

Emirati Journal of Business, Economics and Social Studies
Vol 5 Issue 2 (2026)
Pages 123 - 138
Available at
www.emiratesscholar.com

UAE FININT Resilience using a Network-Based Framework for Countering Terrorist Financing: From AML Compliance to Financial-Hub Resilience, An Attempt to Design an Integrated Counter-Terrorist-Financing Architecture for the United Arab Emirates

Vipul V. Tamhane
Financial Regulatory Consultant, FinGigPro FZ LLC, India

ARTICLE INFO

KEYWORDS
terrorist financing; financial-hub resilience; United Arab Emirates; AML/CFT; financial intelligence; network risk; public-private partnership; typology-led detection

HOW TO CITE
Tamhane, V. V. (2026). UAE FININT Resilience using a Network-Based Framework for Countering Terrorist Financing: From AML Compliance to Financial-Hub Resilience, An Attempt to Design an Integrated Counter-Terrorist-Financing Architecture for the United Arab Emirates. Emirati Journal of Business, Economics and Social Studies, 5(2), 123-138.
https://doi.org/10.54878/mxegpk56

ABSTRACT

The United Arab Emirates (UAE) occupies a distinctive position in the international financial system: its success as a global banking, trade, logistics and virtual-asset hub simultaneously generates economic value and creates a complex exposure surface for transnational terrorist financing. This article argues that institution-level anti-money-laundering and counter-terrorist-financing (AML/CFT) compliance remains necessary but analytically and operationally incomplete for a high-connectivity jurisdiction, and proposes a shift from a compliance-centred architecture to a Financial Hub Resilience Model (FHRM). The study adopts a doctrinal and conceptual research design, combining doctrinal legal analysis of primary instruments (Federal Decree-Law No. 10 of 2025 and Cabinet Resolution No. 134 of 2025), comparative institutional analysis of the United Kingdom, Singapore and United States frameworks, and conceptual synthesis of the regulatory-compliance, network-analytic and geopolitical literatures. The FHRM relocates the unit of defence from the individual regulated entity to the interconnected ecosystem. It rests on two original constructs: the Financial Hub Attack Surface (seven-layer interfaces across banking, informal value transfer, corporate structures, trade, real estate, digital finance and the non-profit sector); and Financial Convergence Risk (individually explicable transactions that form, across institutions, a coherent terrorist-financing pathway invisible to single-institution monitoring). The model yields an operational architecture centred on intelligence fusion, typology-led detection, a bidirectional public-private partnership, and two outcome metrics (Time-to-Disruption and Financial Network Containment). Its central claim is that the UAE's financial connectivity can be converted from a residual vulnerability into a sustained comparative advantage in financial integrity and national security, provided the ecosystem, rather than the firm, becomes the object of defence.

Double-blind peer review by independent reviewers.
Received: 13 Jul 2026, Accepted: 19 Oct 2026, Published: 02 Nov 2026
*Corresponding author: vipul.tamhane@gmail.com
Copyright: © 2026 by the author. Licensee Emirates Scholar Center for Research & Studies, UAE.
Open access under the Creative Commons Attribution (CC BY) license
https://creativecommons.org/licenses/by/4.0

1. Introduction

Global financial centres create prosperity through connectivity, and the same connectivity opens pathways that sophisticated illicit actors can exploit. The United Arab Emirates exemplifies this tension with unusual clarity. In little more than two decades the country has established itself as the pre-eminent financial and commercial hub between Frankfurt and Singapore, a jurisdiction that intermediates a vast share of the payments, trade, remittances, corporate formations, investment flows and, increasingly, virtual-asset activity that move between South Asia, the Gulf, East Africa and Europe. Openness, interconnectedness, regulatory efficiency and a dense business ecosystem are precisely the attributes that attract legitimate capital. They are also the attributes that render the jurisdiction attractive as a transit, conversion, layering and redistribution environment for terrorist and other illicit finance.

The FATF-MENAFATF Mutual Evaluation Report of 2020 (Financial Action Task Force [FATF] & MENAFATF, 2020) identified this paradox in the language of risk. It located the UAE's exposure not in any single institutional failing but in its very status as a global financial centre and trading hub: its geographical position astride major corridors, the scale and diversity of its financial, corporate and trade activity, and the jurisdictional complexity generated by its federal structure, its financial free zones and its multiplicity of supervisors. The subsequent grey-listing on 4 March 2022 confirmed that this structural exposure had translated into demonstrable effectiveness gaps, and the country's removal from the list on 23 February 2024 confirmed that it could close those gaps at speed.

The reforms undertaken between 2022 and 2024 were substantial and are not in dispute here. The UAE established a dedicated Executive Office to combat money laundering and terrorist financing, created specialised courts and prosecutorial capacity, strengthened its Financial Intelligence Unit, and adopted a National Strategy for AML/CFT and counter-proliferation financing for the period 2024-2027. It then went further, replacing its foundational statute altogether: Federal Decree-Law No. 10 of 2025, gazetted on 30 September 2025 and in force from 14 October 2025, repealed Federal Decree-Law No. 20 of 2018 in its entirety, established proliferation financing as a distinct offence, brought virtual assets and encrypted value-transfer channels squarely within its reach, and introduced personal liability for senior management alongside corporate penalties of up to AED 100 million.

These developments demonstrate institutional seriousness of a high order. They do not, however, resolve a deeper structural question, and it is that question this article addresses:

How can a successful global financial hub prevent the very connectivity that constitutes its economic advantage from becoming an infrastructure advantage for terrorist financing?

The article's central argument is that the dominant paradigm of AML/CFT, an institution-centred model in which each regulated entity independently conducts customer due diligence, monitors its own transactions and files suspicious-transaction reports (STRs), is necessary but structurally incomplete for a jurisdiction whose comparative advantage lies in high connectivity across many financial sectors and jurisdictions. The model rests on an implicit assumption: that the critical vulnerability resides inside individual institutions, and that adequate compliance at the entity level aggregates into systemic security. For a high-connectivity hub that assumption is false. A terrorist financier rarely needs to "penetrate" any single bank; it is sufficient to route value across the interfaces between a trading company, a bank, an exchange house, a hawala provider, a virtual-asset service provider (VASP) and a foreign jurisdiction, so that no single institution ever sees a transaction that is, on its own, sufficiently anomalous to report.

This article therefore proposes a shift in the unit of analysis, and in the unit of defence, from the individual institution to the financial hub itself. It develops this shift into a Financial Hub Resilience Model (FHRM) and two supporting constructs. The Financial Hub Attack Surface maps the seven interacting layers of the UAE's financial ecosystem through which value can be moved in combination. Financial Convergence Risk names the specific danger that arises when individually explicable transactions, viewed across institutions, cohere into a terrorist-financing pathway. From these constructs the article derives an operational architecture, intelligence fusion, typology-led detection, a bidirectional public-private partnership, and two outcome metrics, Time-to-Disruption and the Financial Network Containment ratio, intended not as a critique of the UAE's reforms but as the next evolutionary layer built upon them.

