SITJOURNAL
Security Intelligence Terrorism Journal

Security Intelligence Terrorism Journal (SITJ), Vol. 03 No. 02 (2026), pp. 126-137
Research Article
doi: https://doi.org/10.70710/sitj.v3i2.96

Countering Radicalisation Financing Through Financial Intelligence and Predictive Risk Analytics from A Security Governance Perspective

Vipul V. Tamhane[1,a,*]

[1]Department of Law, Northumbria University, Newcastle upon Tyne, UK
[a]vipul.tamhane@gmail.com
*Corresponding author

Article Info
Received: 23-May-2026
Revised: 15-June-2026
Accepted: 30-June-2026

Keywords
AML/CFT; Counter-Terrorist Financing; Financial Intelligence; Financial Intelligence Units; Radicalisation Financing

Abstract
The global counterterrorism financing (CTF) architecture faces a systemic gap. Whereas conventional Financial Intelligence Unit (FIU) frameworks and Anti-Money Laundering/Counter Financing of Terrorism (AML/CFT) regimes were designed to detect operational terrorist financing, the movement of funds toward imminent attacks, they cannot detect the antecedent layer: radicalisation financing. This paper develops a novel framework, the Predictive Security Governance (PSG) model, to address this governance deficit. Drawing from a systematic literature review with expansive sources spanning financial intelligence transformation, machine learning applications, security governance theory, and human rights jurisprudence, the paper puts forward the PSG model as a theoretical frame, shown through four real-world-ish cases. These include Islamic State crowdfunding, Hamas cryptocurrency channels, far-right online donation ecosystems, and South Asian hawala linked networks. The overall idea blends three mutually dependent dimensions, as they feed each other: Institutional Intelligence Fusion; Algorithmic Risk Profiling (rooted in a three layer predictive architecture), and Human Rights Anchored Governance (put into practice via a proportionality triage mechanism). A Bidirectional Analytical Model (BAM) specifies the recursive feedback between intelligence outputs and governance recalibration, including explicit boundary conditions governing BAM functionality in data-sparse and institutionally constrained contexts. Existing CTF frameworks, the FATF risk-based approach, Egmont intelligence-sharing protocols, and UN CTED rights guidance, address radicalisation financing phenomenologically but not governance-systemically; the PSG model is the first framework to integrate institutional, algorithmic, and normative dimensions for this specific domain.

1. Introduction

On 22 March 2016, coordinated bombings in Brussels killed thirty-two civilians. After the incident, some financial forensics looked more closely and suggested the network had been taking money through hawala circuits, cryptocurrency micro-wallets, and even small-denomination bank transfers, months earlier than normal AML triggers could really catch anything. So, what went unseen wasn't exactly the last financing chain, but the earlier setup—like the steady flow of funds that supported ideological indoctrination, the encrypted communications infrastructure, and also preparatory travel. This was not an intelligence failure in the conventional sense, it was a governance architecture failure, the systematic incapacity of existing CTF frameworks to see what preceded the acts they were designed to prevent.

This paper begins with the recognition that radicalisation financing, defined here as the provision, mobilisation, transfer, or accumulation of financial and material resources intended to facilitate ideological dissemination, extremist recruitment, online propaganda, or pre-operational support for violent extremism, occupies a critical lacuna in both the academic literature and the regulatory landscape. The Financial Action Task Force (FATF), global standard-setter for AML/CFT, continues to orient its forty recommendations primarily toward operational financing: the movement of funds toward attack execution. The pre-operational layer, funding that sustains radicalisation as a process, receives fragmented, inconsistent, and largely atheoretical treatment.

Three structural deficits constitute the problem this paper addresses. The first is conceptual: "radicalisation financing" does not exist as a distinct legal or analytical construct in any major CTF framework. Existing practitioner frameworks, FATF typologies, Egmont Group protocols, UN monitoring team reports, address radicalisation financing phenomenologically, identifying modalities and typologies, but do not theorise it governance-systemically (Freeman, 2011; FATF, 2015; Deol, 2019). The PSG model's contribution is not to invent the category ex nihilo but to provide, for the first time, a tripartite governance framework, institutional, algorithmic, and normative, for this specific and underserved domain. The second deficit is institutional: the 2022 empirical study by Jayasekara demonstrated that administrative FIUs, which have proliferated globally, lack the structural architecture for proactive, strategic intelligence production. The third deficit is normative: predictive analytics in CTF have expanded without coherent governance frameworks, risking algorithmic discrimination, financial surveillance overreach, and chilling effects on legitimate religious and humanitarian activity (UN CTED/OHCHR, 2025).

