INTERNATIONAL JOURNAL OF BUSINESS AND ECONOMICS INSIGHTS

Volume: 16; **Issue:** 10
Pages: 01– 31
Accepted: 25 September 2026
Published: 02 October 2026

Artificial Intelligence in Combating Illicit Finance: A Comprehensive Review of TBML, CFT, CPF, and International Sanctions

Mostafa Kamal[1];

[1]. *VP & Unit Head, Import & Export (RMG and non RMG), Trade Services Division, City Bank PLC, Dhaka, Bangladesh; Email: saikatdu20@yahoo.com*

DOI: 10.63125/ppkqpy73
This work was peer-reviewed under the editorial responsibility of the IJBEI, 2026

Abstract
Artificial intelligence (AI) is promoted as the answer to a hard detection problem: finding the few unlawful transactions among billions of lawful ones. This review examines its use against trade-based money laundering (TBML), terrorist financing and proliferation financing, and in the application of international sanctions. It is a narrative review of 100 journal articles, whose bibliographic details were verified in Crossref, and of the official instruments. The study first sets out the three threats, the international framework and the rationale for sanctions. The study then reviews seven families of methods: rules, supervised learning, anomaly detection, graph learning, natural language processing, privacy-preserving learning and generative models. The evidence is uneven. Studies on real bank data report that learned models rank suspicious activity better than rule-based monitoring, and studies on a public Bitcoin benchmark report gains over earlier models. For TBML, statistical screening of prices and mirror trade data is established, while machine learning has addressed customs fraud more than laundering. For terrorist financing, proliferation financing and sanctions screening, peer-reviewed evaluation is thin, and in name screening gains in true matches have come with more false ones. Almost no study reports outcomes after deployment. AI research is therefore strongest where data are abundant and weakest where the concern behind sanctions is greatest, a mismatch explained by fragmented data and scarce confirmed cases more than by algorithms. The sanctions literature adds that effectiveness is conditional, evasion is adaptive, and humanitarian harm, de-risking, weak due process and the disputed legitimacy of unilateral measures are documented; we present opposing positions without endorsing either. AI may ease or aggravate these problems, and brings risks of opacity, bias, automated over-compliance and intrusion on privacy. The study offers nine propositions, including investment in linked trade data, explicit costs for false positives, explainable and contestable models, and evaluation of outcomes. Summaries of most cited studies were not checked against full texts, and no new data are reported.

Keywords
Artificial intelligence; Machine learning; Illicit finance; Trade-based money laundering; Terrorist financing; Proliferation financing; Sanctions screening; Graph learning; Explainability; Financial Action Task Force

INTRODUCTION

Banks, customs authorities and financial intelligence units are asked to find a very small number of unlawful transactions among billions of lawful ones. For three decades the main tools were rules written by experts: thresholds, scenarios and lists. These tools generate large volumes of alerts, most of which prove to be of no interest, and their logic can be learned and avoided (Bolton & Hand, 2002; Chen et al., 2018). Artificial intelligence (AI), by which we mean machine learning and related techniques that infer patterns from data, is now promoted as the way to do better: to rank alerts, to find anomalies and networks that rules miss, to match names across scripts and to read documents (Han et al., 2020; Jensen & Iosifidis, 2023; Kute et al., 2021).

The problems to which AI is applied are not one problem. Rules against money laundering were built from the late 1980s to deprive criminals of their proceeds. Rules on countering the financing of terrorism (CFT) were added after September 2001 (Clunan, 2006; Levi, 2010). Rules on countering proliferation financing (CPF) entered the standards of the Financial Action Task Force (FATF) in 2012, and an obligation to assess proliferation financing risk in 2020. Trade-based money laundering (TBML), the movement of illicit value through invoices and shipments, cuts across all three (Albright et al., 2010; Zdanowicz, 2009); Figure 1 sketches the relationship. And the instrument at the centre of CFT and CPF is sanctions: the freezing of assets of designated persons and entities, surrounded by the wider autonomous sanctions of states and by the public listing of jurisdictions. The use of sanctions has grown markedly (Felbermayr et al., 2020; Morgan et al., 2023), while scholars remain divided on how well they work and at what cost (Baldwin, 2000; Drezner, 2024; Pape, 1997; Peksen, 2019).

These fields have separate literatures. Computer scientists publish detection models, usually for money laundering through banks or for virtual assets. Criminologists and economists assess the anti-money laundering regime. Scholars of international relations and law debate sanctions. This review brings them together around five questions:

RQ1. What are TBML, terrorist financing and proliferation financing, what international framework counters them, and what are sanctions meant to achieve?

RQ2. Which AI methods have been applied to illicit finance, and what do they do?

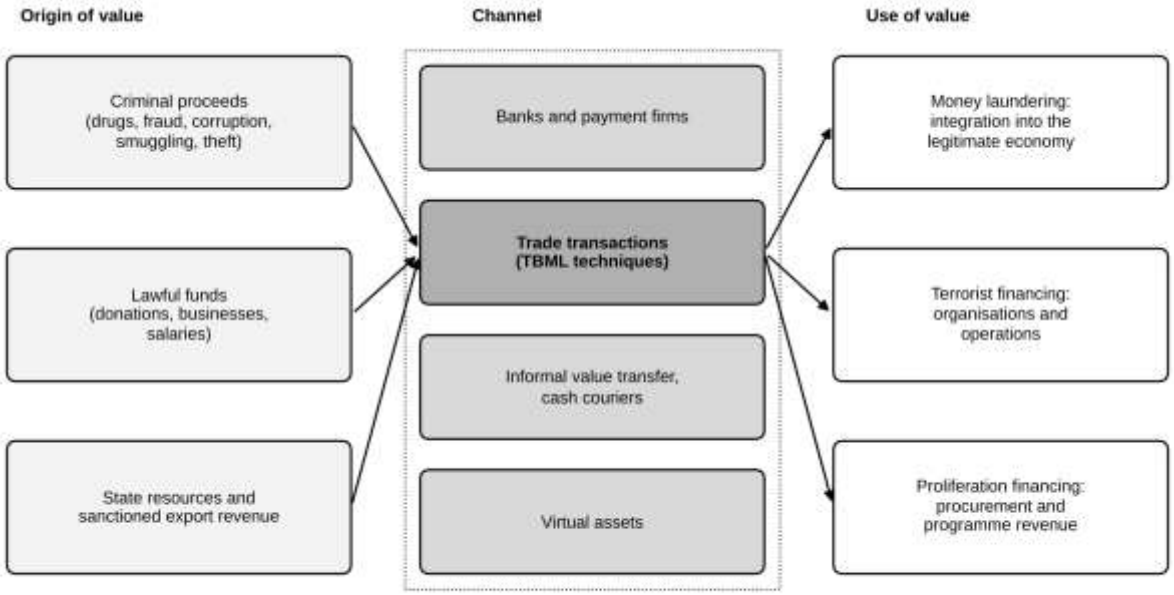
RQ3. What has been reported for each domain (money laundering through banks, virtual assets, TBML, terrorist financing, proliferation financing and sanctions screening), and how strong is the evidence?

RQ4. What does the literature say about the effectiveness and the costs of sanctions, the setting in which these tools operate?

RQ5. What risks does AI introduce, and what safeguards are discussed?

The article is a narrative review based on 100 journal articles and on the official instruments. It presents no new data. Its main finding can be stated at the outset: AI research is concentrated where data are abundant and labelled, in bank transaction monitoring and public blockchains, and is thin where the policy concern about sanctions is greatest, in trade, terrorist financing and proliferation financing. Sanctions are politically contested. We describe the positions taken by states and scholars and the evidence for them; we do not argue that any particular sanctions regime is justified or unjustified.

Figure 1: Origins, channels and uses of illicit value, with trade as a channel common to money laundering, terrorist financing and proliferation financing



APPROACH AND SOURCES

Type of review

The questions span law, policy, criminology and computer science, which do not share outcome measures, so results cannot be pooled. We therefore chose a narrative, integrative design. It is comprehensive in scope, in that it covers all four subjects named in the title, but it is not a systematic review: there was no protocol, no exhaustive search and no screening record, and a reader should not treat the number of studies cited on a point as a measure of the weight of the literature.

Finding the literature

The policy and sanctions literature was selected purposively to represent the main positions in each debate. The AI literature was located through the public interface of OpenAlex, an open index of scholarly works, using title searches for the phrases money laundering; trade-based money laundering; customs fraud detection; terrorist financing; terrorism financing detection; proliferation financing; sanctions screening; sanctions evasion; illicit transactions bitcoin; maritime anomaly detection AIS; federated learning money laundering; and large language models combined with financial crime or money laundering. Results were ordered by citation count and read by title. We retained articles in journals that we judged to be established, preferring empirical studies on real data and reviews, and we looked in particular for studies outside bank transaction monitoring. Ordering by citations favours older work, and the judgement of journals is subjective. Eight methodological references on fraud detection, class imbalance, anomaly detection, explainability and algorithmic bias were carried over from earlier work by the same drafting process.

Three kinds of source

Official instruments. Definitions and obligations are taken from the FATF Recommendations and typology reports and from resolutions of the United Nations Security Council. They are named in the text and tables and are not listed among the references, which are confined to journal articles.

Research literature. The bibliographic details of each of the 100 references (authors, title, journal, volume, issue, pages, year and DOI) were retrieved from its Crossref record. The descriptions of what each article argues or finds were drafted by a language-model tool. For 63 articles the description was compared with the abstract by an independent checking agent; for the rest it rests on the tool's knowledge of the literature or, for a few marked as such in the table of empirical studies, on the title

alone. Full texts were not read. Where we give a number from a study, readers should confirm it in the original before relying on it.

Current facts. Statements about the status of sanctions regimes and FATF lists in 2024 to 2026 were checked against web sources: Security Council Report, the International Peace Institute, a Congressional Research Service brief, government press releases, press reports and professional summaries of FATF plenary outcomes. The FATF's own web pages could not be retrieved in our working environment. These facts are dated in the text and may have changed since.

BACKGROUND: THREATS, FRAMEWORK AND THE RATIONALE FOR SANCTIONS

Terms

Table 1 gives the working definitions. We use sanctions in the broad sense for all restrictive measures short of force, and targeted financial sanctions for asset freezes and related prohibitions against designated persons and entities. We distinguish measures decided by the Security Council, which bind all member states, from autonomous (often called unilateral) measures adopted by states or regional organisations under their own law.