The remainder of the article is organised as follows. Section 2 reviews the three dominant approaches to terrorist financing, regulatory-compliance, network-analytic and geopolitical, and derives the systemic-integrationist gap the article fills. Section 3 sets out the method and research design. Section 4 presents the

ISSN: 2791-3171 - https://doi.org/10.54878/mxegpk56

results and discussion: it develops the FHRM and its constituent constructs, applies the framework to the UAE's "shadow finance ecology," surveys the reformed legal and institutional foundation, sets out the policy architecture in seven recommendations, and discusses the strategic opportunity together with comparative lessons, the amplifying role of artificial intelligence, and the study's limitations. Section 5 concludes.

2. Literature Review

Scholarship on terrorist financing, and on the AML/CFT regimes constructed to counter it, clusters around three broad approaches. Each illuminates part of the problem; none, taken alone, is adequate to the distinctive risk profile of a globally connected financial centre. Read together, they point toward a fourth, integrationist approach that this article develops.

2.1 The Regulatory-Compliance Approach

The first and most voluminous body of work analyses the alignment of national legislation and supervision with the FATF Recommendations, treating compliance as the principal dependent variable (Ryder, 2015). This literature has documented both the remarkable global diffusion of a standardised AML/CFT template and its uneven translation into practice. Sharman (2011) shows how a soft-law regime propagated through blacklisting and reputational pressure rather than binding treaty, producing widespread formal adoption whose substantive effect is frequently uncertain; Nance (2018) traces the maturation of the FATF regime and its shifting theory of influence; and a sharply critical strand, associated with Pol (2020) and with Halliday, Levi and Reuter (2014), argues that the regime's measured impact on criminal finances is strikingly small relative to its compliance cost.

The crucial development for present purposes is FATF's own migration, from its fourth round of mutual evaluations onward, toward the assessment of effectiveness rather than mere technical compliance (FATF, 2023), the eleven Immediate Outcomes that ask not whether a country has the right laws but whether its system actually detects, disrupts and deprives. This is a decisive move, and it is the move on which the present article builds: a jurisdiction can be fully technically compliant and still be strategically exposed, because effectiveness is a property of the system as a whole, not of the sum of its institutions' compliance. Yet the compliance literature, precisely because it takes the regulated institution and the national statute book as its units, rarely theorises the ecosystem-level dynamics on which effectiveness ultimately depends.

2.2 The Network-Analysis Approach

A second approach maps terrorist and criminal financial flows as networks, tracing value through informal value-transfer systems, trade and corporate vehicles. The study of hawala and other informal value-transfer systems is foundational: Passas (2006) established both their legitimate economic function and the conditions under which they are exploited, and cautioned that heavy-handed or purely prohibitionist regulation can be counter-productive, displacing value into still less visible channels (see also FATF, 2013).

Trade-based money laundering (TBML) has generated a parallel literature on mis-invoicing, phantom shipments and multiple invoicing, demonstrating how value moves through the ordinary documentary apparatus of commerce in volumes that dwarf the capacity of any monitoring system to inspect transaction by transaction (FATF, 2021; Teichmann, 2019). Recent empirical work sharpens the picture: a study of 121 documented terrorist-financing cases (Jofre et al., 2024) finds that traditional channels still dominate overwhelmingly, the banking system, foreign shell companies, money transfers, hawala and high-value commodities such as gold, with emerging financial technologies present in only a small minority of cases. This is powerful confirmation that the corporate, trade and informal layers, not the digital frontier alone, are where defensive attention is most needed.

A fast-moving literature nonetheless examines virtual assets and terrorist financing. Studies by RAND (Dion-Schwarz et al., 2019) and by blockchain-analytics researchers (Fanusie & Robinson, 2018) find that, while cryptocurrency has not displaced conventional channels, it offers specific affordances, pseudonymity, speed, cross-border reach and, through mixers and privacy coins, deliberate obfuscation, that reward targeted regulatory attention (FATF, 2019). The UAE's own Financial Intelligence Unit has reported more than 4,000 virtual-asset-related suspicious reports by mid-2025 and detailed analysis of several hundred over a two-year window (UAE Financial Intelligence Unit, 2025b), evidence both of the scale of activity and of the intelligence value latent within it.

What the network literature contributes is the insight that terrorist finance is relational: it lives in the connections between actors, entities and channels, not in any single node. What it has been slower to translate into institutional design is the corollary, that a defensive architecture organised around single nodes will systematically under-detect a threat organised around edges.

2.3 The Geopolitical Approach

A third approach situates terrorist financing within the political economy of conflict and state sponsorship, distinguishing the financial logic of asset-holding sanctioned wealth from the operationally distinct logic of a state proxy that actively moves money to fund clients and operations. Levitt's (2013) work on Hezbollah's global financial footprint, the broader literature on the Islamic Revolutionary Guard Corps (IRGC) as a financial-operational actor (Biersteker & Eckert, 2008), and typological scholarship on the sources and methods of terrorist financing (Freeman, 2011; Zabyelina, 2022) together describe a threat that is ideologically motivated, commercially camouflaged and embedded in regional geopolitics.

This vantage point yields an important analytical caution for any Gulf jurisdiction: the dominant international preoccupation with one form of sanctions evasion can crowd out attention to a functionally different threat, proxy financing that uses front companies, exchange houses and trading entities not to store value but to move it to armed clients. The geopolitical literature, however, tends to operate at the level of strategy and statecraft, and rarely descends to the regulatory-institutional question of how a financial hub should be organised, day to day, to detect such flows within lawful commerce.

2.4 The Gap: A Systemic-Integrationist Approach

Each approach captures something the others miss. The compliance approach understands law and supervision but under-theorises the ecosystem; the network approach understands relational flow but under-specifies institutional design; the geopolitical approach understands strategic intent but abstracts from operational regulation. What is missing is an integrationist approach that unites all three at the level of the financial hub: one that treats the hub's connectivity as the object of both risk and defence, models the threat as a network spanning sectors and jurisdictions, and translates strategic intent into an operational architecture of intelligence and disruption.

The gap is especially pronounced for the UAE, which is not analytically interchangeable with the centres to which it is routinely compared. Unlike Switzerland, Singapore or Luxembourg, its risk profile is shaped by physical proximity to conflict zones, by an economy structurally dependent on expatriate labour and on trade and remittance corridors, and by a rapid and deliberate embrace of fintech and virtual assets. A framework built for a low-connectivity, low-proximity centre will not fit.

2.5 Theoretical Integration: From Three Approaches to One Framework

The Financial Hub Resilience Model integrates the three traditions rather than choosing among them. From regulatory-compliance theory it takes the focus on law, supervision and enforcement, but relocates the unit of analysis from the institution to the ecosystem and substitutes operational effectiveness for technical compliance as the primary criterion. From network analysis it takes the insight that terrorist finance is relational and translates it into a defensive architecture that targets edges rather than nodes; Financial Convergence Risk is the operationalisation of that insight. From geopolitical analysis it takes the understanding that the threat is ideologically driven and commercially camouflaged, and situates the UAE's exposure within the political economy of its region rather than treating it as generic. The synthesis is the contribution: connectivity becomes the object of both risk and defence (Raab & Milward, 2003; Amicelle, 2011; de Goede, 2012).

3. Research Methodology

3.1 Research Design

This article is a conceptual and comparative legal-institutional study; it does not involve primary data collection, human participants or animal subjects, and every source it relies upon is publicly available and cited in the references. Its method is qualitative and interpretive, and combines four complementary strands. The design follows the tradition of analytical eclecticism, which combines partial perspectives from distinct theoretical traditions to address a problem that none explains fully on its own, and it is transparent and replicable in the sense proper to doctrinal and conceptual legal research rather than to statistical inference (Levi et al., 2018).