The paper addresses these deficits through the Predictive Security Governance (PSG) model, a theoretically grounded framework illustrated through four empirically diverse cases. Following Eckstein's (1975) distinction between plausibility probes and crucial case tests, the four cases demonstrate that the PSG model can accommodate diverse radicalisation financing modalities across ideological and geographic contexts. They do not constitute a formal test of the PSG propositions; that requires future research using primary FIU data. The model's four testable propositions are specified for that purpose in Section 3.

The paper makes four distinct contributions. First, it formally constitutes "radicalisation financing" as a governance category, extending prior phenomenological typologies into a systems-level framework. Second, it develops the PSG model as the first framework integrating institutional intelligence fusion, algorithmic risk profiling, and human rights-anchored governance for the radicalisation financing domain. Third, it introduces the Bidirectional Analytical Model (BAM), which reconceptualises the intelligence-governance relationship as recursive rather than unidirectional, and specifies its operational boundary conditions. Fourth, it operationalises human rights principles within predictive CTF systems, bridging the gap between principled rights advocacy and governance specificity.

The paper proceeds as follows. Section 2 reviews the literature across three epistemic pillars. Section 3 develops the PSG model, including the BAM, measurement framework, and legal-institutional interface. Section 4 presents four illustrative cases reframed as plausibility probes. Section 5 discusses governance implications, boundary conditions, and critical counterarguments. Section 6 concludes.

2. Literature Review

2.1. Pillar One: Terrorist Financing and the Radicalisation Layer

The academic literature on terrorist financing has been, invariably shaped by that post-September 11 institutional architectures and academic contributions globally. Levitt and Jacobson (2008) laid out a foundational typology , touching on state sponsorship, criminal enterprises, legitimate business fronts, and charitable organisations , and it became the common analytical vocabulary used in both academic and practitioner talks. Following that, the work by Biersteker and Eckert (2008), Oftedal (2015), and Freeman (2011) kept pushing for more nuanced explanations of the four-stage “Threat Finance” model: generation, movement, storage and use, with each stage getting extra attention or slightly different interpretations. This framework, adopted by the UK Ministry of Defence and widely diffused through FATF mutual evaluations, remains the dominant analytical scaffold for CTF policy.

Yet this literature shares a constitutive limitation: it conceptualises terrorist financing as an operational phenomenon oriented toward attack execution. The pre-operational layer, the financing of ideological mobilisation and preparatory activities, receives marginal treatment. Freeman (2011) distinguishes "support" financing (sustaining the organisation) from "operational" financing (funding specific attacks), but does not develop a governance framework for the precursor layer. Stern and Berger's (2015) influential account of Islamic State financing similarly focuses on revenue generation and operational deployment rather than the radicalisation pipeline. FATF's 2015 ISIL typology report, while documenting external donations and small-value transfers to foreign fighters, does not theorise these flows within a governance framework capable of systematic detection. Deol (2019) comes closest, examining small-value distributed funding ecosystems, but without the institutional or normative architecture required for anticipatory governance.

The emerging financing modalities of the post-2015 period have further strained existing frameworks. Van Wegberg, Oerlemans, and Van Deventer (2018) demonstrate that empirical evidence for cryptocurrency as a dominant terrorist financing vector remains contested; the policy literature has arguably over-indexed on cryptocurrency risk relative to informal value transfer systems and social media micropayments. The FATF's 2021 virtual assets report documents crowdfunding as a radicalisation financing mechanism but does not specify the detection or governance architecture required to address it. Digital hawala, increasingly mediated through WhatsApp, Telegram, and mobile money platforms post-2020, represents a further modality that straddles formal and informal financial infrastructure in ways that challenge both transactional monitoring and OSINT-based detection.

According to Prunckun (2015) in his book Scientific Methods of Inquiry for Intelligence Analysis, intelligence as knowledge may refer to several contexts, including national security, military affairs, law enforcement, business, and other private sectors. Meanwhile, intelligence as a process is understood as a series of steps or procedures summarized within an intelligence cycle, commonly referred to as the intelligence cycle process. In practice, the intelligence cycle generally consists of several interrelated stages, including direction, collection, processing, analysis, dissemination, and feedback. These stages are designed to ensure that information is systematically transformed into intelligence products that support decision-making processes.

2.2. Pillar Two: Financial Intelligence, from Transaction Monitoring to Predictive Analytics

The transformation of Financial Intelligence Units from passive Suspicious Transaction Report repositories to proactive strategic intelligence producers represents the most significant institutional development in CTF governance of the past decade. Jayasekara's (2022) empirical study, drawing on FATF mutual evaluation data across sixty-three jurisdictions, established a negative correlation between administrative FIU models and overall AML/CFT effectiveness. Jayasekara attributes this to structural separation from law enforcement, attenuating the operational feedback mechanisms essential for intelligence calibration. The Council of Europe's (2025) practitioner survey challenges this finding, identifying strategic analysis, a function more naturally situated within administrative FIUs, as the emerging cornerstone of effective CTF, citing the UN goFintel software deployment as demonstrating that analytics-capable administrative FIUs can outperform enforcement-oriented models on strategic intelligence production.

