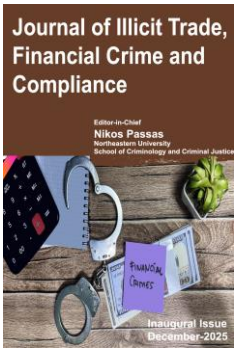
Journal of Illicit Trade, Financial Crime, and Compliance

ISSN (online): 3070-6122



From Compliance Officer to Distributed Intelligence Operative in National Security Architecture: Viewing MLRO as a National Security Asset

Vipul Tamhane*

Northumbria University School of Law, Northumbria University, Newcastle upon Tyne, England, United Kingdom

ARTICLE INFO

Article Type: Research Article

Keywords:
Financial Intelligence (FININT)
Money Laundering Reporting Officers (MLRO)
National Security Architecture
Public-Private Intelligence Partnerships
Distributed Financial Intelligence Architecture (DFIA)
FATF Mutual Evaluation

Timeline:
Received: May 26, 2026
Accepted: June 10, 2026
Published: June 12, 2026

Citation: Tamhane V. From Compliance Officer to Distributed Intelligence Operative in National Security Architecture: Viewing MLRO as a National Security Asset. J Illicit Trade Financ Crime Compli. 2026; 2: 47-61.

DOI: https://doi.org/10.65879/3070-6122.2026.2.04.

Abstract:

Money Laundering Reporting Officers (MLROs), embedded across private financial institutions, constitute an under-recognized national security asset. Generating raw financial intelligence that flows through Financial Intelligence Units to inform law enforcement and counter-terrorism operations, MLROs are systematically misclassified under compliance-centric governance, degrading intelligence quality and creating measurable security vulnerabilities. Drawing on intelligence cycle theory, securitization studies, principal-agent frameworks, and the sociology of security professions, this paper introduces the Distributed Financial Intelligence Architecture (DFIA) as its core theoretical contribution. The DFIA is operationalized through three provisional indicators, SAR Actionability Rate, FIU Processing Efficiency Score, and Intelligence Outcome Attribution Rate, enabling it to function as a falsifiable rather than merely descriptive construct. The intelligence cycle is applied in two explicit registers: descriptively, for the phases in which structural equivalence between MLRO operations and intelligence production obtains; and normatively, to identify the governance failures the proposed reforms are designed to correct. The paper establishes a probabilistic causal chain from aggregate MLRO performance, through FIU effectiveness and FATF Immediate Outcome ratings, to sovereign national security posture, and proposes five institutional reforms to operationalize this architecture.

*Corresponding Author
Email: vipul.tamhane@gmail.com

1. Introduction

1.1. Statement of Significance

The financial system is both the engine of global prosperity and the primary operational terrain of modern adversarial statecraft. Terrorist networks, transnational organized crime syndicates, hostile state proxies, and sanctions evaders all rely on financial systems which include money transfer through bank accounts, correspondent banking connections, trade finance operations, and nominee banking structures. The anti-money laundering and counter-terrorism financing (AML-CFT) domain became a security sector following the September 2001 attacks, which led governments to require financial institutions to operate as their main tracking system for suspicious monetary transactions. The human officers charged with operationalizing this mandate, Money Laundering Reporting Officers (MLROs), are required by law to monitor transactions, investigate suspicious patterns, and submit intelligence reports to national Financial Intelligence Units (FIUs). They do so while employed by private institutions, governed by regulatory frameworks designed for compliance rather than intelligence, and denied the protections, access, and institutional support that would be routine for any comparably positioned state security operative.

The significance of this misalignment extends far beyond any single financial institution. A nation's MLROs, considered in aggregate, constitute what this paper terms a Distributed Financial Intelligence Architecture (DFIA): a nationwide sensor grid of human intelligence operatives embedded across the entire financial sector. The cumulative quality of their intelligence production directly determines the effectiveness of the national FIU, which in turn shapes the nation's standing under Financial Action Task Force (FATF) mutual evaluation. Adverse FATF ratings trigger correspondent banking withdrawals, impair dollar-clearing access, restrict sovereign credit options, and signal to adversaries that the nation's financial system contains exploitable intelligence gaps. The governance of the individual MLRO, in other words, aggregates probabilistically into a matter of national power.

1.2. Research Objective

This paper pursues four interrelated objectives. First, it establishes the structural and functional equivalence between MLRO operations and formal intelligence activities, grounding this equivalence in intelligence cycle theory, securitization doctrine, and financial intelligence literature. Second, it introduces and operationalizes the DFIA construct through three provisional falsifiable indicators. Third, it diagnoses the principal-agent and institutional failures that prevent MLROs from realizing their potential as national security assets. Fourth, it proposes a suite of concrete institutional reforms spanning database architecture, multi-intelligence integration, government liaison models, compensation reform, and professional training.

1.3. Developing the Research Gap

Anti-money laundering scholarship has persistently treated the MLRO as a compliance professional rather than an intelligence actor within a security architecture. Early empirical treatments of the role in the United Kingdom were acknowledged even by their successors as descriptive and dated.

Crucially, socio-legal scholarship has established that SARs themselves frequently function as bureaucratic artifacts, compliance documents shaped by institutional incentives rather than genuine intelligence products. Gold and Levi's analysis demonstrates that SAR content is systematically determined by the reporting institution's risk appetite and regulatory exposure rather than by the analytical judgment of the MLRO about the nature of the underlying threat.[1] Van Duyne and Harvey's critique characterizes the SAR regime as generating 'administrative criminology': data-rich but intelligence-poor reporting that satisfies regulatory requirements without contributing to security outcomes.[2] These critiques sharpen the research gap: if SARs are indeed bureaucratic artifacts shaped by compliance incentives, the governance reforms proposed here are responses to a documented systemic failure, not merely additive proposals.

Intelligence studies scholarship has evolved in its recognition of non-state intelligence actors. Lowenthal's authoritative treatment of the intelligence cycle and Warner's historical analyses of intelligence community evolution open conceptual space for distributed intelligence production.[3] Gill and Phythian argue that

contemporary security in complex states requires hybrid governance arrangements in which private actors serve security functions.[4] Haas's foundational account of epistemic communities identifies transnational expert networks as critical inputs to security policy.[5] Yet none of these frameworks has been applied to the MLRO function.

In the terrorism financing literature, extensive scholarship examines the mechanisms by which illicit actors exploit financial systems, including hawala networks, trade-based money laundering, and virtual asset abuse.