3.2 Method and Sources

First, doctrinal legal analysis. The article interprets the UAE's AML/CFT framework, principally Federal Decree-Law No. 10 of 2025, its Executive Regulations in Cabinet Resolution No. 134 of 2025, the Central Bank of the UAE (CBUAE) Rulebook and associated guidance, and the analytical output of the UAE Financial Intelligence Unit, to establish what the law actually does to the location of counter-terrorist-financing responsibility, and where the legal basis for network-level intelligence and coordination is strong, weak or absent. The doctrinal method is appropriate because the regime

is legally constructed and the gaps at issue are legal-institutional in character.

Second, comparative institutional analysis. The UAE architecture is benchmarked against three comparator jurisdictions whose public-private financial-intelligence models are the most developed: the United Kingdom's Joint Money Laundering Intelligence Taskforce, Singapore's AML/CFT Industry Partnership, and the United States' information-sharing provisions under sections 314(a) and 314(b) of the USA PATRIOT Act. The selection is purposive rather than representative: these cases instantiate contrasting institutional solutions to the shared problem of cross-institutional detection, and therefore offer the most analytically productive comparison for the argument.

Third, conceptual synthesis. The article draws together the regulatory-compliance, network-analytic and geopolitical literatures on terrorist financing and constructs from them the Financial Hub Resilience Model, iterating between the theoretical traditions and the empirical evidence on UAE vulnerabilities and comparative practice.

Fourth, theoretical-framework construction. The article develops and operationalises three original constructs, the Financial Hub Attack Surface, Financial Convergence Risk and the Financial Intelligence Learning Loop, and converts them into usable policy instruments, a diagnostic (presented in the Appendix) and two outcome metrics, following the conventions of concept formation in comparative institutional analysis: from observation to abstraction to operationalisation.

4. Results and Discussion

4.1 The Financial Hub Resilience Model

The Financial Hub Resilience Model (FHRM) reconceptualises the unit of counter-terrorist-financing defence. Where the conventional model runs linearly, regulator to institution to customer or transaction to STR to Financial Intelligence Unit to law enforcement, and assumes that entity-level compliance aggregates into systemic security, the FHRM treats the financial hub, understood as an interconnected ecosystem, as the primary unit of analysis, and defines resilience as the capacity of that ecosystem to convert distributed financial signals into timely, coordinated network disruption.

The Financial Hub Paradox proposition

The model's foundational proposition can be stated formally:

Proposition 1 (Financial Hub Paradox). The greater a jurisdiction's international financial connectivity, the greater both its economic value and its potential exposure to transnational terrorist-financing networks; therefore financial-hub security cannot be achieved through the reduction of connectivity, which would forfeit the economic value, but only through the maximisation of resilience.

The proposition reframes connectivity as a double-edged variable rather than an unqualified good or a simple liability. The appropriate response is not to reduce connectivity but to build a defensive architecture whose reach matches the reach of the exposure it must address. From it the model derives a second, operational proposition developed across Sections 4.4 and 4.5:

Proposition 2 (Financial Hub Resilience). A financial hub's resilience to terrorist financing is determined less by the compliance strength of individual institutions than by the speed and completeness with which regulatory, financial-intelligence, law-enforcement and private-sector actors can transform distributed financial signals into coordinated network disruption.

The Financial Hub Attack Surface

Adapting a concept from information security, the article defines the Financial Hub Attack Surface as the total set of interfaces across the financial ecosystem that can be exploited, singly or in combination, to move terrorist value. In the UAE this surface comprises seven interacting layers (Table 1). The analytical purpose of the construct is to shift attention from the security of any one layer to the exploitability of the interfaces between them.

Layer	Domain	Primary exposure channels
1	Banking	Correspondent banking, private banking, corporate banking, trade finance, remittances, payment systems
2	Informal finance	Registered hawala and money/value-transfer providers, exchange houses, cash-intensive businesses

ISSN: 2791-3171 - https://doi.org/10.54878/mxegpk56

3	Corporate structures	Free-zone entities, shell and front companies, nominee arrangements, opaque beneficial ownership, layered ownership chains
4	Trade	Gold and precious metals, precious stones, commodities, shipping and transshipment, TBML via mis-invoicing
5	Real estate	High-value transactions, corporate ownership of property, intermediaries and cash purchases
6	Digital finance	VASPs, stablecoins, OTC desks, mixers and privacy-enhancing protocols, cross-chain transfers
7	NPO / charitable sector	Cross-border charitable flows; distinction between legitimate humanitarian finance and its exploitation

Table 1. The seven-layer Financial Hub Attack Surface of the UAE.

Two features of the surface deserve emphasis. First, its layers are supervised, but by different authorities and under different logics: the CBUAE oversees banks, exchange houses, payment providers, finance companies and registered hawala providers (Central Bank of the United Arab Emirates [CBUAE], 2024-2026); the financial free zones, the Dubai International Financial Centre and the Abu Dhabi Global Market, operate their own regulators; and the Securities and Commodities Authority and the Ministry of Economy hold further mandates over markets and designated non-financial businesses and professions (DNFBPs). Supervisory pluralism is a strength for market development but a seam for illicit exploitation. Second, the seventh layer, the non-profit sector, requires particular care: the objective of any resilience architecture must be to detect exploitation without indiscriminate de-risking of legitimate humanitarian finance, which itself carries strategic and human costs (de Koker, 2006).

Financial Convergence Risk

The second original construct, Financial Convergence Risk (FCR), captures the danger that arises at the interfaces catalogued above. FCR is the risk that a terrorist-financing pathway is assembled across multiple regulated and semi-regulated nodes, each of which, examined in isolation, appears legitimate, but which together form a coherent movement of value from source to facilitator (Raab & Milward, 2003; Levi & Reuter, 2006).

A stylised pathway illustrates the point:

Foreign source -> UAE free-zone company -> mis-invoiced trade transaction -> bank -> exchange house -> hawala -> third jurisdiction -> terrorist facilitator

At each node the transaction may be individually explicable. The trading company has a licence and a plausible commercial purpose; the bank sees a trade payment supported by documentation; the exchange house processes a remittance consistent with the customer's profile; the hawala provider settles an ordinary transfer. The suspicious pattern exists only in the aggregate, in the sequence and coincidence of counterparties, jurisdictions and timing, and the aggregate is precisely what no single institution can see. Conventional transaction-monitoring systems, optimised on single-institution data and tuned to flag anomalies within one book, are structurally blind to FCR. Because the probability that a distributed pathway is detected by isolated single-institution monitoring falls as the number of nodes rises, while a network-level view can flag the pathway from any one of its nodes, detecting FCR requires network-level visibility and intelligence that spans the interfaces, the design problem the rest of the article addresses.