The machine learning literature demonstrates what predictive analytics can detect but does not address how such systems should be governed. Rajapaksha and colleagues (2024) report an LSTM-based model achieving 94% recall with a 12% false positive rate for temporal transaction anomaly detection, superior to rule-based systems but operationally burdensome at scale. Weber et al. (2019) application of graph neural networks to AML datasets shows that relational features carry predictive information orthogonal to individual transaction characteristics. Morselli's (2014) network analysis approaches, applied to criminal financial networks, demonstrate that graph-theoretic methods identify financing nodes invisible to transaction-level monitoring. The critical gap is not technical but epistemic: almost no research addresses how predictive outputs should be governed, particularly for radicalisation financing where evidence thresholds are legally ambiguous and training datasets are sparse and ideologically skewed.

The OSINT integration literature offers the most direct relevance to radicalisation financing detection. The Moody's (2025) case study documents a 70% reduction in complex corporate structure mapping time through OSINT-financial data integration. For radicalisation financing, OSINT enables correlation of ideological engagement signals, social media activity, platform subscriptions, content creation, with financial behavioural anomalies, enabling detection of the behavioural-financial co-signatures that characterise the pre-operational layer. Kalabukhova (2025) identifies OSINT integration as the decisive differentiator between reactive and anticipatory FIU intelligence production.

2.3. Pillar Three: Security Governance, Balancing Prediction, Prevention, and Rights

The security governance literature provides the most theoretically sophisticated engagement with CTF's institutional dimensions. Krahmann's (2003) conceptualisation of security governance as a shift from hierarchical state control toward multi-stakeholder, accountable, risk-based management supplies the conceptual vocabulary for analysing CTF institutional architectures. Wood and Shearing's (2007) nodal governance framework illuminates how FIUs, banks, technology platforms, civil society, and international bodies constitute a governance network whose effectiveness depends on information flow quality and institutional incentive alignment across nodes rather than centralised command.

Critical scholarship demands explicit engagement here. Bigo's (2002) securitisation theory warns that the expansion of surveillance to pre-criminal domains reproduces the pathologies it seeks to prevent: the targeting of Muslim communities, diaspora populations, and humanitarian organisations through statistical profiling rather than individualised evidence. Amoore's (2013) account of algorithmic governance identifies the "data derivative" as a novel form of power that operates below legal thresholds, generating actionable suspicion without prosecutable evidence. Lyon's (2015) surveillance studies perspective locates predictive CTF within a broader architecture of what he terms "social sorting", the differential allocation of risk and opportunity based on algorithmically assigned categories. These critiques are not peripheral to the PSG model; they are constitutive of its Human Rights-Anchored Governance dimension, which is designed precisely to operationalise structural safeguards against these pathologies.

The human rights literature has been sharpened by the 2025 UN CTED/OHCHR guidance, which identifies four categories of rights risk in predictive CTF: privacy intrusion through financial surveillance without reasonable suspicion; algorithmic discrimination through risk profiles embedding protected characteristics as proxy variables; chilling effects on legitimate political, religious, and humanitarian activity; and due process violations through use of predictive outputs as substitutes for individualised assessment. The ICCPR's proportionality standards (Articles 14, 17, 26), the GDPR's automated decision-making framework (Article 22), and the EU AI Act's high-risk AI system requirements collectively constitute the legal architecture within which any PSG implementation must operate. The OSCE FOLLOW project (2025-2029) specifically addresses the CTF-financial inclusion tension, identifying the absence of proportionality frameworks as a material driver of de-risking, the systemic termination of banking relationships with diaspora communities, NPOs, and money service businesses.

2.4. Synthesis: The Governance Gap

The systematic literature review identifies a gap that no existing framework addresses: the integration of institutional intelligence fusion, algorithmic risk profiling, and human rights-anchored governance within a single architecture for radicalisation financing specifically. Table 1 maps this gap against existing frameworks.