Table 1: Working definitions

Term	Working definition used in this article	Principal basis
Money laundering (ML)	Processing the proceeds of crime to disguise their illegal origin so that they can be used as if legitimate	Vienna (1988) and Palermo (2000) Conventions; FATF Recommendation 3
Trade-based money laundering (TBML)	Disguising the proceeds of crime and moving value through trade transactions in an attempt to legitimise their illicit origin; the aim is the movement of money, not of goods	FATF typologies report (2006); FATF and Egmont Group report (2020)
Terrorist financing (TF)	Providing or collecting funds, by any means, with the intention or knowledge that they will be used to carry out terrorist acts or by a terrorist organisation or individual terrorist; the funds may be of lawful origin	International Convention for the Suppression of the Financing of Terrorism (1999); Security Council resolution 1373 (2001); FATF Recommendation 5
Proliferation financing (PF)	Providing funds or financial services used for the manufacture, acquisition, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons, their means of delivery and related materials, in contravention of national laws or international obligations	FATF working definition (2010 status report; 2021 guidance); Security Council resolution 1540 (2004)
Proliferation financing risk (FATF standard)	The potential breach, non-implementation or evasion of the targeted financial sanctions obligations referred to in Recommendation 7; narrower than the working definition above	FATF Recommendation 1 and its interpretive note, as amended in October 2020
Targeted financial sanctions (TFS)	Asset freezing and prohibitions that prevent funds or other assets from being made available, directly or indirectly, to designated persons and entities	FATF Recommendations 6 and 7; Security Council resolutions adopted under Chapter VII of the Charter
Sanctions (broader sense)	Restrictive measures short of force (asset freezes, travel bans, arms embargoes, trade, sectoral and financial restrictions) adopted by the Security Council, by regional organisations or by individual states	Article 41 of the Charter of the United Nations; national and regional law

Money laundering and the trade channel

Controls on money laundering first concentrated on banks, through customer identification, record keeping and the reporting of suspicious transactions. A recurring argument is that pressure on one channel moves activity to another: tighter rules on banks make cash, informal value transfer and trade

more attractive (Hataley, 2020; Passas, 2006; Unger & den Hertog, 2012). The scale of laundering is uncertain. Estimates from gravity models depend on strong assumptions (Walker & Unger, 2009), and reviewers have warned for two decades that the available figures do not support confident statements about the volume of laundering or the effect of controls (Levi & Reuter, 2006; Levi et al., 2018).

TBML is the use of trade transactions to move value and legitimise its origin. The FATF's 2006 typology report identified the basic techniques, and a joint report with the Egmont Group in 2020 updated them (Table 2). All rely on a gap between what the documents say and what was shipped: the price, the quantity, the quality or the existence of the goods. Academic treatments stress that the term covers different things for different users and that banks, which see payments more often than goods, need an operational definition (McSkimming, 2010; Naheem, 2015).

Table 2: Trade-based techniques and indicators, described at the level of published typologies

Technique	How value is moved	Indicators discussed in typology reports and research
Over-invoicing of imports or under-invoicing of exports	Value leaves the country of the importer, or stays abroad with the buyer	Unit prices far from market or from the range for the product; mismatch between partner countries' trade statistics
Under-invoicing of imports or over-invoicing of exports	Value enters the country of the exporter or importer; may also evade duty	As above; discrepancy correlated with tariff or tax rates
Multiple invoicing	The same shipment is invoiced and paid more than once, often through different banks	Duplicate documents; payments that exceed shipped value
Over- or under-shipment; phantom shipment	Quantity differs from the documents, or no goods move at all	Shipping documents that cannot be matched to vessel or container records
False description of goods	Quality or type is misstated to justify the price	Goods inconsistent with the trader's business; implausible routing
Third-party and offsetting arrangements	Payments made by unrelated parties; value netted between traders, as in black market currency exchange and informal value transfer	Payment from a party or jurisdiction unrelated to the transaction; circular flows
Open-account settlement through front or shell companies	Bank sees only a payment, not the underlying documents	Newly formed companies with large trade flows; opaque ownership

Terrorist financing and proliferation financing

Terrorist financing differs from laundering in ways that matter for detection (Table 3). The funds may be lawful in origin, so the task is to find where money is going, not where it came from. Freeman (2011) classified sources as state sponsorship, illegal activity, legal activity and popular support. Sums can be small, and movement can use informal value transfer systems that leave few records (Basile, 2004; Passas, 2006; Chowdary & Md, 2020; Chowdary & Jamil, 2020). Fund-raising has also moved to social media and online platforms (Asheke & Bin, 2022; Keatinge & Keen, 2019; Mohsin & Jannatul, 2021; Chowdary, 2021). Early assessments doubted that controls designed for laundering would do much damage to resilient networks (Islam & Md, 2023; Basile, 2004; Khalid & Sadmeen, 2022; Maksudul & Islam, 2022), later reviews found the evidence of impact thin (Levi, 2010; Mashfiqur & Jamil, 2023; Md & Kynatun, 2023; Maksudul & Hossen, 2023), and others pointed to collective action problems among states (Clunan, 2006; Mohsin & Kaniz, 2023; Mamunur & Md, 2023; Sadia & Mosheur, 2023).

Proliferation financing is the least developed concept. The FATF's working definition covers the provision of funds or financial services for the acquisition, transfer or use of nuclear, chemical or biological weapons and their means of delivery (Sharmin & Kaniz, 2023; Sharmin & Nishat, 2023; Sadmeen & Khalid, 2023). It has two sides: procurement, in which dual-use goods are paid for through brokers, front companies and trans-shipment hubs in transactions designed to look like ordinary trade

(Albright et al., 2010; Yeasin, 2024a, 2024b; Maishar Mostari, 2024); and revenue, in which a programme is sustained by prohibited exports, labour sent abroad and theft of virtual assets. Stewart et al. (2020) found significant gaps in national implementation and argued that most governments give the subject lower priority than money laundering or terrorist financing. The Democratic People's Republic of Korea (DPRK) is the case most studied (Haggard & Noland, 2010; Mashfiqur, 2024; Masrul & Mashfiqur, 2024; Masrul &Kanti, 2024; Wertz, 2013). According to press coverage of the second report of the Multilateral Sanctions Monitoring Team, published on 22 October 2025, DPRK-linked actors stole about USD 2.8 billion in virtual assets between January 2024 and September 2025; we have not examined the report itself.

The standard is narrower than the concept. FATF Recommendation 7 requires the implementation of targeted financial sanctions under the relevant Council resolutions, and the 2020 amendment to Recommendation 1 defines proliferation financing risk strictly as the risk of breach, non-implementation or evasion of those sanctions. A list-based standard faces a network-based threat, which is one reason for interest in methods that can look beyond names.

Table 3: Money laundering, terrorist financing and proliferation financing compared

Dimension	Money laundering, including TBML	Terrorist financing	Proliferation financing
Origin of funds	Criminal proceeds	Lawful or unlawful: state sponsorship, donations, businesses, crime	Often state resources and revenue from sanctioned exports; also crime, including theft of virtual assets
Purpose of the conduct	Conceal origin; enjoy or reinvest proceeds	Sustain an organisation; fund operations	Pay for and conceal procurement of goods and technology; raise revenue for a weapons programme
Direction of concealment	Hide where the money came from	Hide where the money is going	Hide the end user and, often, the origin as well
Typical amounts	Can be very large	Operations can be cheap; organisations cost more	Individual payments often look like ordinary trade payments
Main actors	Organised crime, professional launderers, complicit traders	Organisations, facilitators, sympathisers, state sponsors	State-directed networks, front companies, brokers, shipping firms
Role of trade	Central to TBML: invoices and shipments carry value	Trade and informal value transfer used by some groups	Central: dual-use goods, trans-shipment hubs, commodity exports
Primary control	Preventive measures, reporting, confiscation	Criminalisation; targeted financial sanctions (Recommendation 6)	Targeted financial sanctions (Recommendation 7); export controls; activity-based prohibitions in Council resolutions
Detection difficulty	Mispricing is hard to prove without reference prices	Small sums and lawful sources leave few signals	Transactions resemble legitimate trade; list screening misses non-designated fronts

The international framework

The framework rests on two pillars of different legal character (Figure 2, Table 4). The Security Council, acting under Chapter VII of the Charter, adopts decisions that bind all member states. The FATF, an intergovernmental body created in 1989, issues Recommendations that are not treaties but are enforced through peer review, follow-up and the public listing of jurisdictions with strategic deficiencies. The two are linked: FATF Recommendations 6 and 7 require countries to implement without delay the

targeted financial sanctions decided by the Council.

On terrorist financing, the 1999 Convention defined the offence; resolution 1267 (1999) imposed measures on the Taliban that were later extended to Al-Qaida and, in 2015, reframed around ISIL (Da'esh) and Al-Qaida; and resolution 1373 (2001) required every state to criminalise terrorist financing and freeze terrorist assets. Sharman (2008) explained the rapid spread of anti-money laundering rules, the base on which CFT rules were built, to developing states less by their demonstrated benefits than by power exercised through blacklisting and by imitation. Morse (2019) found that FATF listing works through markets: banks and investors penalise listed countries, which then criminalise terrorist financing sooner. On proliferation, resolution 1540 (2004) imposed general obligations; country regimes followed for the DPRK (resolution 1718 of 2006 and successors, with sectoral bans added in 2016 and 2017) and for Iran (resolutions from 2006, terminated subject to a reimposition mechanism by resolution 2231 of 2015).

Figure 2: Architecture of the international framework against terrorist and proliferation financing