The Financial Intelligence Learning Loop

If FCR is the problem, adaptive intelligence is the mechanism of response. The FHRM operationalises this through a Financial Intelligence Learning Loop, a continuous cycle that converts investigation into detection capacity and back again (Figure 1):

ISSN: 2791-3171 - https://doi.org/10.54878/mxegpk56

Threat -> detection / STRs -> FIU analysis -> typology generation -> regulatory dissemination -> institutional detection rules -> new STRs -> law-enforcement action -> updated intelligence -> new typology

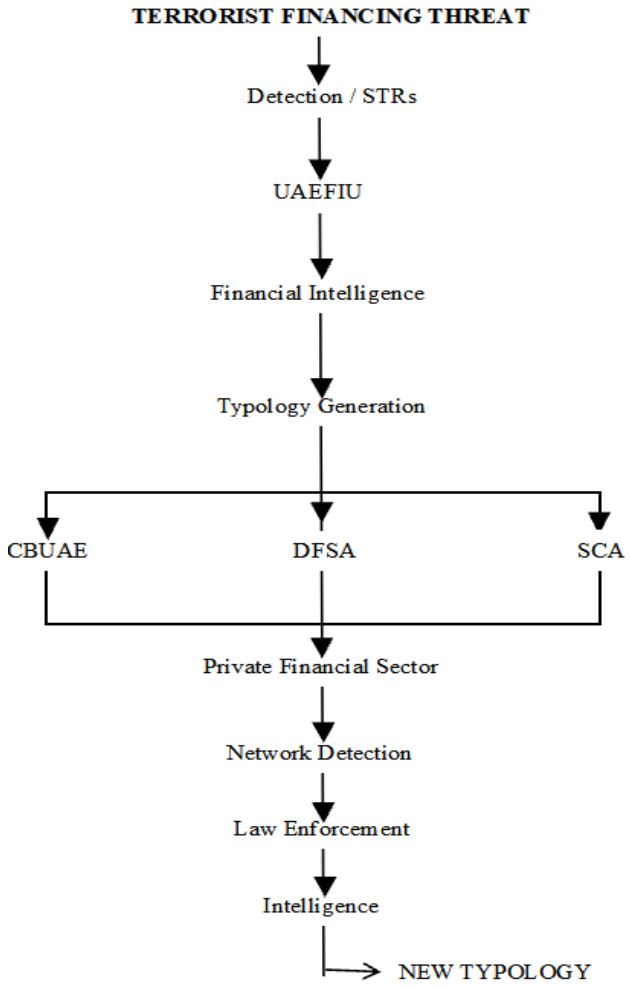


Figure 1. The Financial Intelligence Learning Loop.

The loop reframes the private financial sector not as a population of reporting entities discharging a compliance obligation but as a distributed sensor network whose observations, once fused and analysed, generate typological intelligence that is fed back to sharpen detection. Banks, exchange houses, hawala providers, VASPs, DNFBPs and trade-finance institutions become the sensors; the Financial Intelligence Unit becomes the fusion centre; law enforcement becomes the disruption mechanism. A system so organised learns: each disrupted network yields typologies that improve the detection of the next, so that the ecosystem's defensive capability compounds over time rather than resetting with each isolated case.

4.2 The Shadow Finance Ecology

The FHRM is not an abstraction; it maps onto an identifiable threat ecology in the UAE. This subsection applies the framework to four layers of that ecology, infrastructural, corporate, digital and geopolitical, drawing on the country's own regulatory guidance, its Financial Intelligence Unit's analytical output, and the public record of enforcement.

The infrastructural layer: the conduit economy

The UAE's economy is built on being a conduit for goods, people and capital, and that infrastructure is simultaneously its strength and its principal exposure. TBML is the paradigmatic infrastructural risk: the sheer volume of trade moving through ports such as Jebel Ali makes transaction-by-transaction inspection impracticable, and mis-invoicing and the over- or under-shipment of goods allow value to move within the ordinary documentary flow of commerce. Supervisory guidance on trade-based money laundering and transshipment reflects an accurate reading of this risk, but guidance alone cannot resolve a detection problem that is fundamentally one of scale and of cross-institutional visibility (FATF, 2021; CBUAE, 2024-2026).

The informal and cash-intensive channels present a parallel exposure. Hawala and other money/value-transfer providers are regulated and registered in the UAE, and exchange houses are supervised by the CBUAE; yet regulation does not by itself guarantee visibility. Reported enforcement in 2025, penalties exceeding AED 380 million across 31 financial institutions in the first eight months of the year, including a single fine of AED 200 million against an exchange house, evidences both the persistence of monitoring weaknesses in these channels and the vigour of the supervisory response. Aggregate enforcement of this magnitude is a textbook demonstration of post-delisting credibility; the deterrence literature nonetheless cautions that sanction deters mainly through the probability of detection rather than the severity of penalty (Nagin, 2013; Chaikin, 2009), which returns the argument to detection capacity.

The corporate layer: the commercial-cover nexus

The corporate layer is, on the available evidence, the centre of gravity of the threat. Analytical reporting by the

UAE Financial Intelligence Unit identifies the abuse of corporate structures as the most frequently observed pattern in terrorist-financing cases (UAE Financial Intelligence Unit, 2025a), complex legal arrangements used to move and obscure funds, corporate nominees deployed to conceal true ownership (including by sanctioned persons), and suspicious flows directed toward the real-estate sector, and the finding is corroborated by cross-national empirical work identifying foreign shell companies as a dominant financing method (Findley et al., 2014; Jofre et al., 2024). The operational model revealed in the dismantling of proxy-linked networks is one of commercial cover: financiers establish ostensibly legitimate businesses, trading companies, brokerages, gold and commodity dealerships, that function as laundering and financing vehicles while presenting an unremarkable commercial face.

This finding is decisive for the FHRM. If the dominant typology is the exploitation of licensed corporate vehicles operating across banking, trade and real estate, then the vulnerability is not located inside any one institution but at the interfaces between the company, its banks, its trading counterparties and the property market, exactly the Financial Convergence Risk the model isolates. Beneficial-ownership transparency is therefore not one compliance requirement among many; it is the keystone of network-level visibility.

The digital layer: the crypto conundrum

The UAE's deliberate cultivation of a virtual-asset industry has attracted global talent and created a new frontier of exposure. Federal Decree-Law No. 10 of 2025 brings funds in digital and encrypted form, and conduct executed through virtual-asset channels, expressly within the definition of the relevant offences, and its imposition of personal liability on senior management is a powerful governance lever. The enforcement challenge, however, is technical as much as legal: privacy-enhancing protocols, mixers and cross-chain movement present a moving target that demands sophisticated analytics capacity. The proportionality point matters for resource allocation: the best current evidence places virtual assets in a small minority of terrorist-financing cases (Jofre et al., 2024), so the digital layer warrants vigilance and capability without displacing attention from the corporate, trade and informal layers where most value still moves.

The geopolitical layer: proxy finance under commercial cover

The UAE's position in a volatile region gives the threat a distinct geopolitical texture. The analytically important distinction, developed in the literature and borne out in the enforcement record, is between the passive holding of sanctioned wealth and the active movement of funds by state proxies to armed clients (Levitt, 2013; Biersteker & Eckert, 2008). Networks linked to the IRGC and to organisations such as Hezbollah do not merely park value; they move it, using front companies, exchange houses and trading entities as nodes in sanctions-evasion and financing pathways. The reported dismantling of such networks demonstrates capability, but by its nature describes a reactive success: authorities disrupted a pathway that had already become operational. A pre-emptive posture would read the financial indicators, clusters of accounts linked to sensitive jurisdictions, anomalous trade patterns, characteristic corporate footprints, to anticipate and interdict such networks before they mature.