Table 1. PSG Model vs. Existing CTF Governance Frameworks

Dimension	FATF Risk-Based	Egmont Sharing	UN CTED/OHCHR	PSG Model
Institutional specification	High (Recs 1-40)	Medium (sharing protocols)	Low (principles only)	High (strategic analysis units, fusion infrastructure)

Dimension	FATF Risk-Based	Egmont Sharing	UN CTED/OHCHR	PSG Model
Algorithmic governance	None	None	Low (general AI concerns)	High (3-layer architecture, bias audits)
Rights operationalisation	Low (proportionality principle)	None	Medium (principles without mechanisms)	High (triage, redress, oversight)
Radicalisation financing specific	No	No	No	Yes
Recalibration mechanism	No (static)	No	No	Yes (BAM reverse flow)

Table 2. Epistemic Status of Evidence in This Paper

Claim Type	Evidence Provided	Epistemic Status	Future Research Required
Radicalisation financing is conceptually distinct from operational TF	Logical argument + illustrative cases	**Framework proposal**	Empirical validation of typology across FIU datasets
Existing FIUs lack radicalisation-specific architectures	FATF mutual evaluations; Jayasekara (2022); CoE (2025)	**Documented**	None required (sufficient secondary evidence)
PSG model integrates three dimensions coherently	Theoretical synthesis + plausibility probes	**Plausibility demonstrated**	Comparative institutional testing across FIU models
PSG reduces false positives vs. rule-based systems	No primary data; logical inference	**Hypothesised (P2)**	Controlled experiment or field study with primary FIU data

3. Method

The PSG (Predictive Security Governance) model develops a theoretical framework for governing predictive analytics in the detection of radicalisation financing. It rests on three foundational constructs: risk based governance, like the FATF risk-based approach, but also extended into behavioural and longer-term risk dimensions ; intelligence led security governance (taking from Ratcliffe's 2016 intelligence-led policing), and then repurposed for the FIU setting by Gill and Phythian (2018); and then algorithmic accountability , basically operationalised via the EU AI Act requirements for high-risk automated systems.

These three things are dynamically interdependent. For example risk-based governance without intelligence fusion turns into pretty static models stay vulnerable to the adaptive adversaries, intelligence-led governance without algorithmic accountability ends up pushing things into surveillance overreach, and algorithmic accountability without risk based governance leads to rights compliance frameworks that are, somehow decoupled from what's actually happening operationally.

3.1. Dimension One: Institutional Intelligence Fusion

Dimension One: Institutional Intelligence Fusion mandates structural integration of operational and strategic intelligence functions within FIUs. This is a functional necessity for radicalisation financing detection: a Suspicious Transaction Report involving a small transfer to a Middle Eastern jurisdiction is operationally uninterpretable without strategic intelligence contextualising the radicalisation financing

typologies operating through that corridor. The PSG model mandates dedicated strategic analysis units embedded within administrative FIUs, systematically integrated with operational casework through shared intelligence repositories and mandatory inter-unit consultation protocols. Multi-source data fusion, the systematic integration of STR data with corporate registry information, geospatial intelligence, social media analysis, and cross-border intelligence, constitutes the data infrastructure of this dimension.

3.2. Dimension Two: Algorithmic Risk Profiling

Dimension Two: Algorithmic Risk Profiling specifies a three-layer predictive architecture. Layer One employs unsupervised clustering (k-means, DBSCAN) to establish behavioural baselines by entity typology; radicalisation financing-specific indicators include high-frequency, low-value transfers to conflict-proximate jurisdictions and temporal correlation between financial activity and OSINT-derived ideological engagement markers. Layer Two deploys LSTM neural networks for temporal anomaly detection, capturing the longitudinal escalation patterns characteristic of the radicalisation financing lifecycle that single-point transaction monitoring cannot detect. Layer Three applies graph-theoretic network analysis to identify relational anomalies: entities that are individually low-risk but whose network connections constitute collectively suspicious structures. Composite risk scoring across all three layers feeds the proportionality triage mechanism of Dimension Three.

3.3. Dimension Three: Human Rights-Anchored Governance

Dimension Three, Human Rights anchored Governance operationalises the critical security theory's warnings against surveillance overreach through three mechanisms, not all of them loud. First, proportionality triage sets up a three-tiered response protocol: low-confidence alerts lead to a recalibration loop, and there's no institutional action, like we just adjust and move on. Medium-confidence alerts go to enhanced due diligence via non intrusive information requests, instead of jumping right in. High-confidence alerts then trigger STR filing with a contextual narrative, proper explanation included. Critically, no alert triggers automatic law enforcement referral, human analytical judgment is a required intermediate step at every tier, preserving the distinction between intelligence (which requires probabilistic assessment) and evidence (which requires legal standards of proof). Second, algorithmic transparency requirements mandate documentation of model inputs, feature weights, decision thresholds, and bias audit findings, subject to review by an independent oversight body. Third, redress mechanisms, the operational expression of due process rights under ICCPR Article 14, provide individuals affected by predictive CTF measures with rights of explanation and appeal through an institutional channel independent of the FIU.