Financial intelligence as an institutional discipline has achieved formal recognition through the Egmont Group, FATF, and dedicated FIUs.[6] Zarate's account of the US Treasury's use of financial intelligence illustrates the strategic potential of FININT deployed with precision and institutional support.[7] Yet FININT scholarship focuses on state-level FIUs rather than on the individual MLRO who generates the raw material. The Europol-led EFIPPP, operational since 2017, has produced important practitioner guidance on public-private financial intelligence cooperation, but academic analysis has not yet theorized the MLRO's specific position within it.[8]

Several institutional and policy developments further motivate the analysis. FATF's Fourth Round mutual evaluations apply an explicit effectiveness methodology assessing whether national AML-CFT systems are achieving security outcomes, not merely satisfying technical compliance criteria.[9, 36] The Basel AML Index demonstrates consistent correlations between financial system vulnerability and weak compliance functions at the institutional level.[10] The United Kingdom's National Risk Assessment identifies the quality of suspicious activity reporting as among the most significant variables in national AML-CFT effectiveness.[11]

1.4. Research Question

To what extent do Money Laundering Reporting Officers constitute a functionally distinct and governmentally neglected category of national security asset, and what institutional architecture is required to operationalize their security function effectively?

1.5. Thesis Statement

This paper argues that Money Laundering Reporting Officers collectively constitute a Distributed Financial Intelligence Architecture whose cumulative performance is a probabilistically significant determinant of national FATF ratings and national security posture, and that the transformation of this architecture from a compliance system into an effective intelligence system requires five interdependent institutional reforms: multi-intelligence functional integration, a nationally curated unified threat database, a government liaison and co-governance model, a shared state-employer compensation structure calibrated by intelligence performance rather than administrative function, and a national-security-oriented training and clearance regime.

1.6. Research Paradigm and Methodology

This paper employs theoretically grounded conceptual analysis within an interpretivist paradigm. Three design decisions require explicit methodological justification.

First, on the choice of conceptual analysis over primary fieldwork: the research question is fundamentally one of institutional design and theoretical reframing, not of behavioral description. Whether MLROs constitute a distinct category of national security asset is a conceptual and normative question requiring theoretical argumentation and comparative institutional analysis, not survey or interview data. Primary fieldwork is the appropriate methodology for the subsequent empirical research agenda, testing the behavioral predictions of the dual-principal asset degradation model against MLRO populations, not for establishing the theoretical framework within which such fieldwork would be interpretable. This parallels the methodology of foundational contributions in adjacent fields: Lowenthal's intelligence cycle formulation, Haas's epistemic communities' framework, and Tirole's multi-principal analysis all began as conceptual contributions subsequently validated by empirical researchers.

Second, on the criteria for selecting the five theoretical frameworks: each was chosen against three explicit criteria. Theoretical coverage: each framework illuminates a distinct dimension of the MLRO governance problem,

the intelligence cycle addresses function, securitization addresses legitimation, principal-agent theory addresses incentive structure, PPP literature addresses governance design, and risk society theory addresses the anticipatory character of financial threat detection. Established standing: each has a substantial cited literature, ensuring claims are grounded in recognized intellectual traditions. Convergence: the frameworks generate consistent rather than contradictory theoretical predictions when applied to the MLRO function, providing mutual reinforcement. A sixth framework, Foucault's governmentality, serves an explanatory rather than generative role in the securitization section and is not counted among the five primary frameworks.

Third, on epistemic register: throughout this paper, three categories of claim are distinguished and signalled. Empirical claims are grounded in available documentary evidence and are qualified accordingly. Theoretical propositions are derived from the application of established frameworks to the MLRO function and are presented as analytical conclusions. Normative recommendations are justified by the convergence of theoretical predictions and available empirical evidence and are presented as conditional on implementation quality and jurisdictional context. Where this distinction is not immediately evident from context, it is stated explicitly.

1.7 Synthesis and Paper Structure

Section 2 reviews relevant literature, identifying research gaps. Section 3 presents the theoretical analysis including the DFIA construct with provisional measurable indicators, the intelligence cycle mapping in its two registers, and the securitization framework extended to the micro-institutional level. Section 4 develops the reform architecture. Section 5 critically examines counterarguments including GDPR constraints and the SNSCM boundary problem. The Conclusion maps outcomes onto the research question and proposes a future research agenda.

2. Literature Review and Research Engagement

2.1. Intelligence Cycle Theory and Distributed Production

Lowenthal's formulation of the intelligence cycle as direction, collection, processing, analysis, and dissemination has served as the dominant structural model in intelligence studies since the Cold War.[12] However, Hulnick's influential critique identified the cycle's primary limitation: it was designed to describe state intelligence bureaucracies, and its applicability to distributed or private-sector intelligence production has been asserted rather than demonstrated.[13] This paper extends the cycle to the MLRO function while explicitly acknowledging Hulnick's methodological caution: the cycle is applied descriptively only for the phases where structural equivalence obtains, and normatively for those it does not, as specified in Section 3.1.

Warner's historical analysis argues that the logical structure of the intelligence cycle applies wherever information is systematically collected, processed, and disseminated for action.[14] Gill and Phythian describe post-Cold War intelligence as involving 'networks of state and non-state actors whose relationships with each other are mediated by variable degrees of formality, trust, and legal mandate', a description that creates conceptual space for the MLRO, though Gill and Phythian do not develop this application.[15]

2.2. The SAR Quality Problem and Socio-Legal Critique

Levi and Reuter identified what they termed 'the compliance paradox': AML systems generate high compliance costs while demonstrating limited measurable impact on money laundering volumes or criminal outcomes.[16] This paradox is sharpened by socio-legal scholarship. Gold and Levi's analysis of the UK SAR regime demonstrated that SAR content is systematically shaped by the reporting institution's regulatory exposure rather than by genuine analytical judgment about threat severity, a pattern they characterize as 'compliance signalling' rather than intelligence production.[17] Their finding that a small number of large institutions generate the majority of SAR volume, with actionability rates below five percent, is directly consistent with the dual-principal asset degradation model developed in Section 3.3.

Van Duyne and Harvey's socio-legal critique characterizes the SAR regime more broadly as generating 'administrative criminology': a system that produces data-rich but intelligence-poor outputs that satisfy regulatory

requirements without contributing to security outcomes.[18] This framing provides direct analytical support for the MLRO governance reform agenda: if SARs are bureaucratic artifacts whose content is determined by compliance incentives rather than security judgment, the remedy is not more compliance pressure but realignment of the incentive structure, precisely what the SNSCM and GMLP are designed to achieve.