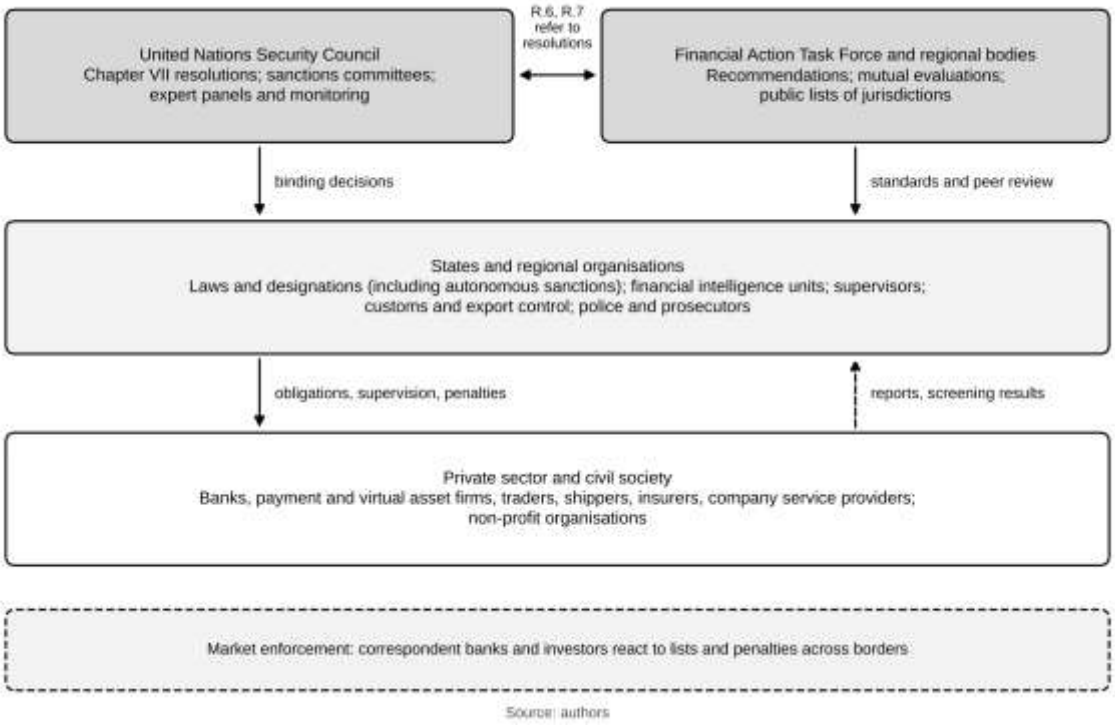
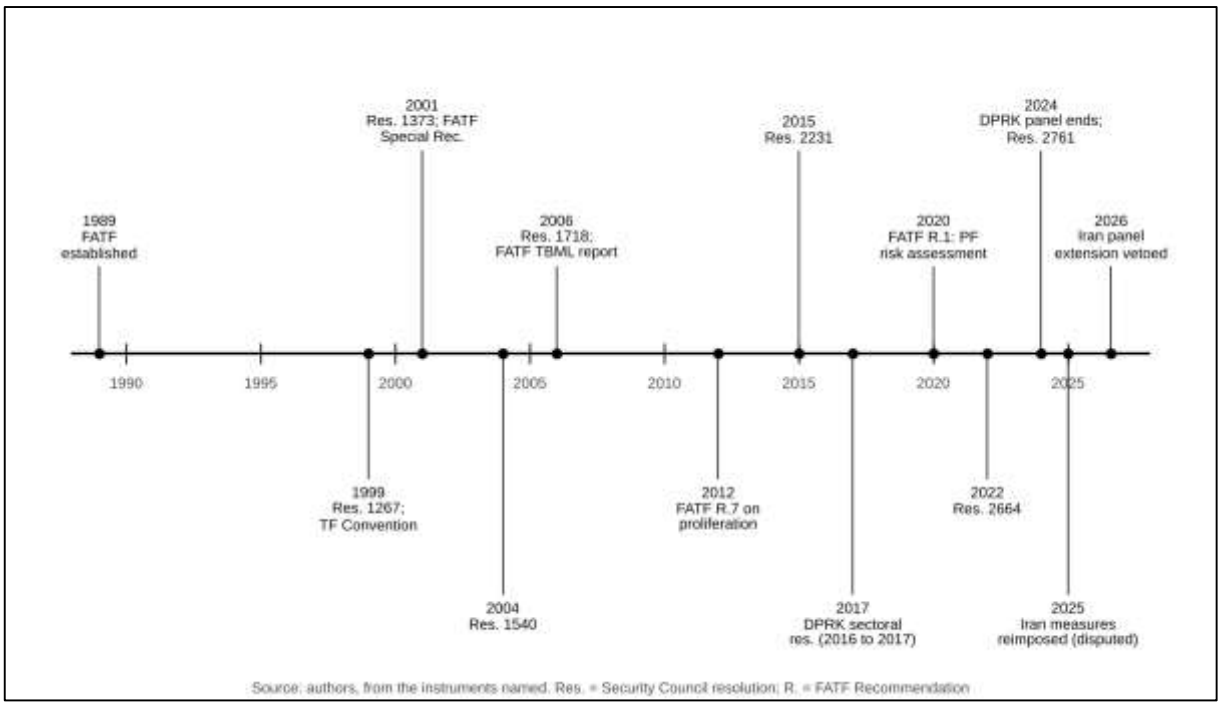


Table 4: Principal international instruments

Instrument	Year	Relevance to TF, PF and sanctions
Charter of the United Nations, Article 41	1945	Authority of the Security Council to decide measures not involving armed force; decisions bind member states (Article 25)
International Convention for the Suppression of the Financing of Terrorism	1999	Defines the offence of terrorist financing; requires criminalisation, freezing and cooperation
Security Council resolution 1267 and successor resolutions	1999	Asset freeze, travel ban and arms embargo; today the ISIL (Da'esh) and Al-Qaida list (resolutions 1989 and 2253) and a separate Taliban regime (resolution 1988)
Security Council resolution 1373	2001	Requires all states to criminalise terrorist financing and to freeze terrorist assets; designations are made nationally

Instrument	Year	Relevance to TF, PF and sanctions
Security Council resolution 1540	2004	Requires all states to prohibit non-state actors from acquiring weapons of mass destruction, including by financing, and to control the financing of related exports and trans-shipment
Security Council resolution 1718 and successor resolutions	2006	Sanctions on the Democratic People's Republic of Korea: designations, financial restrictions and sectoral bans widened in 2016 and 2017
Security Council resolution 2231	2015	Endorsed the nuclear agreement with Iran and terminated earlier Iran resolutions, subject to a reimposition (snapback) mechanism
Security Council resolution 2664	2022	Humanitarian exemption from asset freezes across United Nations regimes; made indefinite for the ISIL and Al-Qaida regime by resolution 2761 (2024)
FATF Recommendations 5 and 6	2001; revised 2012	Terrorist financing offence; targeted financial sanctions related to terrorism and terrorist financing
FATF Recommendation 7	2012	Targeted financial sanctions related to proliferation, implementing the relevant Council resolutions without delay
FATF Recommendation 8	2001; revised 2023	Risk-based protection of non-profit organisations from terrorist financing abuse; revised to discourage disproportionate measures
FATF Recommendations 1 and 2 (amendment)	2020	Countries and private-sector entities to identify, assess and mitigate proliferation financing risk; domestic coordination
FATF Immediate Outcomes 9, 10 and 11	2013; revised 2022	Effectiveness assessed for terrorist financing prosecution, terrorist financing prevention and sanctions, and proliferation financial sanctions

Figure 3: Selected milestones, 1989 to 2026



What sanctions are for

The older literature asked one question of sanctions: did the target change its policy? Galtung (1967), writing about Rhodesia, described what he called the naive theory, that economic pain turns into political compliance, and showed how a target can adapt and its population rally. Pape (1997) re-examined the cases then counted as successes and concluded that few survived scrutiny. Baldwin (2000) replied that an instrument has to be compared with the alternatives, usually diplomacy alone or force, and judged against all of its goals.

Work on United Nations targeted sanctions has since distinguished three purposes: to coerce a change of behaviour, to constrain a target's capacity to act, and to signal or stigmatise the violation of a norm (Biersteker et al., 2018). Policy statements often add two further aims, deterrence of others and protection of the financial system, which Table 6 lists separately. The distinction matters for illicit finance and for the design of detection systems (Figure 4). Few expect an asset freeze to persuade a terrorist organisation to give up its aims; the stated rationale of CFT sanctions is to constrain. CPF sanctions combine purposes: measures against a state are meant to coerce it towards negotiation and to cut the revenue of its programmes, while designations of procurement agents and front companies are meant to constrain. FATF listing is mainly a signal, addressed to markets as much as to governments (Morse, 2019).

Four arguments are made for placing financial measures at the centre. They are an alternative to force (Baldwin, 2000). They have leverage, because international payments run through a small number of currencies, correspondent banks and messaging systems, a condition that Farrell and Newman (2019) called weaponized interdependence; the threat of exclusion induces banks in third countries to comply with measures that do not formally bind them (Drezner, 2015). The action taken by the United States Treasury against Banco Delta Asia in 2005 is the illustration most often given; Wertz (2013) traces the development of financial measures against the DPRK. They can be targeted, in response to the harm attributed to the comprehensive embargo on Iraq in the 1990s (Drezner, 2011; Weiss, 1999). And they delegate enforcement to private firms, which screen customers and payments against lists under threat of penalty. Early and Preble (2020) described a shift in United States enforcement towards fewer and much larger penalties, which, as their abstract states, they trace to the shift of emphasis from Cuba to Iran and to legislation that raised maximum penalties. This fourth argument is where AI enters: delegation creates a very large screening and monitoring task inside private firms, and the cost of error in either direction is high.

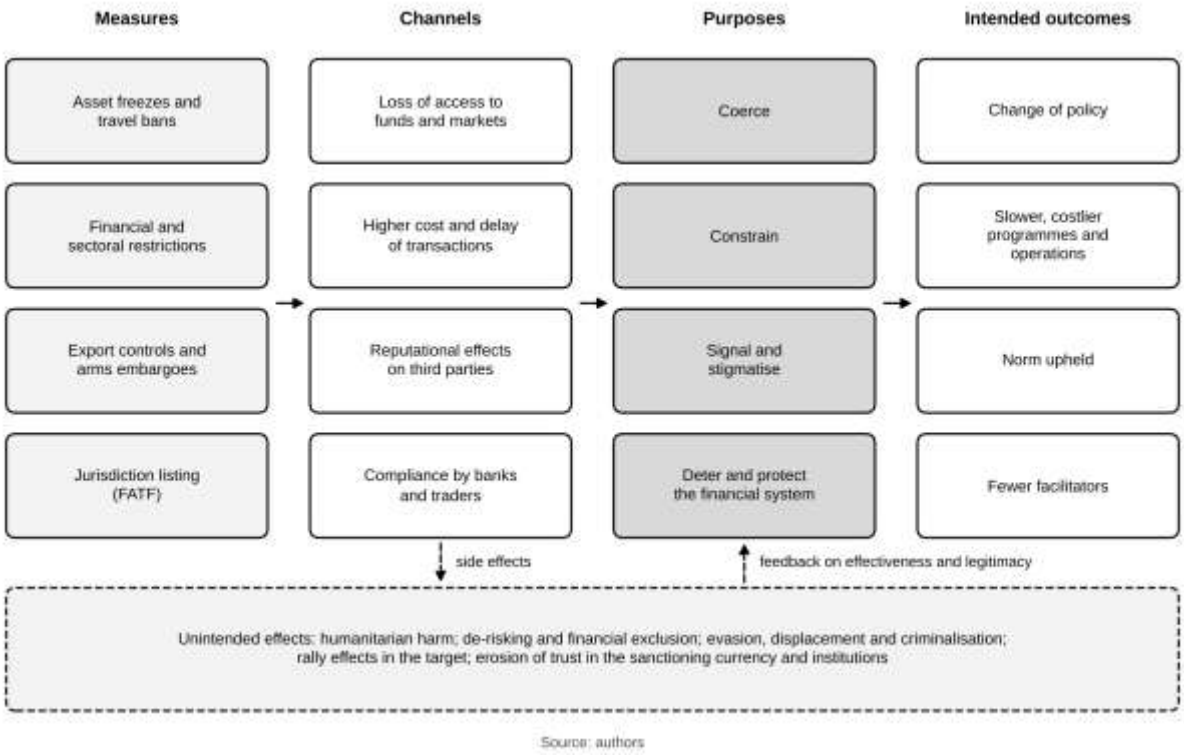
The legal basis differs by measure. Measures decided by the Council rest on the Charter. Autonomous sanctions rest on the domestic law of the sender. Many developing states, and a long series of General Assembly resolutions, describe them as unilateral coercive measures contrary to non-intervention and sovereign equality; the states that use them regard them as a lawful exercise of jurisdiction over their own territory, nationals, currency and markets (Hofer, 2017).