3.4. Legal-Institutional Interface

The PSG governance mechanisms must operate within existing statutory frameworks. Three interface conditions govern this relationship. On STR obligations: in jurisdictions where STR filing is mandatory upon suspicion (e.g., US Bank Secrecy Act Section 5318(g); EU 6AMLD Article 3), the PSG's prohibition on automatic law enforcement referral does not override filing duties. The model distinguishes between filing (a statutory obligation) and referral (a discretionary act): low-confidence alerts trigger neither; medium-confidence alerts trigger filing without referral; high-confidence alerts trigger filing with optional contextual referral. This preserves legal compliance while operationalising proportionality. On oversight body specifications: the "independent oversight body" may take the form of a dedicated CTF algorithmic audit unit within an existing National Human Rights Institution, or a newly mandated subcommittee of the FIU's supervisory board with majority civil society representation. The model requires functional equivalence across five dimensions: independence, technical expertise, access rights, sanctioning power, and transparency reporting. On redress as a statutory right: the right of explanation and appeal must be embedded in primary legislation, not administrative guidance. The model therefore predicts slower PSG adoption in common law jurisdictions (where judicial precedent governs procedural rights) than in civil law systems with dedicated data protection statutes. In jurisdictions with mandatory automatic referral requirements, full PSG implementation requires legislative amendment; the model is presented as a normative target for legal reform in those contexts, not an immediate technical fix.

3.5. The Bidirectional Analytical Model (BAM)

The Bidirectional Analytical Model (BAM) constitutes the theoretical innovation most distinctive to the PSG framework. Existing CTF models conceptualise the intelligence-governance relationship as unidirectional: intelligence informs regulatory and law enforcement action. The BAM posits a recursive feedback loop in which governance outcomes, false positive rates, rights complaint data, judicial review findings, actively recalibrate the intelligence function, preventing the ossification of risk profiles and correcting for algorithmic bias. The forward flow moves from financial and OSINT data through algorithmic processing toward risk classifications and institutional response. The reverse flow returns from outcome data through the governance layer back to algorithmic recalibration. This bidirectionality is not merely procedural but epistemological: it ensures that the knowledge claims produced by predictive systems remain falsifiable and subject to institutional challenge, addressing Amoore's (2013) critique that algorithmic governance operates below accountability thresholds.

3.6. BAM Boundary Conditions

The BAM's recalibration mechanism operates only under specifiable boundary conditions that define its domain of applicability. Three boundary conditions are identified. The data infrastructure boundary: the reverse flow requires outcome data of sufficient quality, timeliness, and granularity. Where FIUs lack access to judicial review outcomes (common in administrative models with limited court feedback loops), or where false positive rates are not systematically tracked, recalibration defaults to static parameterisation, and the BAM functions as a normative aspiration rather than an operational description. The minimum data governance maturity required is equivalent to FATF Recommendation 29's "adequate operational resources and technical systems." The institutional incentive boundary: recalibration requires organisational incentives to update models on the basis of negative feedback. In FIUs where performance metrics reward case volume rather than precision, or where legal liability attaches to missed detection rather than over-reporting, the BAM's reverse flow will be systematically underweighted. The model predicts that PSG effectiveness correlates with False Positive Incentive (FPI) alignment, a construct requiring empirical operationalisation. The technical boundary: recalibration assumes model architectures permitting parameter updating without catastrophic forgetting or bias amplification. Simpler models are more recalibration-friendly than deep neural networks; transparency requirements (Dimension Three) must include recalibration audit trails to prevent path-dependent algorithmic lock-in.

Table 3. BAM Failure Modes and PSG Mitigations

Failure Mode	Description	PSG Mitigation
Data-sparse recalibration	Insufficient outcome data to update parameters	Expert override protocols; conservative default thresholds; sunset clauses on model versions
Politically captured oversight	Independent body co-opted by securitisation actors	International peer review (Egmont Group + UN CTED joint audits); civil society majority on oversight subcommittees
Path-dependent lock-in	Algorithmic bias entrenches through feedback loops	Mandated random audits with reset capability; recalibration audit trails under transparency requirements
Incentive misalignment	FIUs rewarded for case volume rather than precision	Regulatory safe harbours for non-reporting of low-confidence alerts; FPI scoring for FIU evaluations

3.7. Testable Proposition

PSG Model: Four Testable Propositions:

1. P1: FIUs operationalising strategic intelligence functions (data fusion, trend analysis, typology development) will demonstrate higher detection rates of radicalisation financing than FIUs focused solely on operational case processing.

2. P2: Unsupervised clustering combined with LSTM-based anomaly detection identifies pre-operational radicalisation financing signatures with lower false positive rates than rule-based threshold systems.

3. P3: Proportionality triage mechanisms for predictive alerts reduce false positive burdens and rights infringement risks without materially compromising detection effectiveness.

4. P4: Administrative FIUs adopting the PSG framework perform equivalently to law enforcement FIUs on radicalisation financing detection while demonstrating superior rights compliance outcomes.