4.3 The Current UAE Regulatory and Institutional Foundation

The recommendations advanced in Section 4.4 are deliberately framed as the next layer upon an already substantial foundation, not as a remedy for its absence. This subsection surveys that foundation across legislation, institutions, enforcement, strategy and public-private cooperation.

Legislative framework

The core statute is now Federal Decree-Law No. 10 of 2025, supported by its Executive Regulations in Cabinet Resolution No. 134 of 2025; the framework had already been amended once, by Federal Decree-Law No. 7 of 2024, before this consolidating statute. Beyond repealing and replacing the 2018 law, the new framework broadens the definition of "funds" to encompass digital and encrypted assets, captures money laundering executed through virtual-asset channels, establishes proliferation financing as a standalone offence, and, of particular strategic significance, enables UAE courts to recognise and enforce foreign provisional measures and confiscation orders without requiring a parallel domestic investigation. That provision repositions the jurisdiction from a potential safe haven to an active partner in global asset recovery, a reputational and operational asset the resilience architecture can build upon.

Institutional architecture

The institutional map is correspondingly dense. The Financial Intelligence Unit has been strengthened in independence and investigative capacity (UAE Financial Intelligence Unit, 2024); the CBUAE supervises the

banking, exchange, payments and hawala sectors and administers an assertive enforcement function; the DIFC and ADGM regulators, the Securities and Commodities Authority and the Ministry of Economy hold further supervisory mandates; and the Executive Office for Control and Non-Proliferation coordinates targeted financial sanctions (see United Nations Security Council, 1999, 2001). This is a capable architecture. Its principal limitation, from the standpoint of the FHRM, is horizontal: the seams between financial-intelligence, supervisory and national-security functions are where Financial Convergence Risk concentrates, and it is the integration across those seams, rather than the strength of any one institution, that the model seeks to improve (Government of the United Arab Emirates, 2024; CBUAE, 2024-2026).

Enforcement posture

The enforcement record since delisting reflects a conscious strategy of visible deterrence: substantial fines across dozens of institutions, senior-manager liability modelled on the accountability regimes of comparator jurisdictions, and licence actions against serious failures, on the logic that credible, frequent sanction of lesser violations signals that grave ones will meet severe consequences. The academic literature enters an important caveat, already noted: deterrence is a product of the probability of detection at least as much as of the severity of punishment, and even suspicious-transaction-reporting systems convert into enforcement outcomes only where analytical and investigative capacity is present to act on them. Fines therefore deter only to the extent that detection is likely, which returns the argument to the detection capacity that network-level intelligence is designed to raise.

Strategic planning and public-private cooperation

The National Strategy for 2024-2027 (Government of the United Arab Emirates, 2024) is explicitly oriented toward emerging and complex risks, TBML, third-party and legal-structure risk, and new technologies, and toward deeper national and international information sharing. The UAE has also constructed public-private machinery, including a standing partnership committee bringing together government bodies and private-sector entities and a dedicated sub-committee on countering money laundering and terrorist financing. The architecture for cooperation therefore exists. The question the next subsection addresses is whether it operates as a genuinely operational, bidirectional intelligence mechanism or remains, in practice, a largely consultative and one-directional reporting relationship (Maxwell & Artingstall, 2017; Keatinge et al., 2018).

4.4 A Financial Intelligence Fusion Architecture: Seven Recommendations

The FHRM yields a concrete institutional programme, presented here as seven connected recommendations. Together they constitute a Financial Intelligence Fusion Architecture that operationalises the Financial Intelligence Learning Loop and targets Financial Convergence Risk directly. The recommendations are designed to build upon, not duplicate, the existing framework surveyed in Section 4.3, and to be sequenced from low-cost guidance measures toward higher-investment infrastructure.

Recommendation A: Network-level risk assessment

High-risk institutions should be required to assess risk not at the level of the isolated customer or transaction but across the network in which each sits. The article proposes a Network Financial Risk Score (NFRS) whose components extend the conventional risk model to include the relational and cross-channel dimensions that FCR exploits: customer, counterparty, beneficial-ownership, transaction, jurisdictional, intermediary, payment-channel, trade, digital-asset and typology exposure. The NFRS reframes risk from a property of an account to a property of a position within the ecosystem, and gives supervisors a common vocabulary for network-level expectations.

Recommendation B: Cross-sector transaction intelligence

The defining limitation of the present architecture is informational siloing: a bank sees only its own book, a VASP its own flows, an exchange house its own remittances, a DNFBP its own client, while the terrorist-financing network exists across all of them. The recommendation is not unrestricted data pooling, which would be neither lawful nor desirable, but a legally authorised, privacy-preserving intelligence-matching capability, federated analytics and secure multi-party computation operating on a need-to-know basis, through which a national matching layer can identify that a transaction at a bank, a transfer at an exchange house, a corporate structure in a free zone and an on-chain movement belong to a single pathway, without the participants exposing underlying customer data to one another.

Recommendation C: Typology-led intelligence

ISSN: 2791-3171 - https://doi.org/10.54878/mxegpk56

Generic AML rules should be progressively supplemented by intelligence-derived typologies generated from actual investigations and disseminated, in sanitised form, to the private sector. Illustrative typologies, a South Asia-Gulf-East Africa informal-value-transfer corridor; a corporate-entity-plus-trade-mispricing-plus-cash-withdrawal sequence; a crypto-to-hawala conversion pathway, allow institutions to tune their monitoring to live threats rather than to static, generic red flags. This is the engine of the Financial Intelligence Learning Loop: each investigation yields a typology, each typology sharpens detection, and each new detection feeds the next investigation.

Recommendation D: An operational public-private partnership

The existing partnership machinery should be transformed from a consultative body into an operational financial-intelligence partnership defined by bidirectional flow. In the prevailing model the flow is largely one-way: the state sets rules and the private sector reports. In an operational model the public sector shares typological and network intelligence, "we are observing this corridor, these indicators, this corporate footprint", enabling compliance functions to adjust monitoring proactively, while the private sector supplies typology indicators, network indicators, emerging-channel intelligence and cross-border anomalies in return. The private financial sector, so engaged, functions as the distributed sensor network of the resilience model.

Recommendation E: Red-team resilience exercises

To test the system under a dynamic threat, the article proposes annual, scenario-based red-team exercises that simulate a terrorist-financing network across the attack surface, for example, a pathway running from a foreign source through a UAE corporate vehicle, a mis-invoiced trade transaction, an exchange house, a virtual-asset conversion and out to a third jurisdiction. The exercise measures, at each stage, whether the relevant institution detects the activity, whether the Financial Intelligence Unit connects the reports, whether law enforcement receives actionable intelligence, how quickly assets are frozen, and whether international cooperation functions. The output is a Financial Hub TF Resilience Score, which operationalises the CBUAE's stated emphasis on continuous monitoring and outcomes-focused supervision into a measurable, repeatable assessment.