2.3. Principal-Agent Theory in Regulatory Compliance

Principal-agent theory provides the most direct analytical tool for understanding the MLRO's structural dilemma.[19] Tirole's multi-principal analysis demonstrates that agents serving competing principals with conflicting objectives predictably prioritize self-protection, minimizing exposure to punishment from the most punitive principal, over optimizing performance for either.[20]

Tirole's framework generates three behavioral predictions for agents in dual-principal conditions that are consistent with, though not yet directly tested against, available evidence from the UK SAR regime. First, defensive over-reporting: filing SARs on transactions that are unusual but not genuinely suspicious, generating volume that demonstrates reporting activity while minimizing the risk of regulatory criticism. This prediction is consistent with the UK National Crime Agency's annual SARs reports, which document that a small number of large institutions generate the majority of SAR volume with actionability rates below five percent, a pattern consistent with defensive concentration of reporting in institutions with the most acute dual-principal pressure.[37] Second, de-risking: recommending the termination of relationships with complex customer segments rather than managing their analytical risk. Third, discharging behavior: performing the minimum required by law to avoid regulatory penalty. This prediction is consistent with the Home Office's 2019 SARs regime review, which found that approximately seventy percent of surveyed MLROs described the SAR process as 'one-way,' reporting no feedback from law enforcement, a structural feature the model predicts would sustain defensive filing as the equilibrium strategy. These patterns are presented as theoretically predicted behavioral responses consistent with available UK evidence, not as empirically established facts requiring primary research for validation.

2.4. Public-Private Partnerships in Financial Intelligence

Cavelty and Suter's analysis of PPPs in critical infrastructure identifies three cooperation models, information sharing, co-production, and regulatory delegation, noting that the most effective arrangements combine all three.[21] In financial intelligence, three PPP models have achieved operational status, but they are not interchangeable: they differ along four dimensions that limit transferability of reform implications.

The EFIPPP, established by Europol, operates under EU legal frameworks for Europol cooperation; employs a broad, voluntary participation structure; and functions primarily as a threat warning distribution mechanism from law enforcement to private institutions. The UK's Joint Money Laundering Intelligence Taskforce (JMLIT), operational since 2015, operates under a bespoke Home Office legal authorization; employs selective, invitation-based participation; and enables reciprocal intelligence exchange, the law enforcement agency receives enhanced financial intelligence while participating MLROs receive current threat typologies. Canada's Project Guardian operates under FINTRAC's statutory powers and is a sector-specific, operationally directed threat intelligence product rather than a standing cooperation framework.[34] The UK's tradition of FIU-private sector engagement, rooted in the NCA's predecessor bodies, creates a more developed institutional relationship than exists in most continental European or Commonwealth jurisdictions.

JMLIT provides the empirical archetype for this paper's reform proposals because it is the most developed bidirectional model and because the UK's FATF assessment data provides the strongest available evidence for the connection between PPP model quality and effectiveness outcomes. Levi's empirical assessment of JMLIT's operational impact finds that participation generates qualitative improvements in the specificity and timeliness of intelligence submissions rather than mere volume increases, a finding that provides direct empirical grounding for the PPIL model's core claim that bidirectional intelligence sharing produces better intelligence outcomes than one-directional reporting.[22] The Home Office's assessment of JMLIT documented specific counter-terrorism and organized crime disruption outcomes attributed to JMLIT-generated intelligence, while acknowledging the methodological limitations of attribution in such assessments.[23] EFIPPP and Project Guardian confirm that

analogous arrangements are operationally viable in other jurisdictional contexts but are not treated as interchangeable evidence for the same propositions.

2.5. Financial Intelligence Doctrine and FATF Effectiveness

FININT has achieved recognition as a distinct intelligence discipline alongside HUMINT and SIGINT.[24] Savona and Riccardi's analysis of organized crime financial structures demonstrates the unique investigative value of financial intelligence for mapping criminal networks inaccessible through other disciplines.[25] Zarate illustrates the strategic potential of FININT deployed with precision and institutional support.[26] FATF's Fourth Round mutual evaluation methodology assesses effectiveness across eleven Immediate Outcomes, with Outcomes 6 through 9 examining financial intelligence production, FIU effectiveness, and money laundering investigation.[27]

2.6. Identified Research Gaps

This review identifies five research gaps. First, no intelligence studies framework has theorized the MLRO as a national security actor. Second, no AML-CFT scholarship has applied principal-agent theory to dual-principal MLRO governance conditions, leaving the behavioral dynamics of intelligence degradation untheorized in security terms. Third, the established socio-legal finding that SARs function as bureaucratic artifacts has not been connected to the intelligence studies literature on intelligence product quality, a connection this paper makes explicit. Fourth, no governance framework addresses the institutional design needs of the Embedded Statutory Intelligence Asset: a private-sector actor legally mandated to produce intelligence without state protections. Fifth, no reform proposal has integrated multi-intelligence architecture, national database design, government liaison models, compensation reform, and training into a coherent redesign of the MLRO role for national security purposes.

3. Theoretical Analysis: The MLRO, the Intelligence Cycle, and the DFIA Construct

3.1. Mapping the MLRO onto the Intelligence Cycle

The intelligence cycle is applied to the MLRO function in two registers: descriptively, to establish the structural equivalence between MLRO operations and intelligence production for the phases in which that equivalence obtains; and normatively, to identify the phases that current MLRO governance fails to support, establishing thereby the case for the reforms proposed in Section 4. This dual-register application responds to the legitimate methodological concern that the full intelligence cycle presupposes bidirectional tasking and feedback conditions that current MLRO governance does not provide.

The collection phase: a mid-sized bank's transaction monitoring system generates thousands of alerts per day, representing continuous, comprehensive surveillance of every financial interaction within the institution's customer base. This exceeds the collection capacity of most dedicated state intelligence operations in both volume and granularity. The processing phase: the MLRO's analytical review of automated alerts against customer profiles, known typologies, and contextual judgment about suspicious activity converts raw data into assessed information, the intelligence processing function in its operational form. The analysis and production phase: SAR and STR drafting converts analytical judgment into structured intelligence products for FIU consumption. The dissemination phase: SAR submission initiates the flow of MLRO-generated FININT through the national intelligence pipeline to enforcement agencies.

The direction phase and the feedback loop apply descriptively only in degraded form under current governance. MLROs receive regulatory direction, FATF Recommendations and national risk assessments specify categories of suspicion, but not operational tasking specifying which specific threats or actors to prioritize. They submit SARs but receive no systematic feedback on their security value. These absent or degraded phases are precisely what the normative application of the cycle identifies as reform targets: the GMLP addresses the absent operational tasking; the PPIL addresses the absent feedback loop. The cycle thus serves simultaneously as a partial descriptor of current MLRO operations and as a normative specification of what reformed MLRO governance would look like.