Table 6: Purposes of sanctions in the control of illicit finance

Purpose	Logic	Illicit-finance control	What success would look like
Coerce	Raise the cost of a policy until the target changes it	Sectoral and financial sanctions intended to bring a state to negotiate on its nuclear programme	Change in the target's behaviour
Constrain	Deny money, goods and services needed for the proscribed activity	Asset freezes on procurement agents, front companies, financiers and facilitators; bans on revenue-earning exports	Activity made slower, costlier or riskier, even if it continues
Signal and stigmatise	Affirm a norm and mark its violation; inform markets	Listing of terrorist groups; FATF public statements	Norm reinforced; third parties adjust their dealings
Deter	Show others the cost of similar conduct	Penalties on banks and traders that deal with designated parties	Fewer facilitators willing to deal

Purpose	Logic	Illicit-finance control	What success would look like
Protect the financial system	Keep designated actors and high-risk flows out of banks and markets	Screening, correspondent due diligence, countermeasures against high-risk jurisdictions	Lower exposure of institutions; integrity of payment channels

Figure 4: Logic model of sanctions: measures, channels, purposes, intended outcomes and unintended effects



LITERATURE REVIEW: ARTIFICIAL INTELLIGENCE IN THE CONTROL OF ILLICIT FINANCE

From rules to learning

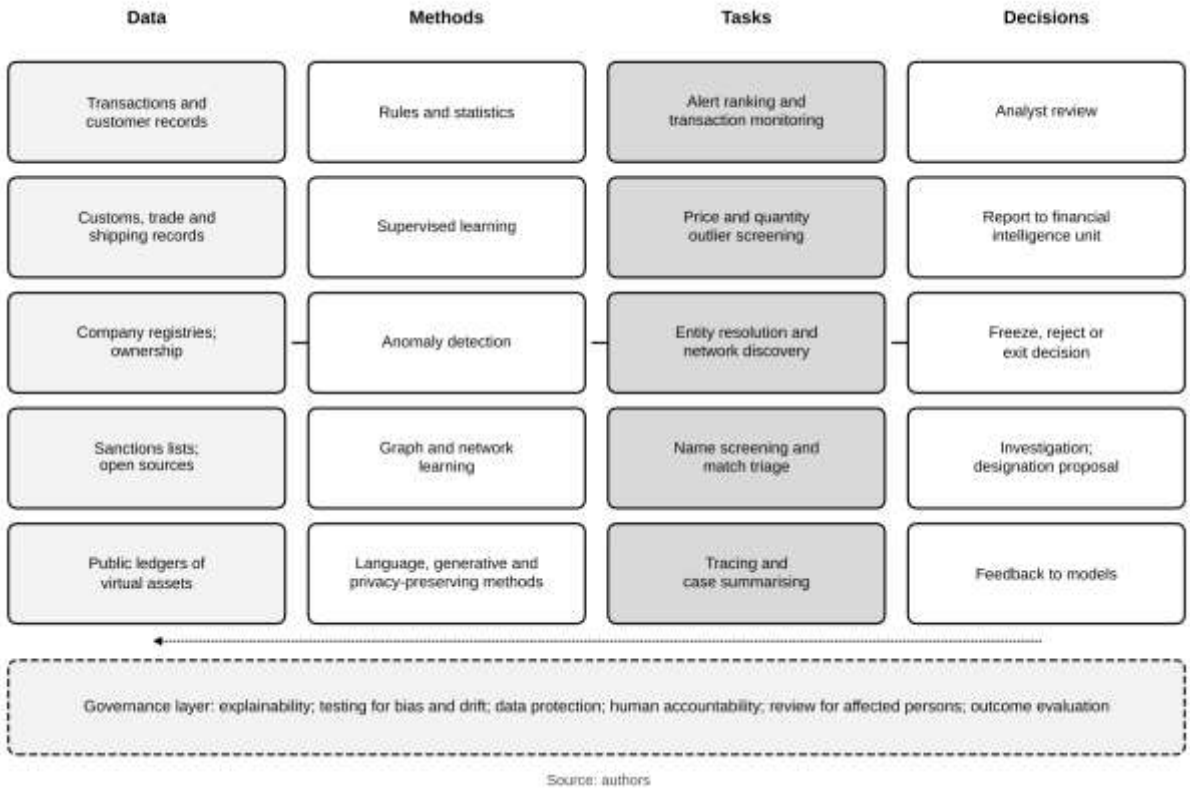
Statistical detection of financial wrongdoing is older than the current interest in AI. Bolton and Hand (2002) set out the two approaches that still organise the field: supervised methods, which learn from examples of known fraud, and unsupervised methods, which look for departures from normal behaviour when examples are few. They also identified the difficulties that recur in every later review: the event is rare, labels are uncertain and arrive late, and offenders adapt. Gao and Ye (2007) proposed an early framework for data mining in anti-money laundering research. A decade later Chen et al. (2018) reviewed machine-learning techniques for suspicious transaction detection; as we recall the review, it covers link analysis, behavioural modelling, risk scoring and anomaly detection.

The motive for moving beyond rules is the alert problem. Rule-based monitoring produces many alerts and few reports, and the economics of reporting make this worse: the model of Takáts (2011) shows how penalties for failing to report lead institutions to report so much that the reports lose their informational value. Semi-structured interviews with eight specialists, reported by Oztas et al. (2024), describe transaction monitoring from the industry's point of view, and the review of Jensen and Iosifidis (2023) divides the technical literature into client risk profiling and the flagging of suspicious behaviour, noting, as we read it, that the lack of public data sets limits comparison between methods. Table 7 summarises the families of methods discussed below, and Figure 5 shows how data, methods, tasks and decisions connect.

Table 7: Families of methods applied to illicit finance

Family of methods	How it works	Typical use in illicit-finance control	Main limitation	Sources
Rules and scenarios	Fixed thresholds and patterns written by experts	Transaction monitoring alerts; list screening by exact or fuzzy match	Many alerts of little value; logic can be learned and avoided	Bolton & Hand (2002); Gao & Ye (2007); Oztas et al. (2024)
Supervised learning	Model trained on past cases labelled suspicious or not (regression, tree ensembles, neural networks)	Ranking alerts or transactions for review; customer risk scoring	Labels are scarce, delayed and reflect past reporting practice; severe class imbalance	Jullum et al. (2020); Zhang & Trubey (2019); He & Garcia (2009)
Unsupervised and anomaly detection	Flags records unlike the rest (clustering, isolation, autoencoders)	Unusual behaviour against own history or peer group; price outliers in trade data	Unusual is not the same as unlawful; hard to validate	Chandola et al. (2009); Liu et al. (2012); Hilal et al. (2022); Rocha-Salazar et al. (2021)
Network and graph learning	Analyses links between accounts, firms, wallets or vessels; graph neural networks learn from structure	Detection of groups, intermediaries and layering; ownership networks; blockchain flows	Needs linked data across institutions; explanations are difficult	Akoglu et al. (2015); Fronzetti Colladon & Remondi (2017); Drężewski et al. (2015); Cheng et al. (2023)
Natural language processing	Matches and interprets text: names, addresses, documents, news	Name screening against sanctions lists; adverse media; trade documents	Transliteration and aliases; trade-off between missed matches and false matches	Kim & Yang (2024); Alkhalili et al. (2021)
Privacy-preserving and federated learning	Trains a shared model without pooling raw data	Detection across banks or jurisdictions under data-protection limits	Early stage; governance and security of the shared model	Bashir et al. (2026)
Generative models, including large language models	Produce or summarise text from prompts	Drafting case narratives; summarising evidence; assisting screening	Little peer-reviewed evaluation in this field; bias and fabrication risks	Tasneem et al. (2026)

Figure 5: From data to decision: where artificial intelligence methods enter the control of illicit finance



Supervised learning for transaction monitoring

Supervised models are trained on past cases labelled as suspicious or not and are used to rank new transactions or alerts for human review. The most cited empirical example is Jullum et al. (2020), who developed and validated a model on data from Norway's largest bank. Their abstract reports that the model outperformed the bank's existing approach on the authors' performance measure, and that leaving non-reported alerts or normal transactions out of the training data was suboptimal. The second point is of general importance: what a model learns depends on which past cases are treated as negatives. Zhang and Trubey (2019) compared five learning algorithms under two schemes for over-representing the rare class, on transaction data from a United States financial institution, and reported potential advantages of machine learning for modelling such events.

Three features of the problem shape this work. The first is class imbalance: suspicious cases are a tiny share of transactions, so accuracy is uninformative and methods and measures suited to rare events are needed (He & Garcia, 2009; Saito & Rehmsmeier, 2015). The second is the nature of the label. A filed report records that an analyst found something suspicious under the rules and practices of the time; it does not record that laundering occurred, and confirmed outcomes are seldom returned to the institution. A model trained on reports therefore learns to reproduce past reporting. The third is evaluation. Studies report performance on historical data from one institution, which cannot be released, so results cannot be replicated or compared (Jensen & Iosifidis, 2023; Levi et al., 2018).

Unsupervised learning and anomaly detection

Where labels are lacking, methods that flag records unlike the rest are used: clustering, isolation-based methods and neural autoencoders (Chandola et al., 2009; Liu et al., 2012). Hilal et al. (2022) reviewed anomaly detection across types of financial fraud. For money laundering and terrorism financing together, Rocha-Salazar et al. (2021) combined comparison of a customer with its own history and with a peer group, using clustering, a new abnormality indicator and neural networks on data from a Mexican financial institution; their abstract reports fewer false positives and lower investigation costs than a rule-based system. Canhoto (2021), in a study based on the affordances that the technology offers to users, argued, as we read it, that the scarcity of confirmed cases limits supervised learning in this

field and that unsupervised methods identify unusual financial behaviour, not actual money laundering. The central difficulty is that unusual is not the same as unlawful. Anomaly scores direct attention; they do not establish anything.

Networks and graphs

Laundering, terrorist financing and sanctions evasion are carried out by groups of connected accounts, firms and persons, and the connections are often more informative than any single transaction. Akoglu et al. (2015) surveyed anomaly detection in graphs. In the money laundering literature, Drężewski et al. (2015) described social network analysis within a system supporting investigators, and Fronzetti Colladon and Remondi (2017) used network metrics to build risk profiles of the clients of a factoring company. Singh and Best (2019) showed how visualisation can help analysts see suspicious patterns. More recently, graph neural networks, which learn from the structure of the network as well as from the attributes of its nodes, have been applied to payment data; Cheng et al. (2023) proposed a group-aware method aimed at the organised, collective character of laundering and, according to their abstract, report results in both offline and online modes, a partial exception to the lack of evidence from use. A critical review of deep learning for money laundering detection notes the promise of such methods and the difficulty of explaining their output (Kute et al., 2021).

Graph methods need linked data. A single bank sees only its own part of a network, and the links that matter for TBML and proliferation financing (shared directors, addresses, vessels, freight forwarders) lie in registries and trade records outside the bank. This is a constraint of data and law more than of algorithm.

Virtual assets

Public blockchains offer what bank data do not: a complete, open record of transactions. Foley et al. (2019) estimated the share of Bitcoin activity associated with illegal use from the network of transactions; according to their abstract, about one quarter of users and 46% of transactions in their sample were so associated, figures that have been debated and that relate to an earlier period. A labelled public data set of Bitcoin transactions has become the standard benchmark for graph learning, and studies report successive gains on it with self-supervised and temporal graph neural networks (Alarab & Prakoonwit, 2023; Lo et al., 2023; Md Hasinur, 2024; Md Maksudul, 2024; Md Mohsin, 2024). Whether benchmark gains carry over to investigations is not shown in these studies. Policy research, meanwhile, has mapped the money laundering and terrorist financing risks of new technologies through an expert Delphi study (Akartuna et al., 2022; Md Tazul Islam, 2024; Md. Mainuddin, 2024; Md. Mamunur, 2024) and a scoping review (Akartuna et al., 2023; Songeta, 2024; Sumaiya, 2024; Tahmedur, 2024), and has drawn attention to the use of digital currencies to evade sanctions (Aminul Islam, 2025; Asheke, 2025; Ashik, 2025; Wronka, 2022). The theft of virtual assets attributed to the DPRK makes this the area where AI research on detection and the policy concern about proliferation financing overlap most directly (Kynatun, 2025; Maishar Mostari, 2025; Masrul, 2025).