Recommendation F: Outcome metrics, Time-to-Disruption and Financial Network Containment

Conventional AML metrics count inputs and outputs, STRs filed, inspections conducted, fines imposed. For counter-terrorist financing, what matters is effectiveness, and the article proposes two outcome metrics to capture it. Time-to-Disruption (TTD) measures the elapsed time from the first suspicious financial event to the disruption of the network, decomposed into identification, FIU dissemination, investigation, asset freezing and operational impact; it turns speed itself into a governed performance variable. The Financial Network Containment (FNC) ratio measures, for an identified network, the proportion of its financial nodes that authorities identify and disrupt, if a network comprises one hundred nodes and fifty-five are disrupted, containment is fifty-five per cent. Both require careful operationalisation and honest treatment of their limits, but both shift assessment from the volume of compliance activity to the completeness and speed of network disruption.

Recommendation G: A National Financial Threat Intelligence Grid

The six preceding recommendations cohere in a single conceptual architecture: a National Financial Threat Intelligence Grid (NFTIG). The NFTIG is not a new bureaucracy or a new regulator; it is a fusion architecture that links the Financial Intelligence Unit, the CBUAE, the free-zone regulators and the Securities and Commodities

4.5 Discussion

Turning connectivity into strategic advantage

The FHRM contains a strategic inversion worth making explicit. The very connectivity that constitutes the UAE's exposure also constitutes an unrivalled intelligence asset. Few jurisdictions observe so large and so varied a volume of international payments, trade, remittances, corporate formations, investment and virtual-asset activity. Under a compliance paradigm this volume is a burden to be monitored; under a resilience paradigm it is a sensing capability to be exploited. A hub that fuses its distributed financial signals into network-level intelligence could develop one of the world's most sophisticated financial-threat-detection systems, and in doing so convert a defensive obligation into a source of regional leadership and comparative advantage in financial integrity.

Comparative insights: three models of financial-intelligence partnership

The proposed architecture is not without precedent, and the UAE has already signalled awareness of the relevant models. Table 2 benchmarks the UAE's current position against three comparators. The United Kingdom's Joint Money Laundering Intelligence Taskforce pioneered operational public-private information sharing between law enforcement and major banks; Singapore's AML/CFT Industry Partnership institutionalised a comparable collaboration under its central bank; and the United States' Bank Secrecy Act of 1970, together with the information-sharing provisions under sections 314(a) and 314(b) of the USA PATRIOT Act, created statutory

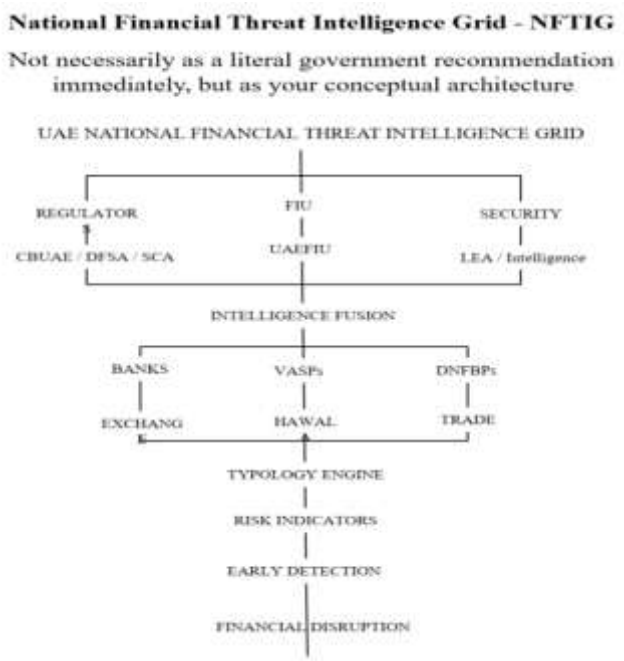


Figure 2. The National Financial Threat Intelligence Grid (NFTIG)

channels for government-to-industry and industry-to-industry sharing under a safe harbour. Each offers transferable lessons, on governance, on the legal basis for sharing, and on managing data-protection constraints, while none maps perfectly onto the UAE's distinctive supervisory pluralism and geopolitical setting (Maxwell & Artingstall, 2017).

Dimension	**UK (JMLIT)**	**Singapore (ACIP)**	**US (§314 / FinCEN)**	**UAE (proposed FHRM)**
Legislative basis	Proceeds of Crime Act 2002; Criminal Finances Act 2017	MAS Act; AML/CFT regulations	USA PATRIOT Act §314(a)/(b)	Federal Decree-Law No. 10 of 2025
FIU model	UKFIU within the National Crime Agency	STRO, Commercial Affairs Department	FinCEN, US Treasury	UAEFIU (statutorily strengthened)
Partnership	JMLIT (law enforcement + major banks)	ACIP (regulator + industry)	§314(b) industry-to-industry sharing	Proposed Operational PPP / NFTIG
Information flow	Bidirectional	Bidirectional	Statutory channels, both directions	Currently largely one-way; bidirectional proposed
Legal protection for sharing	Established	Established	Safe harbour under §314(b)	Emerging; strengthening proposed
Virtual-asset coverage	Developing	Explicit	Evolving	Explicit (2025 law)
Typology dissemination / red-teaming	Yes / limited	Yes / yes	Advisories / limited	Proposed / proposed

Table 2. Comparative financial-intelligence partnership models and the proposed UAE position.

Artificial intelligence as an amplifier of Financial Convergence Risk

Artificial intelligence does not merely add another compliance domain; it changes the character of the detection problem in two directions at once. On the

ISSN: 2791-3171 - https://doi.org/10.54878/mxegpk56

defensive side, network-analytic and machine-learning tools are the natural instruments for detecting Financial Convergence Risk, because they operate on relationships and patterns across large volumes rather than on isolated transactions; the cross-sector matching envisaged in Recommendation B is, in practice, an AI-enabled capability. On the risk side, however, AI also amplifies FCR: as monitoring, screening and onboarding decisions are increasingly automated and outsourced to third-party models, the interval between a financial action and a locus of answerability lengthens, and the candidates for responsibility when a pathway is missed multiply across the deploying institution, the model vendor, the compliance function and the validation team. The appropriate response is not nominal "human-in-the-loop" presence but context-appropriate human control, oversight matched to actual decision authority and risk, together with model governance that fixes accountability for automated decisions. AI is thus both the sharpest tool for closing convergence risk and, ungoverned, a mechanism for widening it (Amicelle, 2011; FATF, 2019).

Tensions and trade-offs

The model must navigate genuine tensions, and it is more credible for naming them. The first is the standing tension between the growth imperative and the security imperative: measures that raise friction can deter legitimate capital, so a resilience architecture must be calibrated to target convergence risk rather than to impose indiscriminate cost on lawful commerce. The second is the tension between intelligence effectiveness and data privacy and protection, acute in a jurisdiction with a federal data-protection law (Federal Decree-Law No. 45 of 2021) and autonomous free-zone regimes, which is why Recommendation B insists on privacy-preserving matching rather than data pooling. The third concerns the non-profit sector, where the objective must be precision rather than de-risking. The fourth is resource intensity: fusion, analytics and red-teaming demand skilled personnel and sustained investment, and the model should be sequenced accordingly.

The FATF effectiveness context

The model should finally be read against FATF's effectiveness paradigm rather than the binary of grey-listing. The salient point is not the risk of a return to the list, which the UAE's reforms have substantially reduced, but the standing requirement to demonstrate that the system produces results, that it detects, disrupts and deprives (Wolfsberg Group, 2019). The FHRM is, in effect, an architecture for effectiveness: its metrics measure disruption, its intelligence loop compounds detection, and its fusion grid targets the systemic seams that effectiveness assessments probe. Positioned this way, the model is the next evolutionary layer of a mature regime, not a critique of a deficient one.