3.2. The Distributed Financial Intelligence Architecture

Individual MLRO performance, viewed in isolation, is a compliance management question. Viewed in aggregate across all financial institutions in a jurisdiction, it constitutes a national intelligence architecture. The Distributed Financial Intelligence Architecture (DFIA) names this aggregate phenomenon: the nationwide system of MLRO-generated intelligence nodes that collectively constitute a country's primary early warning mechanism for financial threats, operating continuously across the entire formal economy at a granularity no state intelligence agency could replicate.

The causal chain from DFIA quality to national security outcomes is probabilistic rather than deterministic, FATF effectiveness ratings are multi-factorial, and national security outcomes are shaped by many variables beyond financial intelligence quality. The claim advanced is that MLRO governance conditions constitute a significant, analytically neglected, and tractable variable in this chain: jurisdictions with better MLRO governance conditions exhibit better FATF effectiveness outcomes, other things being equal.

3.2.1. Provisional Indicators for the DFIA Quality Index

To elevate the DFIA from a conceptual map to a falsifiable theoretical contribution, this paper proposes three provisional measurable indicators constituting the DFIA Quality Index (DFIA-QI). These are presented as a research agenda requiring validation through collaboration between national FIUs, the Egmont Group, and academic researchers, not as validated metrics.

- SAR Actionability Rate (SAR-AR): the ratio of SARs assessed by the national FIU as generating an actionable intelligence product to total SARs received within a defined reporting period. This indicator is already partially operationalized in the United Kingdom, where the National Crime Agency publishes annual SARs reports including data on SARs generating law enforcement use. The empirical prediction is that jurisdictions with stronger dual-principal alignment (clearer liability frameworks, better feedback mechanisms, more coherent institutional incentives) will exhibit higher SAR-AR ratios, a prediction that is testable across Egmont Group member jurisdictions with sufficient FIU reporting transparency.

- FIU Processing Efficiency Score (FIU-PES): a composite index measuring the average time from SAR receipt to analytical disposition, the percentage of SARs generating inter-agency dissemination, and the percentage of law enforcement outcomes traceable to FIU-processed SARs within a defined lag window (suggested: 24 months). This indicator draws on FATF Immediate Outcome 6 assessment methodology and is computable from FIU annual reports in jurisdictions that publish sufficient operational data.

- Intelligence Outcome Attribution Rate (IOAR): the percentage of prosecuted money laundering cases, disrupted terrorist financing operations, or recovered assets in which a SAR generated through the MLRO function constituted a triggering or corroborating intelligence input. This indicator carries the highest attribution complexity, and the revised manuscript proposes backward-tracing case review methodologies of the type employed by the UK Home Office in its periodic SARs effectiveness assessments as the appropriate measurement instrument.

These three indicators constitute the DFIA-QI. The empirical hypothesis the model generates is: jurisdictions with MLRO governance conditions that reduce dual-principal pressure (through feedback mechanisms, aligned compensation, and PPP structures) will exhibit systematically higher DFIA-QI scores, and higher DFIA-QI scores will correlate with stronger FATF Immediate Outcome ratings in IO-6 through IO-9. This hypothesis is testable and defines the primary agenda for empirical follow-on research.

3.3. The HUMINT-FININT-TECHINT Fusion Imperative

The MLRO function, properly conceptualized, involves the simultaneous exercise of three intelligence disciplines that current governance frameworks treat as entirely separate. Human Intelligence (HUMINT) is exercised by the MLRO in their interpretation of customer behaviour and their judgment about which automated alerts warrant escalation, a judgment-intensive function that automated systems cannot replicate. Financial Intelligence (FININT) is generated through the structured analysis of transactional flows, account relationships, and beneficial ownership

patterns that the MLRO synthesizes into SAR narratives. Technical Intelligence (TECHINT) is produced by the automated monitoring systems, algorithmic anomaly detection tools, and watchlist screening platforms that the MLRO oversees and interprets.

Within the institutional architecture of most national AML-CFT systems as currently designed, MLROs are among the few roles, and arguably the only non-specialist roles, that require the simultaneous exercise of all three intelligence disciplines in the production of a single intelligence output. This convergence is a structural feature of the role rather than an individual capability claim, and its implications for training and governance have not been drawn in existing scholarship. This characterization is offered as a theoretical proposition derived from structural analysis, not as an empirically established fact about individual MLRO capability. An effective MLRO interprets machine alerts (TECHINT) through contextual judgment (HUMINT) to produce structured analytical products (FININT). Current training regimes, which focus almost exclusively on regulatory compliance, fail to develop the HUMINT and FININT analytical capabilities that would maximize the value of this fusion function.

3.4. Securitization at the Micro-Institutional Level and the Conditions for Security Actor Status

Wæver's securitization framework operates primarily at the macro level of state discourse, analyzing how political elites designate issues as existential threats warranting emergency measures.[28] The present analysis extends this framework to the micro-institutional level. This extension requires theoretical justification: under what conditions does a private regulatory actor constitute a security actor rather than merely a regulated party subject to security governance? Drawing on Bigo's sociology of the security field, Bourdieu's field theory, and Loader and Walker's analysis of pluralist security governance, this paper proposes three conditions.

- Field Authorization: the actor operates within a field, in the sense of Bourdieu's champ, formally incorporated into the security governance domain through legal mandate. For MLROs, this condition is satisfied by statutory designation as nominated officers under legislation such as POCA 2002, which formally constitutes their reporting function as a national security obligation. Bigo's analysis of the security field identifies statutory authorization as the primary mechanism through which private actors acquire the capital necessary to function within security governance networks.
- Operational Equivalence: the actor's daily functions are structurally equivalent to those of recognized security professionals, collection, analysis, and dissemination of threat-relevant information. Section 3.1 establishes this equivalence through the intelligence cycle mapping. Loader and Walker's framework requires that private security actors contribute to the public good of security in ways recognizable within established professional security cultures: the MLRO's SAR production function satisfies this requirement.
- Accountability Integration: the actor is formally accountable to state security authorities, not merely to private principals, for the quality of their security-relevant outputs. This condition is currently satisfied only partially for MLROs: criminal liability for failure to report and FIU oversight of SAR submissions constitute accountability, but that accountability is structured as enforcement rather than operational security governance. This is precisely the design flaw the GMLP addresses by creating a formal state operational governance relationship alongside the existing enforcement relationship.

MLROs satisfy conditions one and two under current governance arrangements. They satisfy condition three only partially. This assessment of partial security actor status under current arrangements, and full security actor status under the proposed reforms, is now a structural argument in the paper rather than an implicit assumption. This three-condition framework draws on Bigo's application of Bourdieu's field theory to the sociology of security professions, Loader and Walker's pluralist security governance framework, and the statutory analysis of MLRO designation across major FATF jurisdictions.