Trade-based money laundering and customs data

The quantitative literature on TBML is mostly statistical. One approach examines unit prices in transaction-level customs data and flags those far from the usual range for a product; Zdanowicz (2009) applied this to United States trade records. Ferwerda et al. (2013) placed such estimates in a gravity model and, according to their abstract, suggest that criminals use TBML to evade stricter anti-money laundering regulation in financial markets, which is consistent with displacement from the financial channel into trade. Saenz and Lewer (2023), using a latent-variable model for member states of the European Union, report by contrast that TBML complements conventional laundering, so the evidence on displacement is not uniform. A second approach compares what one country reports exporting with what its partner reports importing. Fisman and Wei (2004) showed that the gap between Hong Kong's reported exports to China and China's reported imports rose with the tax rate on the product, and Gara et al. (2019) built risk indicators from mirror statistics for Italy after controlling for legitimate sources of discrepancy. A third tests customs data for conformity with the Newcomb-Benford law of digit frequencies (Barabesi et al., 2018; Md Hasinur, 2025a, 2025b; Md Maksudul, 2025).

Machine learning on trade data has developed mainly for customs fraud, that is, for the evasion of duty. Vanhoeyveld et al. (2020) assessed the value of behavioural and high-cardinality data for customs fraud detection under class imbalance. Studies that address laundering as such are few. Chao et al. (2019)

proposed a monitoring method for TBML that combines knowledge-driven classification with prudential regulation and illustrated it with data from China. Our searches found other recent papers on AI for TBML, but mostly in outlets whose standing we could not judge, and we have not relied on them.

Three reasons for the gap can be given. Data are fragmented: customs sees the goods, the bank sees the payment, the shipping line sees the container, and most trade is settled without a bank examining the documents. Labels are almost absent, because few TBML cases are proved. And the signals are ambiguous: prices vary for legitimate reasons, mirror data differ because of valuation and timing, and the same misinvoicing may reflect tax evasion or capital flight instead of the laundering of criminal proceeds. Statistical and learned screens in this field produce leads for inquiry, not findings.

Terrorist financing

Published AI work that addresses terrorist financing specifically is scarce. Most studies treat it together with money laundering, as Rocha-Salazar et al. (2021) do, and in practice the same monitoring systems serve both. The reasons follow from the nature of the conduct described above. Lawful origin and small amounts leave little for a transaction model to find; confirmed cases are too few to train on; and the most useful information (who is connected to whom, and what they say) lies outside transaction data. Open-source material has become relevant as fund-raising has moved online (Keatinge & Keen, 2019).

There is also a critical literature. Amoore (2009) examined how algorithmic practices that cross commercial, security and military spheres use association rules between people, places, objects and events to draw lines between the normal and the suspicious in everyday life. Research on the non-profit sector has examined the FATF's effort to prevent terrorist financing through charities and, as its title indicates, the need to protect them from counter-terrorism measures as well as from terrorists (Md Momen Shahriar, 2025; Md Tazul Islam, 2025; Md. Mamunur, 2025; Romaniuk & Keatinge, 2018). These concerns are sharper for learned models than for rules, because proxies for religion, nationality or region can enter a model without being named.

Proliferation financing and sanctions evasion

We found no journal article that evaluates a machine-learning model for the detection of proliferation financing. The relevant work lies in adjacent fields. One is maritime surveillance. Vessels broadcast identity and position through the automatic identification system (AIS), and reporting on the evasion of sectoral sanctions describes the manipulation or switching-off of these signals; Watterson et al. (2020) analysed open ship registries as an enabler of maritime sanctions evasion. Wolsing et al. (2022) reviewed 44 papers on anomaly detection in AIS tracks, and d'Afflisio et al. (2021) proposed a statistical framework for detecting spoofed positions and deliberate gaps, which the checking of its abstract indicates was tested on simulated data. A second is entity resolution and network analysis across corporate registries and trade records, which corresponds to how procurement networks operate (Albright et al., 2010; Sadia, 2025; Shabbir, 2025; Sharmin, 2025) but which we found described in institutional reports more than in journals. A third is the tracing of virtual assets, discussed above. The absence of evaluated methods is consistent with the low priority that Stewart et al. (2020) found the subject to have, and with the narrow, list-based definition of risk in the standard.

Evasion is adaptive, which bears on any detection method. Third countries replace lost trade, and commercial partners and even allies of the sender are among them (Early, 2009). Evasion builds smuggling networks, front companies and corrupt relationships that persist after sanctions are lifted (Andreas, 2005; Songeta, 2025; Sumaiya Sadmeen, 2025; Tahmedur, 2025). A model trained on last year's typologies is tested against this year's adaptations.

Sanctions screening

Screening compares the names of customers and of parties to payments with lists of designated persons. It is the most widespread automated control and the one most directly created by sanctions. The difficulty is linguistic: names are transliterated between scripts, abbreviated, reordered and deliberately varied, and lists contain aliases. Fuzzy matching finds more true matches at the price of many false ones. Kim and Yang (2024) state that false-positive rates in screening exceed 90% and tested a prototype natural language processing tool; according to their abstract it substantially improved detection of true matches but also raised false positives, and the authors argue that reducing missed matches should take priority. Alkhalili et al. (2021) applied machine learning to the triage of watch-list

matches, with the aim of reducing analysts' workload, and found that a support vector machine performed best of the three classifiers compared.

Two observations follow. The trade-off between missed and false matches is a policy choice as much as a technical one, because the costs fall on different people: a missed match exposes the institution to penalties, while a false match delays or denies service to a customer who shares a name with a listed person (Ahmed, 2026; Asheke, 2026; Ashik, 2026). And screening by name addresses only designated parties. It does not find the non-designated fronts on which evasion relies, which again points towards network methods (Gazi Yeasin, 2026; Kynatun, 2026; Maishar Mostari, 2026). Field research on banks in Lebanon found that the adoption of screening and monitoring technology was driven mainly by coercive pressure, in particular from United States regulation, and that vendor selection, data quality and the geopolitical setting limited its effectiveness (Bakhos Douaihy & Rowe, 2023).

Privacy-preserving and generative approaches

Two newer strands should be noted, with the caution that the journal literature on both is young. Federated learning trains a shared model across institutions without pooling raw data, which would address the fragmentation described above within data-protection limits; Bashir et al. (2026) is a recent example aimed at evolving laundering patterns. Large language models are being discussed for drafting case narratives, summarising evidence and assisting screening (Md Hasinur, 2026; Md Maksudul, 2026; Md Mohsin, 2026). Our searches found very few peer-reviewed evaluations of them in this field. One, by Tasneem et al. (2026), examined summaries of financial-crime news produced by three proprietary models and found small but statistically significant differences when demographic identity terms were swapped. Claims made for generative AI in compliance currently run well ahead of published evidence.

What the literature shows, by domain

Table 8 lists the empirical studies discussed, with the basis for our description of each, and Table 9 gives our assessment by domain. Figure 6 arranges 39 of the studies cited in this review by domain and method. In our selection, work on learning methods is concentrated on money laundering through banks; the virtual-asset studies of graph learning share one public benchmark; and for TBML the cited work is mostly statistical. For terrorist financing, proliferation financing and sanctions screening, the areas most closely tied to sanctions, the peer-reviewed evidence on AI is thin (Md Momen Shahriar, 2026; Md Saddam, 2026; Md. Mainuddin, 2026). Across all domains, results are reported as predictive performance on historical or benchmark data; with the partial exception noted above, we found no study reporting what happened when a model was put to use (Sadia, 2026; Songeta, 2026).

Table 8: Empirical studies of artificial intelligence and statistical methods discussed in this review

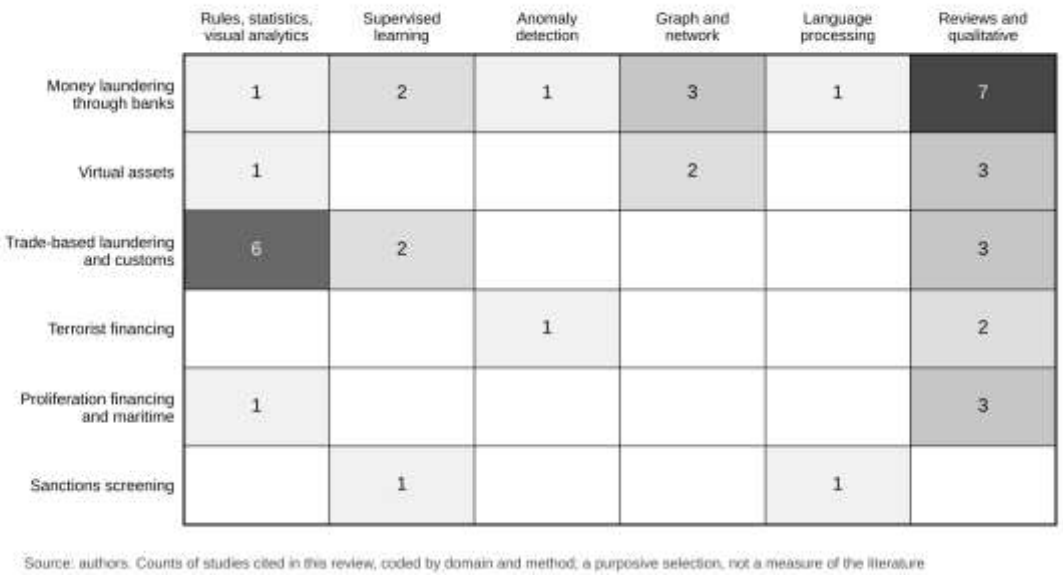
Study	Task and data	Method	Result as stated in the abstract or as we characterise it	Basis
Jullum et al. (2020)	Prioritising transactions for money laundering review; data from a large Norwegian bank	Supervised learning trained on normal transactions, alerts and reported cases	Outperformed the bank's existing approach on the authors' measure; excluding non-reported alerts or normal transactions from training was suboptimal	Abstract
Zhang & Trubey (2019)	Money laundering detection with rare events; a United States financial institution	Five learning algorithms under two schemes for over-representing the rare class	Potential advantages of machine learning for modelling such events	Abstract
Rocha-Salazar et al. (2021)	Suspicious transactions for money laundering and terrorism financing; a Mexican financial institution	Clustering, an abnormality indicator and neural networks	Fewer false positives and lower investigation cost than a rule-based system	Abstract