Table 4. PSG Model - Three Dimensions and Operational Specifications

Dimension	Key Components	Rights Safeguard
1. Institutional Intelligence Fusion	Strategic analysis units; multi-source data fusion (FININT, OSINT, GEOINT, HUMINT); cross-border coordination; shared intelligence repositories	Data minimisation; need-to-know access; sharing agreements with rights clauses
2. Algorithmic Risk Profiling	Layer 1: Unsupervised clustering (behavioural baselines); Layer 2: LSTM anomaly detection (temporal patterns); Layer 3: Graph-theoretic network analysis; composite risk scoring	Mandatory bias audits; explainability requirements; human analytical review at each layer output
3. Human Rights-Anchored Governance	Three-tier proportionality triage; algorithmic transparency documentation; independent oversight body review; rights-compliant data retention; institutional redress channels	Prohibition on automatic law enforcement referral; right of explanation and appeal; legislative embedding of redress rights

4. Results and Discussion

The four cases that follow are presented as theory-illustrative exemplars, not hypothesis tests. Following Eckstein's (1975) framework, they function as plausibility probes: they demonstrate that the PSG model accommodates diverse radicalisation financing modalities across ideological and geographic contexts without internal contradiction. Each case is analysed through three lenses, financing modality, detection failure mode, and PSG remedy, to demonstrate the model's analytical purchase. Causal claims regarding PSG effectiveness are hypothesised, not empirically established; they constitute Propositions P1-P4 for future testing.

4.1. The Islamic State External Fundraising Network (2014-2022)

The Islamic State's external fundraising network (2014-2022) provides the baseline illustration of radicalisation financing below conventional CTF detection thresholds. Post-hoc analyses documented individual transfers of €50-€200 to content creators and online platform operators that were entirely invisible to transaction monitoring systems calibrated for operational financing (Combating Terrorism Center, 2014-2019; FATF, 2015). The detection failure mode was threshold-based: rule-based systems

were calibrated to flag large, structured, or cross-border transfers, systematically missing the small-value, high-frequency, ideologically networked transfers sustaining the radicalisation ecosystem. The PSG remedy, LSTM temporal detection and graph-theoretic network analysis, addresses this failure mode by detecting longitudinal escalation and relational network structures rather than individual transaction anomalies. This case illustrates Proposition P2 (LSTM + clustering outperforms rule-based threshold detection.

4.2. Hamas Cryptocurrency Fundraising (2019-2023)

Hamas's cryptocurrency fundraising campaigns (2019-2023) illustrate the convergence of digital asset ecosystems and radicalisation financing. Blockchain forensic analyses estimated cumulative flows of approximately $41 million, though this figure is contested due to chain-hopping obfuscation that may have caused misattribution errors (Chainalysis, 2023). The detection failure mode was topological: individual wallet analysis could not detect the distributed solicitation network without graph-theoretic analysis of wallet relationships across campaigns. The PSG remedy, network analysis combined with OSINT correlation of social media solicitation campaigns to blockchain wallet clusters, addresses this failure mode. This case illustrates Proposition P1 (strategic OSINT-integrated intelligence fusion outperforms transaction-level analysis) and the BAM's OSINT integration requirement.

4.3. Far-Right Online Donation Ecosystems (2018-2024)

Far-right online donation ecosystems in the United States and Europe (2018-2024) provide the ideologically heterogeneous comparator essential for avoiding conflation of radicalisation financing with jihadist financing. Following mainstream de-platforming, financing networks migrated to alternative infrastructure, Telegram, Gab, cryptocurrency payment processors, generating distributed flows averaging $23-$47 per donation, with network-level aggregates reaching an estimated $2.3 million annually to the ten largest far-right content ecosystems (FinCEN, 2021). The detection failure mode was displacement-blindness: de-platforming by mainstream financial institutions did not disrupt the financing ecosystem but displaced it to infrastructure less visible to conventional monitoring. The PSG remedy, OSINT-financial co-signature detection tracking platform migration patterns alongside financial anomalies, addresses displacement dynamics directly. This case illustrates the BAM's recalibration requirement: risk models calibrated on traditional jihadist typologies systematically underperform on far-right financing without iterative recalibration.

4.4. South Asian Hawala-Linked Networks (2015-2023)

South Asian hawala-linked radicalisation networks (2015-2023) present the analytically most challenging case for the PSG model precisely because they involve minimal formal financial footprint. Documented networks linked to Lashkar-e-Taiba and Jaish-e-Mohammed combined formal hawala transfers with in-kind resource provision, accommodation, transportation, materials for propaganda production, that generates no transactional signature in formal financial systems. Post-2020 digital hawala adaptations, coordinating through WhatsApp and mobile money platforms, have partially increased the OSINT-detectable footprint, but the fundamental challenge remains. The PSG remedy, integration of FININT with HUMINT and GEOINT, and indirect indicator modelling based on associated digital behaviour, partially addresses this failure mode. Partially is the operative word: this case constitutes the clearest illustration of a BAM boundary condition. Where financing flows predominantly through informal, non-financial channels, predictive analytics operating on financial data will generate systematic blind spots regardless of algorithmic sophistication. The PSG model must explicitly acknowledge this non-predictability boundary rather than overclaiming its scope.