4.6 Limitations, Counter-arguments and Research Agenda

Counter-arguments

Three objections merit a direct answer. First, it may be said that the model describes an ordinary compliance problem soluble through existing powers. It does not: FCR is a network-level problem that institution-level powers cannot solve even in combination, because the vulnerability sits at the interfaces between institutions rather than within any one of them. Second, it may be said that the Central Bank already possesses sufficient supervisory authority. That is true but beside the point: the issue is not the CBUAE's authority but the structure of detection, and a supervisor cannot see what no institution can see, cross-sector visibility requires a fusion capability that no single supervisor provides. Third, it may be said that the architecture is too resource-intensive. Its cost must be weighed against the cost of relapse, reputational damage and undetected terrorist financing; the scale of 2025 enforcement indicates that the underlying risk is real, and the sequencing proposed in Section 4.4 allows the lower-cost measures to precede the higher-investment infrastructure.

Limitations

The FHRM is conceptual and doctrinal, and its empirical validation is a task for further research. Four limitations should be acknowledged. First, the absence of access to confidential STR data, classified intelligence or privileged enforcement material means the analysis relies on publicly available sources. Second, the operationalisation of the Time-to-Disruption and Financial Network Containment metrics requires data-collection protocols that are not yet in place. Third, the comparative analysis is illustrative rather than exhaustive, focusing on three jurisdictions with mature public-private partnerships. Fourth, the article does not quantitatively test the model's predictive power against case data.

Research agenda

These limitations define the agenda. The central next step is the construction of a UAE terrorist-financing financial-hub dataset that links terrorist organisations, facilitators, companies, beneficial owners, financial institutions, jurisdictions, transaction methods, predicate offences and enforcement outcomes, drawing on FATF and

ISSN: 2791-3171 - https://doi.org/10.54878/mxegpk56

MENAFATF evaluations, UAEFIU and CBUAE material, free-zone regulators, prosecutorial and court records, and cognate international sources. Such a dataset would allow the FHRM to be tested against the conventional compliance model as an explanation of the UAE's exposure and resilience, and would permit the Time-to-Disruption and Financial Network Containment metrics to be computed on real cases. Comparative study of public-private intelligence models, empirical analysis of enforcement and STR typologies, and assessment of the efficacy of network-analytic and blockchain-analytic technologies follow naturally (Levi & Soudijn, 2020; Jofre et al., 2024).

5. Conclusion

A globally connected financial centre cannot achieve sustainable counter-terrorist-financing effectiveness through institution-level compliance alone. The connectivity that generates its prosperity also generates an exposure distributed across sectors, channels and jurisdictions, and a defensive architecture organised around single institutions will systematically under-detect a threat organised around the interfaces between them. This is the Financial Hub Paradox, and it is the problem the United Arab Emirates must solve to convert its regulatory achievements into durable strategic advantage.

This article has proposed a solution in the Financial Hub Resilience Model. By elevating the unit of analysis from the institution to the hub, the model reframes the policy problem; through the Financial Hub Attack Surface it maps the terrain of exposure; through Financial Convergence Risk it names the specific vulnerability at the interfaces; and through the Financial Intelligence Learning Loop it supplies the adaptive mechanism by which the ecosystem learns. From these foundations it derives an operational programme, network-level risk scoring, privacy-preserving cross-sector intelligence, typology-led detection, an operational public-private partnership, red-team resilience testing, the Time-to-Disruption and Financial Network Containment metrics, and a National Financial Threat Intelligence Grid to bind them together.

The framework is offered constructively and with due acknowledgement of what the UAE has already built. Its strengthened Financial Intelligence Unit, its overhauled 2025 legislation, its assertive enforcement, its national strategy and its public-private machinery are the necessary foundation on which a resilience architecture can be raised; the argument here is that they are necessary but not, by themselves, sufficient for the effectiveness the next phase demands. The model is also portable: with appropriate adaptation, its constructs and metrics apply to other globally connected centres facing the same paradox, and the UAE is well placed to pioneer them. If the UAE takes up that agenda, it will be positioned to master its risk environment rather than merely to manage it, and to make its financial connectivity a sustained advantage in financial integrity and national security rather than a residual vulnerability.

Declarations

Funding. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing interests. The author reports no competing interests to declare.

Data availability. No new data were generated or analysed in support of this research. The study draws entirely on publicly available primary documents and secondary literature, all of which are cited in the references.

Ethics. This research did not involve human participants, human data, or animal subjects, and no ethical approval was required.

Author contributions (CRediT). Conceptualization: V. V. Tamhane; Methodology: V. V. Tamhane; Investigation: V. V. Tamhane; Formal analysis: V. V. Tamhane; Writing - original draft: V. V. Tamhane; Writing - review & editing: V. V. Tamhane.

AI-Usage

The author acknowledges the use of AI-based language tools for grammar and style checking, citation formatting and reference verification. Their use was limited to linguistic and formatting refinement. All ideas, analysis, argumentation and framework development are solely those of the author, who takes full responsibility for the content.

References

References follow APA 7th edition style. Journal articles carry digital object identifiers (resolvable via https://doi.org/); legislation, regulatory instruments and institutional reports are cited to their official web locations; and, per APA 7th edition, print monographs without an assigned DOI are cited to the publisher.

Legislation and Regulatory Instruments

Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (United States). https://www.fincen.gov/resources/statutes-regulations/bank-secrecy-act

Cabinet Resolution No. 134 of 2025 Concerning the Executive Regulations of Federal Decree-Law No. 10 of 2025 (United Arab Emirates). https://rulebook.centralbank.ae/en/rulebook/cabinet-resolution-no-134-2025-regarding-executive-regulations-federal-decree-law-no-10

Central Bank of the United Arab Emirates. (2024-2026). AML/CFT Rulebook and supervisory guidance (including guidance on trade-based money laundering, correspondent banking, and proliferation financing). https://www.centralbank.ae

Federal Decree-Law No. 7 of 2024 amending the Anti-Money Laundering and Combating the Financing of Terrorism framework (United Arab Emirates). https://rulebook.centralbank.ae/en/rulebook/federal-law-decree-no-7-2024-amending-certain-provisions-federal-law-law-no-20-2018-anti

Federal Decree-Law No. 10 of 2025 Regarding Combating Money Laundering Crimes, Combating the Financing of Terrorism and the Financing of Arms Proliferation (United Arab Emirates). https://rulebook.centralbank.ae/en/rulebook/federal-decree-law-no-10-2025-regarding-anti-money-laundering-and-combating-financing

Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Illegal Organisations (repealed) (United Arab Emirates). https://uaelegislation.gov.ae/en/legislations/1500

Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data (United Arab Emirates). https://uaelegislation.gov.ae/en/legislations/3912

United Nations Security Council. (1999). Resolution 1267 (S/RES/1267). https://main.un.org/securitycouncil/en/s/res/1267 -(1999)

United Nations Security Council. (2001). Resolution 1373 (S/RES/1373). https://www.un.org/securitycouncil/content/resolutions

USA PATRIOT Act of 2001, Pub. L. No. 107-56, §§ 314(a)-(b), 115 Stat. 272 (United States). https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act

Scholarship and Reports

Amicelle, A. (2011). Towards a "new" political anatomy of financial surveillance. Security Dialogue, 42(2), 161-178. https://doi.org/10.1177/0967010611401472

Biersteker, T. J., & Eckert, S. E. (Eds.). (2008). Countering the financing of terrorism. Routledge.