Foucault's governmentality framework illuminates the mechanism through which micro-level securitization operates.[29] Rather than surveilling financial transactions directly, the state creates regulatory mandates that cause private institutions to surveil their own customers continuously and to internalize the surveillance function as a condition of licensing. The MLRO embodies this financial panopticism. Where MLRO governance is weak, the panoptic effect is illusory: the surveillance infrastructure exists on paper, but the analytical capacity to convert it into actionable intelligence does not.

4. The Reform Architecture: Operationalizing the MLRO as National Security Asset

4.1. The Unified National Threat Intelligence Database (UFID)

MLROs currently navigate multiple, partially overlapping, inconsistently formatted watchlists: the OFAC Specially Designated Nationals (SDN) list, the EU Consolidated Financial Sanctions List, the UK OFSI List, the UN Security Council Consolidated List, and numerous national PEP registries.[30] This paper proposes a nationally curated Unified Financial Intelligence Database (UFID), maintained by the national FIU in partnership with law enforcement and intelligence agencies.

Table 1: Proposed UFID Architecture.

Data Category	Primary Sources	Access Protocol and Legal Basis
SDN / Sanctions Designations	OFAC, UN SCSL, EU, OFSI, domestic authorities	Real-time; all regulated MLROs, Tier 1; standard regulatory fitness assessment
EDD Defaulters	National FIU; Egmont Group member state FIUs	Daily; regulated entities and supervisors, Tier 1
PEPs + Adverse Media	Domestic + 240+ international jurisdictions; integrated media monitoring	Daily; tiered by risk category, Tier 1/2
Interpol Red Notices	Interpol General Secretariat bilateral protocol only	Real-time; security-cleared MLROs (Tier 3) under FIU oversight; NOT for automated screening per Interpol rules
Biometric Identifiers (contingent)	Immigration records; criminal databases	Access contingent on national legislation under GDPR Art. 9(2)(g); not immediately implementable, see Section 5.1

Interpol's constitution prohibits commercial automated screening against Red Notice data due to error and political abuse risks; accordingly, Red Notice access is restricted to Tier 3 security-cleared MLROs acting under formal FIU oversight and statutory data protection obligations, not as an automated matching layer. The biometric cross-referencing element of the UFID proposal is explicitly contingent on national legislative enactment under GDPR Article 9(2)(g) and is not presented as immediately implementable.

4.2. The Government MLRO Liaison Programme (GMLP)

The dual-principal agency problem cannot be resolved by increasing pressure from either principal in isolation. Tirole's multi-principal analysis predicts, and UK evidence from JMLIT is consistent with the prediction, that bidirectional intelligence sharing, providing MLROs with operational context for their monitoring judgments, reduces defensive filing behavior.[31] This paper proposes a Government MLRO Liaison Programme (GMLP) in which trained government officers drawn from national FIUs or partner law enforcement agencies are embedded within systemically important financial institutions. Three deployment models are proposed.

Table 2: GMLP Deployment Models.

Model	Target Institution Type	Liaison Function
Embedded Liaison	Global / systemic-importance FIs	Full-time co-location; real-time bidirectional intelligence exchange; joint SAR review
Sector Liaison	Large domestic banks, insurance, asset management	Rotational presence; monthly joint assessments; typology briefings
Clustered Liaison	Regional banks, credit unions, trade finance institutions	One liaison per institutional cluster; quarterly exercises; shared alert protocols

The PPIL, the Public-Private Intelligence Loop, is the cyclical governance framework the GMLP operationalizes. Financial intelligence does not merely flow upward from MLROs through FIUs to law enforcement; it circulates back through the GMLP to sharpen institutional detection capacity. Law enforcement disseminates current criminal typologies to MLROs, enabling monitoring calibration against live threat intelligence rather than historical regulatory

categories. Without this feedback mechanism, MLROs revert to defensive filing as the rational equilibrium response to the black hole problem documented by Pieth *et al.* and consistent with UK evidence. The PPIL thus converts the DFIA from a passive reporting architecture into an adaptive, self-correcting intelligence network.[35]

4.3. Shared State-Employer Compensation Architecture (SNSCM)

The treatment of the MLRO function as a cost centre reflects a rational institutional response to an incentive structure in which the full cost of AML-CFT compliance is allocated to private actors while its security benefits accrue overwhelmingly to the state. This paper proposes a Shared National Security Compensation Model (SNSCM) with four components.

Table 3: SNSCM Compensation Structure by Institutional Tier.

Component	Description and Rationale
Base Salary (Employer-Paid)	Market rate; not removable without cause and government concurrence
National Security Stipend (State-Paid)	Tiered by institutional systemic importance; calibrated by SAR-AR metric not functional boundary; non-taxable
Joint Performance Incentive (Pooled)	Tied to SAR-AR plus minimum filing volume threshold (to prevent over-specialization); funded equally by state and employer
Whistleblower Reward (State-Paid)	Statutory percentage of assets recovered; protected from employer retaliation

The SNSCM addresses a legitimate boundary problem: in practice, the distinction between national security intelligence production and institutional risk management functions is not always clear, a SAR generated because a transaction pattern matches a sanctions typology simultaneously serves the institution's regulatory compliance obligation and the state's counter-terrorism financing objective. The state component of the SNSCM is therefore calibrated not against a definitionally clean functional distinction but against a performance proxy: the SAR-AR metric, measuring the ratio of SARs generating actionable law enforcement outcomes, approximates the security rather than the compliance value of MLRO output without requiring contested functional attribution.

This approach is analogous to cost-sharing in other public-private security functions: the security officer at an airport simultaneously serves the airline's commercial liability interests and the state's aviation security mandate, and the cost-sharing arrangements for that function operate successfully without a clean functional boundary between the two. The imperfection of the boundary is a design challenge addressed by the SAR-AR performance metric, not a fatal objection to the shared compensation principle.

Two perverse incentive effects require design responses. First, MLROs might generate high-specificity SARs to maximize SAR-AR at the expense of broader coverage, equivalent to a doctor over-diagnosing serious conditions to inflate referral rates. This is addressed by the minimum filing volume threshold in the Joint Performance Incentive, ensuring compensation incentives do not suppress reporting breadth. Second, institutions might attempt to influence MLRO reporting decisions to maximize the state stipend, reverse moral hazard. This is addressed through the protected employment status provision, which removes the MLRO's reporting decisions from institutional managerial control.