Study	Task and data	Method	Result as stated in the abstract or as we characterise it	Basis
Fronzetti Colladon & Remondi (2017)	Risk profiles of clients of a factoring company	Social network metrics	Network measures helped to identify higher-risk clients	Abstract
Drężewski et al. (2015)	Support for money laundering investigations	Social network analysis within an analyst system	Assigns roles to actors in a network built from financial records	Abstract
Cheng et al. (2023)	Detection of laundering groups in payment data	Group-aware deep graph learning	Reported improvement over baseline methods, in offline and online modes	Abstract
Lo et al. (2023); Alarab & Prakoonwit (2023)	Illicit transactions in a public labelled Bitcoin dataset	Self-supervised and temporal graph neural networks	Reported gains over earlier models on the same benchmark	Abstract
Alkhalili et al. (2021)	Watch-list filtering: deciding whether a name match is true	Support vector machine, decision tree, naive Bayes	Support vector machine performed best; aim was to reduce analysts' workload	Abstract
Kim & Yang (2024)	Sanctions screening of entities and transactions	Prototype natural language processing tool	More true matches found, but more false positives as well	Abstract
Vanhoeyveld et al. (2020)	Customs fraud detection under class imbalance	Learning from behavioural and high-cardinality data	Assessed the value of such data for detection	Title only
Barabesi et al. (2018)	Customs fraud detection	Tests of conformity with the Newcomb-Benford law	Statistical tests of conformity for customs data	Abstract
Chao et al. (2019)	Trade-based money laundering; data from China	Knowledge-driven multi-class classification	Monitoring method for recognising and classifying suspicious behaviour	Abstract
d'Afflisio et al. (2021)	Vessel tracking: spoofed or switched-off position signals	Statistical anomaly detection	Framework for detecting spoofing and stealth deviations, tested on simulated data	Abstract
Tasneem et al. (2026)	Summaries of financial-crime news by large language models	Identity-swap tests on three proprietary models	Small but statistically significant differences by demographic identity	Abstract

Table 9: Artificial intelligence by domain: data, uses and state of the evidence

Domain	Data available	Uses reported in the literature	State of the evidence, as we judge it	Sources
Money laundering through banks	Transactions, customer records, past alerts and reports	Alert ranking; anomaly detection; network analysis; visual analytics	Most developed. Several studies on real bank data; few report operational outcomes	Chen et al. (2018); Jullum et al. (2020); Jensen & Iosifidis (2023); Oztas et al. (2024); Singh & Best (2019)
Virtual assets	Public ledgers; a small number of labelled datasets	Graph learning on transaction networks; tracing	Active research on benchmark data; transfer to practice unclear	Foley et al. (2019); Lo et al. (2023); Alarab & Prakoonwit (2023); Akartuna et al. (2023)
Trade-based money laundering	Customs declarations, trade statistics, shipping records, trade finance documents	Price outliers; mirror statistics; customs fraud models; behaviour classification	Thin. Statistical screening established; few machine-learning studies address laundering as such	Zdanowicz (2009); Gara et al. (2019); Vanhoeyveld et al. (2020); Chao et al. (2019)
Terrorist financing	Same bank data; open-source and social media material	Combined money laundering and terrorism financing models	Thin. Few labelled cases; small sums; lawful sources	Rocha-Salazar et al. (2021); Canhoto (2021); Keatinge & Keen (2019)
Proliferation financing	Trade and shipping data; corporate registries; vessel tracking	Vessel anomaly detection; entity networks	Very thin in journals; methods exist in adjacent fields but are not evaluated for this purpose	Stewart et al. (2020); Wolsing et al. (2022); d'Afflisio et al. (2021)
Sanctions screening	Lists of designated persons; customer and payment names	Name matching; triage of matches	Emerging. Clear trade-off between missed and false matches	Kim & Yang (2024); Alkhalili et al. (2021)

Figure 6: Studies cited in this review by domain and method



Source: authors. Counts of studies cited in this review, coded by domain and method; a purposive selection, not a measure of the literature

SANCTIONS AS THE OPERATING CONTEXT: EVIDENCE AND CRITICISMS

Detection systems are means to the ends of the regimes they serve. Whether better detection matters depends on whether those regimes work and on what they cost.

Do sanctions work?

Table 10 summarises the studies discussed. Across the three purposes taken together, the datasets of the Targeted Sanctions Consortium assess United Nations targeted sanctions as effective 22% of the time in 63 episodes (Biersteker et al., 2018); we did not verify the breakdown by purpose. On coercion, the evidence is mixed and conditional. Large-sample studies find that multilateral sanctions succeed more often than unilateral ones (Bapat & Morgan, 2009), and reviews conclude that success depends on the goal sought, the costs imposed, the target's political system and the conduct of third parties (Drezner, 2024; Peksen, 2019). Targeting has not clearly made sanctions better at extracting concessions (Drezner, 2011). On constraint, the purpose most relevant to CFT and CPF, rigorous evidence outside that assessment is scarce, because what a group or programme would have done with unrestricted finance cannot be observed. The DPRK has continued to develop and test weapons under one of the most extensive regimes ever adopted, while paying a price in lost trade and in the cost and complexity of its procurement (Albright et al., 2010; Haggard & Noland, 2010). Whether that is failure or partial success depends on the purpose against which it is judged.

On the wider regime, assessments are sober. Reviewers find little reliable evidence that anti-money laundering and CFT controls have reduced crime or terrorist capability, and argue that the data needed to evaluate them do not exist (Levi, 2010; Levi & Reuter, 2006; Levi et al., 2018). Pol (2020) argued that only a very small fraction of criminal proceeds is recovered, at high compliance cost. A field experiment found that many corporate service providers, including in major financial centres, were willing to supply anonymous shell companies in breach of international standards (Findley et al., 2013). These findings set a limit on what detection can achieve: a model can rank cases well and still change little if the structures that conceal ownership remain available and if reports are not acted on.

Table 10: Selected findings on the effectiveness and costs of sanctions and of the wider regime

Question	Source	Finding as we characterise it
Do sanctions change behaviour?	Pape (1997)	Re-examined a widely used set of cases and judged that few were successes attributable to sanctions
	Baldwin (2000)	Argued that sanctions must be judged against the costs and prospects of the alternatives, not against an absolute standard
	Biersteker et al. (2018)	Datasets of 23 United Nations regimes and 63 episodes (1991 to 2013) assess targeted sanctions as effective 22% of the time, all purposes together
	Bapat & Morgan (2009)	Multilateral sanctions more often succeed than unilateral ones in a large dataset of threats and impositions
	Peksen (2019); Drezner (2024)	Reviews: success is conditional on goals, costs imposed, target regime and third-party behaviour; use has grown faster than evidence of effect
Are targeted measures better?	Drezner (2011); Gordon (2011); Portela (2016)	Targeting was intended to reduce harm to populations and does not remove it; it is not clearly more effective at winning concessions; some 'targeted' measures are broad in practice
Does financial leverage work?	Drezner (2015); Farrell & Newman (2019); Wertz (2013)	Centrality of a few currencies and institutions gives senders strong leverage over banks worldwide
	Morse (2019)	FATF listing leads market actors to penalise listed countries, which then adopt terrorist financing laws sooner
	McDowell (2021); Arnold (2016)	Leverage has costs: political risk attached to the sanctioning currency, and incentives to build alternatives

Question	Source	Finding as we characterise it
Are sanctions evaded?	Early (2009); Andreas (2005); Haggard & Noland (2010)	Third countries, including partners of the sender, replace lost trade; evasion builds criminal networks that outlast the sanctions; the target's trade shifts towards less restrictive partners
Does the AML and CFT regime work?	Levi & Reuter (2006); Levi et al. (2018); Pol (2020)	Little reliable evidence of effect on crime or on terrorist capability; data do not allow evaluation; very small share of criminal proceeds recovered
	Findley et al. (2013)	Field experiment: many corporate service providers offered anonymous companies without required identification
What are the human costs?	Neuenkirch & Neumeier (2015); Gutmann et al. (2021); Peksen (2009)	Sanctions episodes are associated with lower growth, shorter life expectancy and worse human rights conditions in target states
	Rodríguez et al. (2025)	Unilateral sanctions associated with higher mortality in a panel of 152 countries (1971 to 2021); no such association found for United Nations sanctions

Humanitarian effects

Table 11 collects the main criticisms and the responses to them. The first is that sanctions harm populations more than the leaders they are aimed at. Cross-national studies associate sanctions with lower economic growth (Neuenkirch & Neumeier, 2015), shorter life expectancy, with larger effects on women (Gutmann et al., 2021), and worse human rights conditions (Peksen, 2009). A 2025 panel study of 152 countries associated unilateral sanctions with about 564,000 deaths a year over 1971 to 2021 and found no statistically significant association for United Nations sanctions (Rodríguez et al., 2025). Earlier studies point the other way on that comparison: Gutmann et al. (2021) estimated a larger fall in life expectancy under United Nations than under United States sanctions, and Peksen (2009) found multilateral sanctions more damaging to human rights than unilateral ones. The literature does not agree on which kind does more harm. These are observational estimates; sanctioned states differ from others in ways, including conflict and misgovernment, that are hard to separate from the effect of sanctions. Defenders of sanctions add that responsibility for hardship is shared with the governments whose conduct led to the measures. Even targeted regimes have humanitarian effects, through their breadth in practice and through the caution of private firms (Gordon, 2011; Portela, 2016).

De-risking, over-compliance and due process

Because penalties are severe and rules complex, banks often withdraw from whole categories of business (correspondent relationships with small jurisdictions, money transfer operators, charities working in conflict zones) instead of assessing each customer. The result is financial exclusion and, plausibly, the movement of transactions into less visible channels (Arnold, 2016; Passas, 2006; Pavlidis, 2023); an early analysis linked customer due diligence rules to financial exclusion (de Koker, 2006). The FATF has said that wholesale de-risking is not what its standards require and revised Recommendation 8 in 2023 to discourage disproportionate treatment of non-profit organisations.

Individuals and entities are listed on the basis of information that is often confidential. The absence of independent review for those on the United Nations terrorism list drew sustained criticism and adverse court rulings in Europe (Heupel, 2009). The Council created the Office of the Ombudsperson in 2009 for what is now the ISIL and Al-Qaida list; other lists have only a focal point. A recent comparison of the counter-terrorism and counter-proliferation regimes concludes that legal protections have become more formal but remain unequal and lack independent judicial determination even where they are most developed (Birkett & Goldbarsht, 2026).

Legitimacy and system costs

States subject to autonomous sanctions, and many that are not, argue that they are applied selectively and that their extraterritorial reach compels third countries to follow policies they did not choose (Hofer, 2017). Senders reply that the Council is often blocked by the veto, that inaction in the face of proliferation or terrorism also has victims, and that no state is obliged to offer access to its markets and

currency. This article does not resolve the disagreement. Two observations can be made without taking sides. First, the events of 2024 to 2026 (the end of the DPRK panel, the dispute over Iran and the veto on its panel) show that the multilateral basis of CPF sanctions, on which the FATF standard relies, has weakened. Second, heavy use of financial leverage gives targets and bystanders an incentive to reduce their exposure to the sanctioning currency and institutions (Farrell & Newman, 2019; McDowell, 2021); how far this has gone is an empirical question on which evidence is still limited.