Chaikin, D. (2009). How effective are suspicious transaction reporting systems? Journal of Money Laundering Control, 12(3), 238-253. https://doi.org/10.1108/13685200910973628

de Goede, M. (2012). Speculative security: The politics of pursuing terrorist monies. University of Minnesota Press. https://doi.org/10.5749/minnesota/9780816675890.001.0001

de Koker, L. (2006). Money laundering control and suppression of financing of terrorism: Some thoughts on the impact of customer due diligence measures on financial exclusion. Journal of Financial Crime, 13(1), 26-50. https://doi.org/10.1108/13590790610641206

Dion-Schwarz, C., Manheim, D., & Johnston, P. B. (2019). Terrorist use of cryptocurrencies: Technical and organizational barriers and future threats. RAND Corporation. https://www.rand.org/pubs/research_reports/RR3026.html

Fanusie, Y. J., & Robinson, T. (2018). Bitcoin laundering: An analysis of illicit flows into digital currency services. Center on Sanctions and Illicit Finance & Elliptic. https://www.fdd.org/analysis/2018/01/10/bitcoin-laundering-an-analysis-of-illicit-flows-into-digital-currency-services/

Financial Action Task Force. (2013). The role of hawala and other similar service providers in money laundering and terrorist financing. FATF. https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Role-hawalas-in-ml-tf.html

Financial Action Task Force. (2019). Guidance for a risk-based approach to virtual assets and virtual asset service providers. FATF. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Rba-virtual-assets-2019.html

Financial Action Task Force. (2021). Trade-based money laundering: Trends and developments. FATF. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Trade-based-money-laundering-trends-and-developments.html

Financial Action Task Force. (2023). Methodology for assessing technical compliance with the FATF Recommendations and the effectiveness of AML/CFT systems (updated). FATF. https://www.fatf-

gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html

Financial Action Task Force & MENAFATF. (2020). Anti-money laundering and counter-terrorist financing measures, United Arab Emirates: Mutual evaluation report. FATF. https://www.fatf-gafi.org/en/publications/Mutualevaluations/Mer-uae-2020.html

Findley, M. G., Nielson, D. L., & Sharman, J. C. (2014). Global shell games: Experiments in transnational relations, crime, and terrorism. Cambridge University Press. https://doi.org/10.1017/CBO9781107337848

Freeman, M. (2011). The sources of terrorist financing: Theory and typology. Studies in Conflict & Terrorism, 34(6), 461-475. https://doi.org/10.1080/1057610X.2011.571193

Government of the United Arab Emirates. (2024). National strategy for anti-money laundering, combating the financing of terrorism and proliferation financing 2024-2027. https://www.namlcftc.gov.ae

Halliday, T. C., Levi, M., & Reuter, P. (2014). Global surveillance of dirty money: Assessing assessments of regimes to control money-laundering. Center on Law and Globalization. https://doi.org/10.2139/ssrn.4928216

Jofre, M., Aziani, A., & Villa, E. (2024). Terrorist financing: Traditional vs. emerging financial technologies. Terrorism and Political Violence, 38(4), 354-367. https://doi.org/10.1080/09546553.2024.2433635

Keatinge, T., Carlisle, D., & Keen, F. (2018). Virtual currencies and terrorist financing: Assessing the risks and evaluating responses. European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs. https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2018)604970

Levi, M., & Reuter, P. (2006). Money laundering. Crime and Justice, 34(1), 289-375. https://doi.org/10.1086/501508

Levi, M., Reuter, P., & Halliday, T. (2018). Can the AML system be evaluated without better data? Crime, Law and Social Change, 69(2), 307-328. https://doi.org/10.1007/s10611-017-9757-4

Levi, M., & Soudijn, M. (2020). Understanding the laundering of organized crime money. Crime and Justice, 49(1), 579-631. https://doi.org/10.1086/708047

Levitt, M. (2013). Hezbollah: The global footprint of Lebanon's Party of God. Georgetown University Press.

Maxwell, N. J., & Artingstall, D. (2017). The role of financial information-sharing partnerships in the disruption of crime (Occasional Paper). Royal United Services Institute. https://www.rusi.org/explore-our-research/publications/occasional-papers/role-financial-information-sharing-partnerships-disruption-crime

Nagin, D. S. (2013). Deterrence in the twenty-first century: A review of the evidence. Crime and Justice, 42(1), 199-263. https://doi.org/10.1086/670398

Nance, M. T. (2018). The regime that FATF built: An introduction to the Financial Action Task Force. Crime, Law and Social Change, 69(2), 109-129. https://doi.org/10.1007/s10611-017-9747-6

Passas, N. (2006). Fighting terror with error: The counter-productive regulation of informal value transfers. Crime, Law and Social Change, 45(4-5), 315-336. https://doi.org/10.1007/s10611-006-9041-5

Pol, R. F. (2020). Anti-money laundering: The world's least effective policy experiment? Together, we can fix it. Policy Design and Practice, 3(1), 73-94. https://doi.org/10.1080/25741292.2020.1725366

Raab, J., & Milward, H. B. (2003). Dark networks as problems. Journal of Public Administration Research and Theory, 13(4), 413-439. https://doi.org/10.1093/jpart/mug029

Ryder, N. (2015). The financial war on terrorism: A review of counter-terrorist financing strategies since 2001. Routledge. https://doi.org/10.4324/9780203722589

Sharman, J. C. (2011). The money laundry: Regulating criminal finance in the global economy. Cornell University Press. https://doi.org/10.7591/9780801463198

Teichmann, F. M. J. (2019). Recent trends in money laundering and terrorism financing. Journal of Financial Regulation and Compliance, 27(1), 2-12. https://doi.org/10.1108/JFRC-03-2018-0042

UAE Financial Intelligence Unit. (2024). Annual report 2024. UAEFIU. https://www.uaefiu.gov.ae/en/more/knowledge-centre/publications/annual-report/annual-report-2024/

UAE Financial Intelligence Unit. (2025a). Strategic analysis report on terrorist financing. UAEFIU. https://www.uaefiu.gov.ae/en/more/knowledge-centre/publications/trends-typology-reports/strategic-analysis-report-on-terrorist-financing/

UAE Financial Intelligence Unit. (2025b). Misuse of virtual assets in financial crime. UAEFIU. https://www.uaefiu.gov.ae/en/more/knowledge-centre/publications/trends-typology-reports/misuse-of-virtual-assets-in-financial-crime/

Wolfsberg Group. (2019). Wolfsberg Group statement on effectiveness. https://wolfsberg-

group.org/news/wolfsberg-group-statement-on-effectiveness-2019/

Zabyelina, Y. (2022). The “Capone Discovery”: Extortion as a method of terrorism financing. Studies in Conflict & Terrorism, 45(5-6), 501-516. https://doi.org/10.1080/1057610X.2019.1678860