4.5. Discussion

South Asian hawala-linked radicalisation networks (2015-2023) present the analytically most challenging case for the PSG model precisely because they involve minimal formal financial footprint. Documented networks linked to Lashkar-e-Taiba and Jaish-e-Mohammed combined formal hawala transfers with in-kind resource provision, accommodation, transportation, materials for propaganda production, that generates no transactional signature in formal financial systems. Post-2020 digital hawala

Table 5. Cross-Case Synthesis, Financing Modalities, Detection Failures, and PSG Application (Illustrative)

Case	Ideology	Primary Modality	Detection Failure Mode	PSG Application
Islamic State	Jihadist-Salafi	Crowdfunding; crypto micro-wallets	Threshold-based monitoring; below STR triggers	LSTM temporal detection; network analysis (P2)
Hamas	Islamist-Nationalist	Cryptocurrency solicitation	Individual wallet analysis; no topology review	Graph analysis; OSINT-blockchain correlation (P1)
Far-Right	White Nationalist	Alternative payment platforms	De-platforming displaces rather than disrupts	OSINT co-signature; platform migration tracking (BAM recalibration)
South Asian Hawala	Jihadist; ethno-nationalist	Informal transfer; in-kind provision	No formal financial footprint	FININT-HUMINT-GEOINT integration; BAM boundary condition illustrated

adaptations, coordinating through WhatsApp and mobile money platforms, have partially increased the OSINT-detectable footprint, but the fundamental challenge remains. The PSG remedy, integration of FININT with HUMINT and GEOINT, and indirect indicator modelling based on associated digital behaviour, partially addresses this failure mode. Partially is the operative word: this case constitutes the clearest illustration of a BAM boundary condition. Where financing flows predominantly through informal, non-financial channels, predictive analytics operating on financial data will generate systematic blind spots regardless of algorithmic sophistication. The PSG model must explicitly acknowledge this non-predictability boundary rather than overclaiming its scope.

5. Conclusion

This paper has addressed a genuine gap in the CTF literature: the absence of a coherent governance framework for predictive analytics in the detection of radicalisation financing. The PSG model, integrating institutional intelligence fusion, algorithmic risk profiling, and human rights-anchored governance within a recursive feedback architecture, provides that framework as a theoretical proposal requiring empirical validation.

Four theoretical contributions are advanced. The paper formally constitutes radicalisation financing as a governance category, extending phenomenological typologies (Freeman, 2011; FATF, 2015; Keatinge, et al., 2019) into a systems-level framework. It develops the PSG model as the first tripartite integration of institutional, algorithmic, and normative dimensions for this domain. It introduces the BAM as a recursive intelligence-governance architecture with explicit boundary conditions. And it operationalises critical security theory's warnings against surveillance overreach through structural safeguards rather than declaratory principles.

The practical implications are direct. Administrative FIUs require not additional technology but institutional restructuring: strategic analysis unit embedding, multi-source fusion infrastructure, and proportionality triage protocols. The FATF must develop radicalisation financing-specific guidance, including typology appendices and mutual evaluation indicators. Legislatures must create legal frameworks distinguishing predictive intelligence from criminal evidence. These are reform targets, not immediate prescriptions; their feasibility varies by jurisdiction.

The limitations are substantive. The PSG model is theoretical; the four illustrative cases are plausibility probes, not hypothesis tests. Training data for radicalisation financing predictive systems are sparse and ideologically skewed. The BAM's recalibration mechanism depends on outcome data that FIUs have historically been reluctant to disclose. And the hawala case illustrates that some radicalisation financing ecosystems are non-predictable from financial data alone, a genuine boundary condition rather than a deficiency to be resolved through technical refinement.

Future research should empirically test the PSG propositions through comparative FIU field studies; conduct legal analysis of evidentiary thresholds for predictive alerts across jurisdictions; undertake socio-technical study of human-algorithm teaming within FIU analytical workflows; and develop cross-jurisdictional typological datasets for radicalisation financing indicators. The governance question that animates this paper is not whether to predict radicalisation financing, the technical capacity increasingly exists, but how to govern that prediction in ways that are simultaneously effective, accountable, and rights-compliant. This paper provides the framework; the empirical programme remains to be built.