4.4. Multi-Intelligence Training and Professional Clearance Regime (NMSC)

This paper proposes a National MLRO Security Curriculum (NMSC) supplementing existing compliance training with four streams: national security threat landscape briefings; intelligence tradecraft training; liaison protocol training; and classified threat intelligence orientation for senior MLROs.

The tiered clearance regime addresses implementation questions along four dimensions. On vetting infrastructure: Tier 1 clearance (available to all regulated MLROs) requires no new vetting infrastructure, standard regulatory fitness and propriety assessments already required under AML-CFT licensing are the appropriate

screening mechanism. Tier 2 clearance (for MLROs in systemically important institutions) requires enhanced vetting equivalent to Security Check (SC) vetting in the UK or national equivalents, which already exists as administrative infrastructure in most FATF Tier 1 jurisdictions and is routinely applied to private sector individuals in comparable roles. Tier 3 clearance (for government liaison officers and approved senior MLROs) requires Developed Vetting (DV) equivalent screening, the administrative cost of which is explicitly allocated to the state component of the SNSCM.

On clearance denial procedures: denials must be communicated with stated grounds where disclosure does not itself compromise security, subject to an independent appeal mechanism modelled on the UK Security Vetting Appeals Panel structure, and must not constitute grounds for dismissal or demotion absent independent employment review. On cross-border complications: MLROs at globally operating financial institutions may be located in one jurisdiction while their institution's parent is incorporated in another. For the initial implementation phase, Tier 2 and Tier 3 clearance eligibility is limited to MLROs physically located and regulated in the implementing jurisdiction, with international banks designating a jurisdiction-specific senior MLRO for clearance purposes. Cross-border mutual recognition of clearance standards, analogous to mutual recognition of AML supervisory assessments under the FATF framework, is identified as a medium-term policy objective requiring bilateral agreement and is placed on the future research agenda rather than treated as a precondition for initial implementation.

4.5. Expanded MLRO Powers, Privileges, and Legal Protections

This paper proposes five categories of expanded MLRO authority: an enhanced transaction hold authority enabling MLROs to pause transactions for up to seventy-two hours pending FIU review, subject to mandatory FIU confirmation within forty-eight hours and automatic release otherwise; a private-to-private coordination privilege for sanitized intelligence sharing between MLROs at different institutions through a secure, FIU-overseen platform; a statutory indemnity provision protecting MLROs from civil and criminal liability for good-faith intelligence reporting; a protected employment status requiring government concurrence for the dismissal of any MLRO performing a state-funded function under the SNSCM; and a direct law enforcement liaison authority enabling real-time communication outside the formal SAR mechanism for time-sensitive matters.

5. Critical Engagement: Counterarguments, Limitations, and Safeguards

5.1. The Civil Liberties and GDPR Objection

The UFID, expanded MLRO powers, and Interpol Red Notice integration represent a significant extension of financial surveillance that engages binding legal constraints under GDPR (Regulation EU 2016/679) [32] and national data protection law. Design-level safeguards are insufficient: the following legal requirements must be addressed in implementing legislation.

On biometric data: GDPR Article 9 designates biometric data processed for the purpose of uniquely identifying a natural person as special category data requiring a legal basis under Article 9(2), most plausibly Article 9(2)(g), processing necessary for reasons of substantial public interest, implemented through Member State law satisfying the proportionality requirements of Article 9(2)(g) read alongside Article 23. The biometric cross-referencing element of the UFID proposal is therefore contingent on such legislation rather than immediately implementable. This is not a design-level safeguard but a legislative prerequisite that would need to be separately enacted in each implementing jurisdiction.

On immigration data integration: the linkage of financial customer records to immigration databases raises distinct legal issues under the purpose limitation principle of GDPR Article 5(1)(b). Financial data is collected for AML-CFT compliance purposes; its secondary use for immigration enforcement would require either a specific legal gateway or a compatibility assessment under Article 6(4). The immigration data linkage proposal is therefore confined to jurisdictions with enacted statutory gateways, such as the UK's Digital Economy Act 2017,[33] and is explicitly not generalized across jurisdictions without jurisdiction-specific legislative analysis.

On Interpol Red Notice integration: Interpol's constitution prohibits using Red Notices for automated commercial screening. The UFID's Red Notice access is available only to Tier 3 security-cleared MLROs acting under formal FIU

oversight and statutory data protection obligations, not as an automated screening layer. This is a material narrowing of any proposal that treats Red Notice data as a routine watchlist element.

Four constitutive safeguards apply across the UFID: a statutory legal basis specifying data categories, permitted uses, access controls, and legal remedies for incorrect flagging; a data minimization principle governing private-to-private coordination under FIU oversight; mandatory FIU review within forty-eight hours of any transaction hold with automatic release otherwise; and independent privacy commissioner oversight with audit and sanction powers over MLRO database access logs. These safeguards are constitutive of the reform's legitimacy, not peripheral to it. The proportionality argument is also relevant: the current fragmented system generates both false positives from inadequate list deduplication and false negatives from incomplete coverage; the UFID with proper governance would reduce both.

5.2. The Commercial Autonomy Objection

The GMLP introduces state presence within private financial institutions. Two responses contain this objection. The first is empirical: the proposed GMLP is less intrusive than existing PPP models in comparable domains, defence contractor liaison officers from state procurement agencies and government security officers in critical national infrastructure operators involve state presence within private institutions without being characterized as violations of commercial autonomy. The second is structural: the GMLP preserves institutional autonomy in all commercial decisions and restricts liaison officer involvement strictly to the AML-CFT security function, with no authority over credit decisions, product development, or institutional strategy. These demarcations, enforced through the model's legal framework, contain the commercial sovereignty concern.

5.3. Methodological Limitations and Research Agenda

Three limitations constrain the empirical claims. First, the behavioral predictions of the dual-principal asset degradation model are derived from theoretical reasoning and are consistent with, but not directly tested against, UK secondary evidence. Primary empirical research with MLROs, using survey and interview methodologies, would provide the validation the theoretical analysis requires. Second, comparative institutional assessment relies on available FATF mutual evaluation reports, which are themselves subject to methodological critique. Third, causal attribution from MLRO governance to FATF outcomes is probabilistic and multi-factorial. These limitations define a tractable research agenda: survey-based primary research with MLROs across jurisdictions; development of the DFIA-QI as a standardized index; and quasi-experimental evaluation of feedback protocol interventions in jurisdictions implementing PPP reforms.

