telegram, Meta, and the TON ecosystem are important for an adaptive CFT response. However, adopting legislation such as the UK's Online Safety Act 2023 could exceed the bureaucratic and legislative capacity at this time. Alternatively, bilateral information-sharing mechanisms with such platforms, focused on flagged account activity, will be useful (K. Iqbal, personal communication, 2026).

For example, Nigeria and Kenya's efforts against platform-based fundraising for groups like Al-Shabaab and Boko Haram. Moreover, a legal instrument such as a Digital Platform Counter-Terrorism Financial Cooperation Ordinance could enable platform disclosure orders targeting the financial networks of terrorist organizations, thereby satisfying international due-process standards and providing actionable financial intelligence.

Conclusion

In conclusion, this paper explores how TF has shifted from incremental to qualitative change. The four drivers of globalisation-enabled financial permeability, cryptocurrency transfers, fintech exploitation, and AI-driven obfuscation work together to evade detection. A TF operation using Telegram, EasyPaisa wallets, P2P crypto exchanges, and AI tools represents a more advanced hawala, a distinct system that requires new countermeasures.

The typological analysis reveals a convergence pattern that is crucial for risk assessment and resource allocation. Neo-jihadi groups are highly advanced in fintech. There is also a perception that ethno-nationalist and sectarian groups are highly tech-savvy. From BLA's extortion proceeds via mobile wallets, LeJ's fundraising through digital channels to evade AML controls, and JuD's QR code fundraising on WhatsApp, these activities have raised hundreds of millions of rupees outside formal enforcement. This tech convergence across groups means Pakistan's counter-terrorism efforts cannot treat neo-jihadi groups as the primary threat while overlooking sectarian and nationalist financing.

Hence, Pakistan must adopt this approach to comply with FATF and eliminate threats. *FATF Recommendation 15* states that compliance with FATF standards, which Pakistan worked hard to meet, conflicts with a regulatory vacuum in virtual assets and digital platforms. Post-Grey List compliance was a significant achievement, but it should serve as a foundation for a second phase of CTF reform that is technologically adaptive.

Conflict of Interest: The author declares no conflict of interest.

Funding: This research received no external funding.

References

AAJ News. (2026, April 13). Pakistan detains 3 accused of spying for RAW. AAJ News. https://english.aaj.tv/news/330456863/pakistan-detains-3-accused-of-spying-for-raw

Ahmed. (2024, April 5). Terrorism financing. FMU. https://www.fmu.gov.pk/terrorism-financing-vbied/

Ali, K. (2017, February 7). Black money in property market risks creating a bubble. *DAWN*. https://www.dawn.com/news/1313182

Andreopoulos, M. (2026, February 5). Terrorist Financing and Pakistan's Illusion of Compliance. Geopolitics News & Risk Analysis. Retrieved April 17, 2026, from https://www.geopoliticalmonitor.com/terrorist-financing-and-pakistans-illusion-of-compliance/

Bilal, M. (2026, April 22). FIA seizes Rs. 2 billion, including Iranian currency, in major Hawala bust. ProPakistani. Retrieved April 24, 2026, from https://propakistani.pk/2026/04/22/fia-seizes-rs-2-billion-and-iranian-currency-in-major-hawala-bust/

Bindner, L., & Gluck, R. (2026, February 9). Telegram stars: Exploring Micropayment exploitation, digital goods and the evolving tactics of terrorist financing. GNET. Retrieved April 6, 2026, from https://gnet-research.org/2026/02/09/telegram-stars-exploring-micropayment-exploitation-digital-goods-and-the-evolving-tactics-of-terrorist-financing/

Bukhari, S. A. A. (2026, April 18). Personal interview.

Center for Preventive Action. (2025, February 12). *Instability in Afghanistan*. Global Conflict Tracker. Retrieved April 2, 2025, from https://www.cfr.org/global-conflict-tracker/conflict/war-afghanistan

Chainalysis Team. (2026, January 30). OFAC designates Iranian-linked crypto exchanges. Chainalysis. Retrieved April 20, 2026, from https://www.chainalysis.com/blog/ofac-designates-iranian-crypto-exchanges-january-2026/

Feyissa, D., & Gebresenbet, F. (2026). Transnational Flow of Finance in the Hadiya–South Africa Corridor. In Migration as a collective project: A temporal perspective on Hadiya migration to South Africa. Taylor & Francis. https://doi.org/10.4324/9781003617938

Financial Monitoring Unit. (2021). *Clarification–Dissemination of Financial Intelligence by Financial Monitoring Unit*. https://www.fmu.gov.pk/docs/2021/Clarification-Circular-Dissemination-of-Financial-Intelligence

Financial Action Task Force. (2025). *Status of implementation of Recommendation 15 by FATF members and jurisdictions with materially important virtual asset activity (VACG roadmap: Jurisdictions with materially important virtual asset activity)*. https://www.fatf-gafi.org/en/publications/Virtualassets/VACG-Snapshot-Jurisdictions.html

Financial Action Task Force. (2025). *Targeted update on implementation of the FATF standards on virtual assets and VASPs*. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

Global AML/CFT. (2025, April 1). *Global AML/CFT Context*. EU AML/CFT Global Facility. https://www.global-amlcft.eu/global-anti-money-laundering-and-countering-terrorism-financing-context/

Habilian. (2024). *Habilian Releases Annual Terrorism Report for 2023-2024*. https://www.habilian.ir/en/202410054968/news/habilian-releases-annual-terrorism-report-for-2023-2024.html

Institute of Economics and Peace. (2024). *Global Terrorism Index 2025*. https://www.visionofhumanity.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025

Iqbal, S. (2026, April 15). Pakistan legalises virtual assets. DAWN. https://www.dawn.com/news/1991807

Iqbal, K. (2026, April 20). *Personal interview*.