Table 11: Main criticisms of sanctions and the responses adopted or proposed

Criticism	Substance	Responses adopted or proposed
Humanitarian harm	Broad measures and over-compliance reduce imports of food and medicine and impede relief work	Targeting; standing humanitarian exemptions (resolutions 2664 and 2761); general licences; clearer guidance to banks
De-risking and financial exclusion	Banks withdraw from correspondent relationships, remittance corridors and charities instead of managing risk	Risk-based approach applied proportionately; revision of FATF Recommendation 8 (2023); supervisory statements that wholesale exit is not required
Displacement	Regulation of banks pushes flows into trade, informal value transfer, cash and virtual assets	Extend coverage to trade data and virtual assets; cooperation between customs, financial intelligence units and banks
Defensive over-reporting	Fear of penalties produces reports with little information value	Feedback to reporting entities; penalties proportionate to fault; public-private information sharing
Due process	Individuals listed on confidential evidence with limited review	Office of the Ombudsperson for the ISIL and Al-Qaida list; focal point for other lists; judicial review in regional and national courts
Legitimacy of unilateral and secondary sanctions	Many states regard measures without Council authorisation, and their extraterritorial reach, as contrary to international law; senders regard them as lawful policy	No agreed resolution; recurrent General Assembly and Human Rights Council debate; blocking statutes; alternative payment arrangements
Selectivity and politicisation	Listing and delisting reflect the interests of powerful states; monitoring depends on consensus that can break down	Transparent criteria; independent expert monitoring; regular review and termination clauses
Weak evidence base	Outputs (laws passed, reports filed, assets frozen) are counted; outcomes are rarely measured	Outcome-based evaluation; access for researchers to administrative data

RISKS AND GOVERNANCE OF ARTIFICIAL INTELLIGENCE IN THIS FIELD

The criticisms of sanctions and of the wider regime do not disappear when detection is automated. Some may be eased and some made worse. Table 12 sets out the risks and the safeguards discussed in the literature.

Explainability

Decisions in this field have consequences: an account is closed, a payment is blocked, a report is sent to the authorities, a name is proposed for designation. Those who take such decisions must be able to give reasons. Rudin (2019) argued that in high-stakes settings interpretable models should be preferred to opaque models explained after the fact, where they perform as well. Explanation methods based on Shapley values are widely used with tree-based models (Lundberg et al., 2020), and a critical review of deep learning for money laundering detection gives explainability a central place (Kute et al., 2021). Bertrand et al. (2021) examined AI-based anti-money laundering systems against European

fundamental rights; according to their abstract, the case law of the Court of Justice raises serious questions about the compatibility of such systems with data-protection law and the Charter, and anti-money laundering law would need substantial modification if machine-learning tools are introduced.

Bias, proxies and unequal burdens

Models learn from labels, and labels in this field reflect past practice. If reports were filed more readily on customers of certain nationalities, regions or occupations, a model trained on them will rank such customers higher. Evidence from another sector shows how an algorithm built on an administrative proxy reproduced a racial disparity that its designers did not intend (Obermeyer et al., 2019). In sanctions screening the burden of false matches falls on people whose names resemble listed names, which is not evenly distributed across populations. The study of language-model summaries by Tasneem et al. (2026) is an early indication that generative tools need the same scrutiny. The critical literature on algorithmic security makes the general point that suspicion assigned by association is hard for the person concerned to contest (Amoore, 2009).

Automation and de-risking

AI could reduce de-risking. A bank that can assess customers individually and cheaply has less reason to exit a whole category, and fewer false positives mean fewer delayed payments for legitimate customers and charities. It could also increase it. A model tuned to avoid any missed case, because missed cases are what regulators punish, will exclude more people, and will do so in a way that is harder to see than a published policy. Which effect dominates depends on the costs written into the model's objective and on what supervisors reward. We found no empirical study of the question, which is a gap of practical importance given the documented concerns about de-risking and financial exclusion (de Koker, 2006; Pavlidis, 2023).

Adaptation, drift and evaluation

Offenders respond to controls (Hataley, 2020; Unger & den Hertog, 2012). A deployed model changes the behaviour it was trained on, so performance measured on past data overstates future performance, and models need monitoring and retraining. Evaluation is the weakest part of the literature reviewed. Performance is reported on private data or on a single public benchmark, comparison with simple baselines is not routine, and outcomes (reports that led to investigations, assets frozen, evasion disrupted) are almost never reported. This repeats, for the tools, the criticism that has long been made of the regime as a whole (Levi et al., 2018; Pol, 2020).

Privacy, data sharing and due process

Detection improves when data on many people, almost all of them innocent, are pooled across institutions and borders. That conflicts with data-protection law and with commercial confidentiality, which is the motive for privacy-preserving methods (Bashir et al., 2026). It also raises the questions of compatibility with fundamental rights examined by Bertrand et al. (2021). Finally, algorithmic output may feed decisions against which there is little recourse. If the legal protections available to persons listed by the Security Council are uneven (Birkett & Goldbarsht, 2026; Heupel, 2009), those available to a customer whose account is closed after a model score are weaker still. Keeping consequential decisions with accountable humans, recording reasons and providing review are safeguards that do not depend on the choice of algorithm.

Standards and regulation

The FATF published a report on the opportunities and challenges of new technologies for anti-money laundering and CFT in 2021, which encouraged responsible use while noting explainability, data quality and data-protection constraints; we describe it from our knowledge of the document and did not re-read it. General AI regulation, such as the European Union's Artificial Intelligence Act of 2024, sets obligations for systems classed as high-risk. Whether a particular compliance tool falls within such a class depends on its use, which we did not analyse, and the dates from which the high-risk obligations apply were reportedly deferred in 2026, which we did not verify in the Official Journal. Supervisors' expectations for model risk management apply to detection models as to other models.

Table 12: Risks of artificial intelligence in the control of illicit finance and safeguards discussed

Risk	Why it arises	Safeguards discussed in the literature
Opacity	Complex models cannot give reasons that an analyst, a customer or a court can test	Prefer interpretable models where they perform as well; explanation methods; documentation
Bias and unequal burden	Labels reflect past reporting; names, nationality and geography act as proxies	Testing of error rates across groups; review of features; human review of adverse decisions
Feedback and label bias	Models learn what was reported before, not what was unlawful	Use of confirmed outcomes; sampling of unflagged cases; feedback from authorities
Adaptation by offenders	Offenders change behaviour in response to controls	Retraining; monitoring for drift; combination of rules, models and investigation
Automation of over-compliance	Models tuned to avoid any miss may exclude whole groups of customers	Explicit cost of false positives in model objectives; supervisory guidance against wholesale exit
Privacy and data protection	Detection improves with pooled data on many innocent people	Proportionality assessment; data minimisation; privacy-preserving computation
Due process in listing and freezing	Algorithmic output may feed designations or account closures without reasons	Reasons and review for affected persons; keeping decisions with accountable humans
Weak evaluation	Results reported on private or benchmark data, by accuracy alone	Out-of-time tests; comparison with simple baselines; reporting of yield per case reviewed

DISCUSSION AND CONCLUSIONS

Answers to the research questions

RQ1. TBML, terrorist financing and proliferation financing are distinct. Laundering conceals the origin of criminal money; terrorist financing conceals the destination of money that may be lawful; proliferation financing conceals the end use of payments that look like ordinary trade and the origin of revenue earned in breach of sanctions. TBML is a method that serves all three. The framework has two pillars, binding Security Council decisions and FATF standards enforced by peer review and listing; since 2024 the first has been strained in the area of proliferation. Sanctions in this field are meant mainly to constrain and to signal, and to coerce only in state-directed cases.

RQ2. Seven families of methods have been applied: rules and scenarios; supervised learning; unsupervised and anomaly detection; network and graph learning; natural language processing; privacy-preserving learning; and generative models. They serve a small number of tasks: ranking alerts, finding outliers, discovering networks, matching names and tracing flows.

RQ3. The evidence is uneven. It is most developed for money laundering through banks and for virtual assets. For TBML, statistical screening of prices and mirror data is established and machine learning has addressed customs fraud more than laundering. For terrorist financing, proliferation financing and sanctions screening, peer-reviewed evaluation of AI is thin. Reported results are predictive performance on historical data; operational outcomes are almost never reported.

RQ4. Sanctions impose costs and sometimes contribute to changes of policy, more often when multilateral; evidence that they disrupt terrorist or proliferation finance is largely indirect; evasion is routine and adaptive. Humanitarian harm, de-risking, weak due process and contested legitimacy are documented costs.

RQ5. AI brings risks of opacity, bias, feedback from past practice, adaptation by offenders, automated over-compliance, intrusion on privacy and weak evaluation. Safeguards are known and are mostly organisational.

A mismatch between where AI is strong and where the need is greatest

The central observation of this review is a mismatch. The policy concern expressed through sanctions is greatest for proliferation and terrorist financing and for evasion through trade. AI research is strongest where data are plentiful and labels exist. The mismatch is explained by data, not by a lack of algorithms. Bank transactions are held by one institution in structured form, and public blockchains are open. Trade data are divided among customs, carriers, banks and registries in different countries; confirmed cases of TBML and proliferation financing are few and often classified; and the public sources of case material, the United Nations expert panels, have been reduced. It follows that the first investment needed in these domains is in data: linkage, quality, lawful gateways for sharing and feedback from investigations. Complex models come after.

Detection serves a purpose

A second observation links the two halves of the review. A detection system has no value apart from the regime it serves. If the purpose of a designation is to constrain, the relevant measure for a screening or monitoring tool is whether designated actors and their fronts find it harder and costlier to move money, not how many alerts were closed. If humanitarian exemptions are to work, tools must be able to recognise exempt transactions instead of blocking them by default. Stating the purpose of each sanctions measure, as the sanctions literature recommends, would also tell the designers of models what to optimise and what harm to avoid. None of this settles whether a given regime is justified, which involves judgements about the gravity of the threat and the alternatives on which reasonable people and states differ.

Propositions for policy and research

Table 13 sets out nine propositions. They are offered as matters for debate, and several involve trade-offs. Wider data sharing raises privacy and confidentiality concerns. Interpretable models may give up some predictive performance. Pricing false positives requires supervisors to accept that some risk will be taken. For research, the priorities are evaluation of outcomes, for which access to administrative data is needed (Levi et al., 2018); studies of AI for TBML, terrorist financing and proliferation financing on real data; study of whether automation reduces or increases de-risking; and independent evaluation of generative tools before they are relied on.