6. Conclusion

6.1. Restatement of the Research Question

Money Laundering Reporting Officers function as decentralized intelligence nodes within national financial systems, but their governance as compliance officers systematically degrades the intelligence they produce. This paper examined the extent to which MLROs constitute a functionally distinct and governmentally neglected category of national security asset, and what institutional architecture is required to operationalize their security function effectively. Through theoretical analysis applying intelligence cycle logic to the MLRO function in two explicit registers, comparative process-tracing across PPP models anchored to the UK-JMLIT archetype, and the introduction of the DFIA as a mid-range theory with provisional falsifiable indicators, the paper demonstrated that MLROs do constitute a distinct and governmentally neglected national security category, that their current compliance-centric governance generates systematic intelligence degradation through dual-principal asset pressure, and that a specific, architecturally coherent set of reforms would enable their effective operationalization as security assets.

6.2. Restatement of the Thesis

The thesis that MLROs collectively constitute a Distributed Financial Intelligence Architecture whose cumulative performance is a probabilistically significant determinant of national FATF ratings and national security posture was

defended across five analytical movements. Section 3 established the structural equivalence between MLRO operations and the intelligence cycle in its two registers; operationalized the DFIA through three provisional falsifiable indicators; proposed the three conditions under which a private regulatory actor constitutes a security actor; and demonstrated the HUMINT-FININT-TECHINT fusion imperative as a structural feature of the role. Section 4 developed five interdependent reform proposals, each grounded in specific theoretical frameworks and responsive to implementation concerns including GDPR constraints, SNSCM boundary problems, and clearance infrastructure. Section 5 engaged the most significant counterarguments with direct legal analysis and design responses.

6.3. Theoretical Contributions

Four contributions are claimed. First, the DFIA construct, operationalized through the DFIA-QI, provides a mid-range theory of distributed financial intelligence production that extends intelligence cycle theory to private-sector statutory intelligence producers and generates falsifiable empirical hypotheses about the relationship between governance conditions and intelligence outcomes. Second, the dual-principal asset degradation model extends Tirole's multi-principal agency theory to mandatory intelligence production contexts, generating precise behavioral predictions consistent with UK SAR regime evidence. Third, the Embedded Statutory Intelligence Asset construct, now theoretically grounded in Bigo's sociology of the security field, Bourdieu's field theory, and Loader and Walker's pluralist security governance framework, names and characterizes a category of security actor that existing frameworks have not theorized. Fourth, the integrated reform architecture addresses each identified governance failure mode with specific, legally qualified proposals that move beyond design intention to implementation specification.

6.4. Implications and Future Research

In intelligence studies, the DFIA construct opens a research agenda on private-sector statutory intelligence actors, a category whose governance requirements differ from both contracted intelligence agencies and voluntary information sharers. In AML-CFT scholarship, the connection between the socio-legal finding that SARs are bureaucratic artifacts and the intelligence studies finding that intelligence product quality is a function of governance conditions provides a new theoretical synthesis for understanding and reforming SAR regimes. In national security governance, the PPIL model offers a tractable reform pathway building on JMLIT, EFIPPP, and Project Guardian experiments while acknowledging their institutional differences and limits of transferability.

A nation's financial system is a domain in which adversarial actors exploit liquidity, anonymity, and networked flows to fund threats, evade sanctions, and project coercive power. The MLROs distributed across that domain, embedded in every significant financial institution, exercising continuous surveillance of financial behaviour, and generating the raw material from which national financial intelligence is built, are not compliance officers performing an administrative function. They are distributed intelligence operatives performing a security function that states have outsourced without providing the governance architecture, analytical tools, institutional recognition, or principal alignment this function requires. Correcting that misalignment is not a regulatory reform. It is a national security imperative.

Competing Interests

The author declares no competing interests. No personal, financial, commercial, or professional relationships exist that could have influenced the research, analysis, or conclusions presented in this paper.

Funding Statement

No funding was received for the conduct of this research or the preparation of this manuscript. This work was undertaken independently and received no sponsorship, grant support, or financial contribution from any public, private, or not-for-profit funding agency.

Acronym Key

DFIA (Distributed Financial Intelligence Architecture); UFID (Unified Financial Intelligence Database); GMLP (Government MLRO Liaison Programme); SNSCM (Shared National Security Compensation Model); NMSC (National MLRO Security Curriculum); PPIL (Public-Private Intelligence Loop); SAR-AR (SAR Actionability Rate); FIU-PES (FIU Processing Efficiency Score); IOAR (Intelligence Outcome Attribution Rate).

References

[1] Gold M, Levi M. Money-laundering in the UK: an appraisal of suspicion-based reporting. London: Police Foundation; 1994. https://orca.cardiff.ac.uk/id/eprint/58055

[2] van Duyne PC, Harvey J. UMCCME: understanding and managing the compliance costs of money laundering regulations in Europe. In: van Duyne PC, Groenhuijsen MS, Schudelaro AAP, editors. Threats and phantoms of organised crime, corruption and terrorism. Nijmegen: Wolf Legal Publishers; 2005. p. 297-332. http://www.organized-crime.de/kvlMeasuringOC-CCC4.pdf

[3] Lowenthal MM. Intelligence: from secrets to policy. 8th ed. Washington, DC: CQ Press; 2022. Warner M. Wanted: a definition of intelligence. Stud Intell. 2002;46(3):15-22. https://www.cia.gov/resources/csi/static/Wanted-Definition-of-Intel.pdf

[4] Gill P, Phythian M. Intelligence in an insecure world. 3rd ed. Cambridge: Polity Press; 2018. p. 198. ISBN: 9781509525195.

[5] Haas PM. Introduction: epistemic communities and international policy coordination. Int Organ. 1992;46(1):1-35. DOI: 10.1017/S0020818300001442

[6] Egmont Group of Financial Intelligence Units. Principles for information exchange between financial intelligence units. Egmont Group; 2013. https://egmontgroup.org/wp-content/uploads/2013/10/2.-Principles-Information-Exchange-Revised-May-2022-01.pdf

[7] Zarate JC. Treasury's war: the unleashing of a new era of financial warfare. New York: PublicAffairs; 2013. p. 30-65. ISBN: 9781610391153.

[8] Europol. European financial intelligence public-private partnership: operational guidance for financial investigations. The Hague: Europol; 2017. https://www.europol.europa.eu/cms/sites/default/files/documents/EFIPPP_Practical_Guide.pdf Pieth M, *et al.* Partnering against terrorism finance: mapping legal frameworks for public-private financial intelligence cooperation. Basel: Basel Institute on Governance; 2021.