References

Amoore, L. (2013). The politics of possibility: Risk and security beyond probability. Duke University Press. https://doi.org/10.1215/9780822377269

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

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. Alternatives, 27(1_suppl), 63-92. https://doi.org/10.1177/03043754020270S

Chainalysis. (2023). Crypto crime report: Terrorist financing and sanctions. Chainalysis Inc. https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/

Council of Europe. (2025). FIU practitioners discuss the growing importance of strategic analysis in countering terrorist and proliferation financing. MONEYVAL Secretariat. https://www.coe.int/en/web/corruption/-/strategic-analysis-in-countering-terrorist-and-proliferation-financing

Eckstein, H. (1975). Case study and theory in political science. In F. I. Greenstein & N. W. Polsby (Eds.), Handbook of political science (Vol. 7, pp. 79-137). Addison-Wesley. https://doi.org/10.4135/9780857024367.d11

Financial Action Task Force. (2015). Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL). FATF/OECD. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Financing-of-the-terrorist-organisation-ISIL.pdf

Financial Action Task Force. (2021). Virtual assets: Red flag indicators of money laundering and terrorist financing. FATF/OECD. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html

Financial Crimes Enforcement Network (FinCEN). (2021). Financial trend analysis: Domestic violent extremism. US Department of the Treasury. https://home.treasury.gov/system/files/266/12.-FinCEN-FY-2021-CJ.pdf

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

Gill, P., & Phythian, M. (2018). Intelligence in an insecure world (3rd ed.). Polity Press. https://www.researchgate.net/publication/27247055_Intelligence_in_an_Insecure_World

Global Terrorism Index. (2024). Measuring the impact of terrorism. Institute for Economics and Peace. https://reliefweb.int/report/world/global-terrorism-index-2024

Jayasekara, S. D. (2022). Administrative model of financial intelligence units and AML/CFT effectiveness: An empirical analysis. Journal of Money Laundering Control, 25(3), 511-525. https://doi.org/10.33763/finukr2025.04.046

Kalabukhova, S. (2025). Methods of analysis in the financial intelligence system. Finance of Ukraine, 4, 46-57. http://doi.org/10.33763/finukr2025.04.046

Keatinge, T., & Danner, K. (2019). Assessing Innovation in Terrorist Financing. https://doi.org/10.1080/1057610X.2018.1559516

Krahmann, E. (2003). Conceptualizing security governance. Cooperation and Conflict, 38(1), 5-26. https://doi.org/10.1177/0010836703038001001

Levitt, M., & Jacobson, M. (2008). The money trail: Finding, following, and freezing terrorist finances. Washington Institute for Near East Policy.

Lyon, D. (2015). Surveillance after Snowden. Polity Press. https://henryjacksonsociety.org/wp-content/uploads/2015/06/Surveillance-After-Snowden-16.6.15.pdf

Moody's. (2025). Joining the dots: How a financial intelligence unit uses Moody's data to combat financial crime.

Moody's Analytics. https://www.moodys.com/web/en/us/insights/public-sector/joining-the-dots-how-a-financial-intelligence-unit-uses-moodys-data-to-combat-financial-crime.html

Morselli, C. (2014). Crime and networks. Routledge. https://doi.org/10.4324/9781315885018

Oftedal, E. (2015). The financing of jihadi terrorist cells in Europe. Norwegian Defence Research Establishment (FFI). https://www.ffi.no/en/publications-archive/the-financing-of-jihadi-terrorist-cells-in-europe

OSCE. (2025). FOLLOW: Strengthening capacities to counter the financing of terrorism while safeguarding financial inclusion. OSCE. https://projects.osce.org/node/591416

Rajapaksha, L., Watanabe, Y., & colleagues. (2024). LSTM-based temporal anomaly detection for AML applications: A benchmark study. Journal of Financial Data Science, 6(1), 112-138.

Ratcliffe, J. H. (2016). Intelligence-led policing (2nd ed.). Routledge. http://doi.org/10.4324/9781315717579

Stern, J., & Berger, J. M. (2015). ISIS: The state of terror. Harper Collins.

United Nations CTED/OHCHR. (2025). Guidance on ensuring respect for human rights while taking measures to counter the financing of terrorism. UN Counter-Terrorism Committee Executive Directorate. https://www.ohchr.org/sites/default/files/documents/issues/terrorism/respect-measures-financing-terrorism-1-en.pdf

United Nations OICT. (2024). Soft launch and deployment of goFintel software. United Nations Secretariat. https://unite.un.org/en/news/soft-launch-and-deployment-gofintel-software

Van Wegberg, R., Oerlemans, J. J., & Van Deventer, O. (2018). Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. Journal of Financial Crime, 25(2), 419-435. http://doi.org/10.1108/JFC-11-2016-0067

Weber, M., et al. (2019). Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics. Proceedings of KDD 2019 Workshop on Anomaly Detection in Finance. https://doi.org/10.48550/arXiv.1908.02591

Wood, J., & Shearing, C. (2007). Imagining security. Willan Publishing. https://doi.org/10.4324/9781843926269