Khanum, K. A. (2026, January). *Terrorism & evolving technologies* (Policy Brief No. 15). Islamabad Policy Research Institute (IPRI). https://ipripak.org/terrorism-evolving-technologies/

Levi, M., & Reuter, P. (2006, February). Money Laundering. *Crime and Justice*, *24*(1), 289-375. http://www.jstor.org/stable/10.1086/501508

Messenger, D. A. (2026). Bombing and Civil Defense in Alicante, Cartagena, and Villena. In Civilian bombing and civil defence in the Spanish Civil War: Bombs along the Mediterranean. Springer Nature. https://doi.org/10.1007/978-3-032-10610-0_3

Mohamed, A. A. (2023). Quantifying the role of mobile money services to financial inclusion: Evidence from EVC-PLUS in Somalia. Global Social Welfare, 12(1), 29-39. https://doi.org/10.1007/s40609-023-00286-7

Movchan, A., Shliakhovskyi, O., Kozii, V., & Fedchak, I. (2023). Investigating cryptocurrency financing crimes terrorism and armed aggression. Social Legal Studios, 6(4), 123-131. https://doi.org/10.32518/sals4.2023.123

NACTA. (2024). Proscribed Organizations. https://nacta.gov.pk/wp-content/uploads/2024/10/proscribed-organizations-06-oct-2024.pdf

Pietschmann, T. (2011). *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*. UN. https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf

Reynie, D. (2024). *Islamist Terrorists Attacks in the World 1979-2024*. Fondation pour l'innovation politique. https://www.fondapol.org/en/study/islamist-terrorist-attacks-in-the-world-1979-2024/

Rousselle, A. (2025, October 24). Closing the enforcement gap: AI, illicit liquidity, and the next phase of counter-terrorist finance. GNET. Retrieved April 11, 2026, from https://gnet-research.org/2025/10/24/closing-the-enforcement-gap-ai-illicit-liquidity-and-the-next-phase-of-counter-terrorist-finance/

SATP. (2024). *Terrorism in Pakistan*. South Asia Terrorism Portal (SATP). https://www.satp.org/terrorist-groups/pakistan

Shah, S. A., & Zaidi, S. A. (2025). Navigating Fintech landscapes: A comparative analysis of Pakistan, China, and Turkey. Policy Vanguard, 1(1), 48-64. https://doi.org/10.65928/pv.1.1.2025.8

Shahid, S. (2025). BLA extorting money from mine owners, claims Balochistan minister. *DAWN*. https://www.dawn.com/news/1865284

Spyra, M., Balina, R., Idasz-Balina, M., Zając, A., & Różyński, F. (2025). Cryptocurrencies as a tool for money laundering: Risk assessment and perception of threats based on empirical research. Risks, 13(10), 189. https://doi.org/10.3390/risks13100189

State Bank of Pakistan. (2024). Annual Payment Systems Review – FY24. https://www.sbp.org.pk/PS/PDF/FiscalYear-2023-24

Global and the Local. (2020). In L. T. Waha (Ed.), United by Violence, Divided by Cause?: A Comparison of Drivers of Radicalisation and Violence in Asia and Europe. & Co. https://doi.org/10.5771/9783748905738-153

TRM. (2025, October 22). 2025 crypto crime report. https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-crime-report

Tsvetovat, M., & Carley, K. M. (2005). Generation of realistic social network datasets for testing of analysis and simulation tools. SSRN Electronic Journal, 1-27. CMU-ISRI-05-130

Tsvetovat, M., & Carley, K. M. (2005, January). Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence. *Journal of Open Source Software*, *6*(1), 1-22. https://www.cmu.edu/joss/content/articles/volume6/TsvetovatCarley/

Pervaiz, U. (2026, April, 22). *Personal interview*.

United Nations Security Council. (2001, September 28). *Adopted by the Security Council at its 4385th meeting, on 28 September 2001 (S/RES/1373)*. https://undocs.org/S/RES/1373(2001)

United Nations. (2019). *S/RES/2462(2019) | Security Council*. United Nations Security Council. https://main.un.org/securitycouncil/en/content/sres24622019

UNODC. (2026). Building skills in reporting suspicious financial activities by high-risk sectors in Pakistan. https://www.unodc.org/copak/en/Stories/SP2/building-skills-in-reporting-suspicious-financial-activities-by-high-risk-sectors-in-pakistan.html

Verma, A., Baloch, I., & Valle, R. (2025). The Baloch Insurgency in Pakistan: Evolution, Tactics, and Regional Security Implications. Combating Terrorism Center, 18(4). https://ctc.westpoint.edu/the-baloch-insurgency-in-pakistan-evolution-tactics-and-regional-security-implications/

Virk, S. (2023). National internal security policy: An assessment. Journal of Public Policy Practitioners, 1(2). https://doi.org/10.32350/jppp.12.03

Wolfberg, A. (2025). Different Kinds of Threat. In *Climate Security Intelligence: From Knowledge Transfer to Co-Creation* (p. 107–125). Springer Nature.

Zia Khan Dawar, M. B., & Afridi, M. S. (2021). Cryptocurrency and Terror Financing: Threats and Policy Options for Pakistan. PJTR, 4(1), 80-105. https://pjtr.nacta.gov.pk/index.php/Journals/article/view/73