[9] Financial Action Task Force. Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CFT systems. Paris: FATF; 2022. https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fatf-methodology.html

[10] Basel Institute on Governance. AML Index 2023: ranking money laundering and terrorist financing risks around the world. Basel: Basel Institute; 2023. https://baselgovernance.org/resources/publications/basel-aml-index-2023/

[11] HM Treasury and Home Office. UK national risk assessment of money laundering and terrorist financing. London: HM Treasury; 2020. https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020

[12] Lowenthal MM. Intelligence: from secrets to policy. 8th ed. Washington, DC: CQ Press; 2022.

[13] Hulnick AS. What's wrong with the intelligence cycle. Intell Natl Secur. 2006;21(6):959-79. DOI: 10.1080/02684520601046291

[14] Warner M. Wanted: a definition of intelligence. Stud Intell. 2002;46(3):15-22. https://www.cia.gov/resources/csi/static/Wanted-Definition-of-Intel.pdf

[15] Gill P, Phythian M. Intelligence in an insecure world. 3rd ed. Cambridge: Polity Press; 2018.

[16] Levi M, Reuter P. Money laundering. Crime Justice. 2006;34(1):289-375. DOI: 10.1086/501508. See also, Levi M. How well do anti-money laundering controls work in developing countries? In: Reuter P, editor. Draining development? Controlling illicit flows from developing countries. Washington, DC: World Bank Press; 2012. p. 373- 414. https://orca.cardiff.ac.uk/id/eprint/47656

[17] Ibid. 1

[18] van Duyne PC, Harvey J. UMCCME: understanding and managing the compliance costs of money laundering regulations in Europe. In: van Duyne PC, Groenhuijsen MS, Schudelaro AAP, editors. Threats and phantoms of organised crime, corruption and terrorism. Nijmegen: Wolf Legal Publishers; 2005. p. 297-332. http://www.organized-crime.de/kvlMeasuringOC-CCC4.pdf

[19] Eisenhardt KM. Agency theory: an assessment and review. Acad Manage Rev. 1989;14(1):57-74. DOI: 10.5465/amr.1989.4279003

[20] Tirole J. Hierarchies and bureaucracies: on the role of collusion in organizations. J Law Econ Organ. 1986;2(2):181-214. DOI: 10.1093/oxfordjournals.jleo.a036907

[21] Cavelty MD, Suter M. Public-private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection. Int J Crit Infrastruct Prot. 2009;2(4):179-87. DOI: 10.1016/j.ijcip.2009.08.006

[22] Levi M. Evaluating the control of money laundering and its underlying offences: the search for meaningful data. Asian J Criminol. 2020;15(4):301-320, DOI: 10.1007/s11417-020-09319-y. [Note: Author acknowledges that Levi's specific JMLIT empirical assessment is drawn from practitioner reports and parliamentary evidence given the limited peer-reviewed literature on JMLIT to date; also see reference 23.]

[23] Home Office. Suspicious activity reports regime: a call for information. London: Home Office; 2019. HM Treasury and Home Office. UK

national risk assessment of money laundering and terrorist financing. London: HM Treasury; 2020. p. 43-47. https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020

[24] Lowenthal MM, Clark RM, editors. The five disciplines of intelligence collection. Washington, DC: CQ Press; 2016.

[25] Savona EU, Riccardi M, editors. From illegal markets to legitimate businesses: the portfolio of organised crime in Europe. Trento: Transcrime; 2015. Available from: https://www.transcrime.it/wp-content/uploads/2015/03/OCP-Full-Report.pdf

[26] Zarate JC. Treasury's war: the unleashing of a new era of financial warfare. New York: PublicAffairs; 2013.

[27] Financial Action Task Force. Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CFT systems. Paris: FATF; 2022. p. 15-30. https://www.fatf-gafi.org/content/dam/fatf-gafi/methodology/FATF-Assessment-Methodology-2022.pdf

[28] Wæver O. Securitization and desecuritization. In: Lipschutz RD, editor. On security. New York: Columbia University Press; 1995. p. 46-87.

[29] Bigo D. Security and immigration: toward a critique of the governmentality of unease. Altern Glob Local Polit. 2002;27(1 Suppl):63-92. DOI: 10.1177/03043754020270S105;
Loader I, Walker N. Civilizing security. Cambridge: Cambridge University Press; 2007, DOI: 10.1017/CBO9780511611117;
Bourdieu P. The logic of practice. Nice R, translator. Cambridge: Polity Press; 1990.

[30] Foucault M. Discipline and punish: the birth of the prison. Sheridan A, translator. New York: Vintage Books; 1977. p. 195-228. https://monoskop.org/images/4/43/Foucault_Michel_Discipline_and_Punish_The_Birth_of_the_Prison_1977_1995.pdf
Burchell G, Gordon C, Miller P, editors. The Foucault effect: studies in governmentality. Chicago: University of Chicago Press; 1991. DOI: 10.7208/chicago/9780226028811.001.0001

[31] European Banking Authority. Opinion on the implementation of customer due diligence measures in the AML/CFT framework. London: EBA; 2020. p. 22-35. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2020/931093/EBA%20Report%20on%20the%20future%20of%20AML%20CFT%20framework%20in%20the%20EU.pdf
Deloitte. Seventh annual compliance trends survey. New York: Deloitte; 2021. https://www.deloitte.com/content/dam/assets-zone1/au/en/docs/services/audit-assurance/2023/au-audit-state-of-compliance-survey-2022.pdf

[32] Tirole J. Hierarchies and bureaucracies: on the role of collusion in organizations. J Law Econ Organ. 1986;2(2):181-214. p. 194-201. DOI: 10.1093/oxfordjournals.jleo.a036907

[33] European Parliament and Council. Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). OJ L 119. Brussels: Official Journal of the European Union; 2016. Arts 5, 6, 9, 23. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Digital Economy Act 2017. UK Public General Acts. London: HMSO; 2017. Chapter 30. https://www.legislation.gov.uk/ukpga/2017/30/contents

[34] Financial Transactions and Reports Analysis Centre of Canada (FINTRAC). Project guardian: money laundering associated with fentanyl trafficking. Ottawa: FINTRAC; 2019. https://fintrac-canafe.canada.ca/intel/operation/iso-osi-eng.pdf

[35] Marsh S. Public-private partnerships for financial intelligence sharing. Basel: Basel Institute on Governance; 2024. https://baselgovernance.org/sites/default/files/2024-11/Quick-Guide-34.pdf

[36] Financial Action Task Force. International standards on combating money laundering and the financing of terrorism and proliferation. Paris: FATF; 2012 (updated 2023). https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

[37] UK National Crime Agency. Suspicious activity reports annual report 2022. London: NCA; 2022. https://www.nationalcrimeagency.gov.uk/who-we-are/publications/632-2022-sars-annual-report-1/file