Table 13: Propositions for policy and research

Area	Proposition
Define the purpose	State for each sanctions measure whether it is meant to coerce, constrain or signal, and for each model which decision it supports; assess both against that purpose
Start from the data, not the algorithm	Join customs, shipping, registry and payment data before investing in complex models; the trade channel is where data are most fragmented
Treat proliferation financing as a network problem	Use entity resolution and graph methods to look beyond designated names, with human analysis of the results
Price false positives	Give missed matches and false matches explicit costs, so that models do not automate de-risking
Keep baselines and test over time	Compare every model with rules and simple statistics on later data; publish negative results
Explain and allow challenge	Use interpretable models where they perform as well, record reasons, and give affected persons a route of review
Share safely	Develop privacy-preserving methods and legal gateways for sharing between institutions and across borders
Preserve multilateral monitoring and humanitarian safeguards	Restore or replace independent expert reporting where it has lapsed; make exemptions usable in practice
Measure outcomes	Report disruption, cost imposed and side effects, and open administrative data to independent evaluation

Limitations

This article has important limitations. (1) It is a narrative review. The policy literature was chosen purposively, and the AI literature was found by title searches in one open index, ordered by citation count and screened by one reviewer, a language-model tool, without a recorded protocol. Relevant work has certainly been missed, in particular conference papers, which carry much of the machine-learning literature, preprints, work not in English and reports of international organisations and research institutes, none of which are cited. The statement that evidence in a domain is thin means thin among journal articles found in this way. (2) The descriptions of what the cited articles argue and find were drafted by a language-model tool. For 63 of the 100 articles they were compared with the abstract, as returned in paraphrase by a retrieval tool, by an independent checking agent; for the others they rest on the tool's knowledge or, where marked, on the title. Full texts were not read. Each characterisation should be confirmed in the original before it is relied on. (3) The coding of studies by domain and method in Figure 6 was done once by the same tool; it covers 39 of the studies cited here, two of them in two cells, and leaves out general methodological and legal references. (4) Official instruments are described from their text as we know it and were not re-read line by line. (5) Current facts were checked on a single day against web sources, some of them secondary or press reports; the FATF's own pages could not be retrieved. (6) The article presents no new data, tests no model and makes no causal claims of its own. (7) On contested political questions we have tried to state the main positions fairly, but selection and wording involve judgement.

Conclusion

Artificial intelligence has been applied to illicit finance for two decades, and studies on real bank data report that learned models can rank suspicious activity better than existing rule-based monitoring, while studies on a public Bitcoin benchmark report successive gains over earlier models. The same cannot yet be said, on the published evidence we found, for trade-based money laundering, terrorist financing or proliferation financing, which are the areas that international sanctions are chiefly meant to address, nor is there published evidence of what these tools achieve once in use. Sanctions themselves have a stated rationale (to constrain and to signal without resort to force) for which the evidence is weaker than the scale of their use would suggest, with documented costs to civilians, to legitimate finance and to the rights of those listed. Better detection cannot repair a weak evidence base for the regime it serves, but it can reduce error in both directions if it is built on better data, kept explainable and contestable, and judged by outcomes. A use of sanctions and of AI that carries stated purposes, usable humanitarian safeguards, attention to the trade channel and independent evaluation would be consistent with what is known; whether sanctions should be used more or less is a judgement this review does not make.

REFERENCES

[1]. Ahmed, H. C. H. R. (2026). AI-Enabled IT and Supply Chain Resilience for Anticipating and Mitigating Critical Medical-Supply Disruptions in U.S. Healthcare Systems. *International Journal of Business and Economics Insights*, *16*(01), 01–42. https://doi.org/10.63125/dhdew369

[2]. Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy delphi study. *Technological Forecasting and Social Change*, *179*, 121632. https://doi.org/10.1016/j.techfore.2022.121632

[3]. Akartuna, E. A., Johnson, S. D., & Thornton, A. E. (2023). The money laundering and terrorist financing risks of new and disruptive technologies: A futures-oriented scoping review. *Security Journal*, *36*(4), 615-650. https://doi.org/10.1057/s41284-022-00356-z

[4]. Akoglu, L., Tong, H., & Koutra, D. (2015). Graph based anomaly detection and description: A survey. *Data Mining and Knowledge Discovery*, *29*(3), 626-688. https://doi.org/10.1007/s10618-014-0365-y

[5]. Alarab, I., & Prakoonwit, S. (2023). Graph-based LSTM for anti-money laundering: Experimenting temporal graph convolutional network with bitcoin data. *Neural Processing Letters*, *55*(1), 689-707. https://doi.org/10.1007/s11063-022-10904-8

[6]. Albright, D., Brannan, P., & Stricker, A. S. (2010). Detecting and disrupting illicit nuclear trade after A.Q. Khan. *The Washington Quarterly*, *33*(2), 85-106. https://doi.org/10.1080/01636601003673857

[7]. Alkhalili, M., Qutqut, M. H., & Almasalha, F. (2021). Investigation of applying machine learning for watch-list filtering in anti-money laundering. *IEEE Access*, *9*, 18481-18496. https://doi.org/10.1109/access.2021.3052313

[8]. Aminul Islam, M. (2025). Calibrated Machine Learning for Reducing Decision Risk and Improving Forecast Reliability in U.S. Enterprise Analytics. *American Journal of Interdisciplinary Studies*, *15*(12), 01-36. https://doi.org/10.63125/869qdj55

[9]. Aminul Islam, M., & Md, A. (2023). Adaptive Class-Imbalance Learning for High-Sensitivity Fraud Detection in Large-Scale Digital Transaction Networks. *International Journal of Business and Economics Insights*, *13*(09), 01-33. https://doi.org/10.63125/bmxwv741

[10]. Amoore, L. (2009). Algorithmic war: Everyday geographies of the war on terror. *Antipode*, *41*(1), 49-69. https://doi.org/10.1111/j.1467-8330.2008.00655.x

[11]. Andreas, P. (2005). Criminalizing consequences of sanctions: Embargo busting and its legacy. *International Studies Quarterly*, *49*(2), 335-360. https://doi.org/10.1111/j.0020-8833.2005.00347.x

[12]. Arnold, A. (2016). The true costs of financial sanctions. *Survival*, *58*(3), 77-100. https://doi.org/10.1080/00396338.2016.1186981

[13]. Asheke, M. (2025). Artificial Intelligence Driven Supply Chain Risk Forecasting and Optimization for Resilient Industrial Production Networks. *ASRC Procedia: Global Perspectives in Science and Scholarship*, *1*(01), 2923–2960. https://doi.org/10.63125/rapn5860

[14]. Asheke, M. (2026). Intelligence Driven Project Risk Prediction and Resource Optimization for Complex Engineering and Manufacturing Projects. *American Journal of Data Science and Analytics*, *7*(10), 126-164. https://doi.org/10.63125/hv05m379

[15]. Asheke, M., & Tashriq Ahmed Bin, A. (2022). Federated Learning and Differential Privacy for Cross-Firm Construction-Materials Supply-Chain Disruption Forecasting: A Quantitative Analysis of Privacy-Utility Trade-Offs. *American Journal of Advanced Technology and Engineering Solutions*, *12*(09), 01-40. https://doi.org/10.63125/g4at4237

[16]. Ashik, M. (2025). PRISMA-Based Systematic Literature Review of Reliability-Centered Turnaround Planning for Reducing Downtime in Power Generation Facilities. *American Journal of Scholarly Research and Innovation*, *4*(01), 1036–1080. https://doi.org/10.63125/2878n718

[17]. Ashik, M. (2026). RCM and PSM Strategies for Strengthening Asset Integrity Across U.S. Energy Facilities: A Systematic Meta-Analysis. *American Journal of Interdisciplinary Studies*, *16*(06), 38-81. https://doi.org/10.63125/p87z7q36

[18]. Bakhos Douaihy, H., & Rowe, F. (2023). Institutional pressures and RegTech challenges for banking: The case of money laundering and terrorist financing in Lebanon. *Journal of Information Technology*, *38*(3), 304-318. https://doi.org/10.1177/02683962231152968

[19]. Baldwin, D. A. (2000). The sanctions debate and the logic of choice. *International Security*, *24*(3), 80-107. https://doi.org/10.1162/016228899560248

[20]. Bapat, N. A., & Morgan, T. C. (2009). Multilateral versus unilateral sanctions reconsidered: A test using new data. *International Studies Quarterly*, *53*(4), 1075-1094. https://doi.org/10.1111/j.1468-2478.2009.00569.x

[21]. Barabesi, L., Cerasa, A., Cerioli, A., & Perrotta, D. (2018). Goodness-of-fit testing for the Newcomb-Benford law with application to the detection of customs fraud. *Journal of Business & Economic Statistics*, *36*(2), 346-358. https://doi.org/10.1080/07350015.2016.1172014

[22]. Bashir, Z., Verma, M., & Krishna Mohan, C. (2026). Hybrid federated continual graph contrastive learning for evolving money laundering threats. *Data Mining and Knowledge Discovery*, *40*(2), 19. https://doi.org/10.1007/s10618-026-01192-0

[23]. Basile, M. (2004). Going to the source: Why Al Qaeda's financial network is likely to withstand the current war on terrorist financing. *Studies in Conflict & Terrorism*, *27*(3), 169-185. https://doi.org/10.1080/10576100490438237

[24]. Bertrand, A., Maxwell, W., & Vamparys, X. (2021). Do AI-based anti-money laundering (AML) systems violate European fundamental rights? *International Data Privacy Law*, *11*(3), 276-293. https://doi.org/10.1093/idpl/ipab010

[25]. Biersteker, T. J., Eckert, S. E., Tourinho, M., & Hudáková, Z. (2018). UN targeted sanctions datasets (1991–2013). *Journal of Peace Research*, *55*(3), 404-412. https://doi.org/10.1177/0022343317752539

[26]. Birkett, D. J., & Goldbarsht, D. (2026). Formalised yet uneven: Legal protections in United Nations Security Council counter-terrorism and counter-proliferation financing sanctions regimes. *Journal of Money Laundering Control*, *29*(4-5), 186-199. https://doi.org/10.1108/jmlc-02-2026-0031

[27]. Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, *17*(3), 235-255. https://doi.org/10.1214/ss/1042727940

[28]. Canhoto, A. I. (2021). Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research*, *131*, 441-452. https://doi.org/10.1016/j.jbusres.2020.10.012

[29]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *41*(3), 1-58. https://doi.org/10.1145/1541880.1541882

[30]. Chao, X., Kou, G., Peng, Y., & Alsaadi, F. E. (2019). Behavior monitoring methods for trade-based money laundering integrating macro and micro prudential regulation: A case from China. *Technological and Economic Development of Economy*, *25*(6), 1081-1096. https://doi.org/10.3846/tede.2019.9383

[31]. Chen, Z., Van Khoa, L. D., Teoh, E. N., Nazir, A., Karuppiah, E. K., & Lam, K. S. (2018). Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review. *Knowledge and Information Systems*, *57*(2), 245-285. https://doi.org/10.1007/s10115-017-1144-z

[32]. Cheng, D., Ye, Y., Xiang, S., Ma, Z., Zhang, Y., & Jiang, C. (2023). Anti-Money laundering by group-aware deep graph learning. *IEEE Transactions on Knowledge and Data Engineering*, *35*(12), 12444-12457. https://doi.org/10.1109/tkde.2023.3272396

[33]. Clunan, A. L. (2006). The fight against terrorist financing. *Political Science Quarterly*, *121*(4), 569-596. https://doi.org/10.1002/j.1538-165x.2006.tb00582.x

[34]. d'Afflisio, E., Braca, P., & Willett, P. (2021). Malicious AIS spoofing and abnormal stealth deviations: A comprehensive statistical framework for maritime anomaly detection. *IEEE Transactions on Aerospace and Electronic Systems*, *57*(4), 2093-2108. https://doi.org/10.1109/taes.2021.3083466

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

[36]. Dreżewski, R., Sepielak, J., & Filipkowski, W. (2015). The application of social network analysis algorithms in a system supporting money laundering detection. *Information Sciences*, *295*, 18-32. https://doi.org/10.1016/j.ins.2014.10.015

[37]. Drezner, D. W. (2011). Sanctions sometimes smart: Targeted sanctions in theory and practice. *International Studies Review*, *13*(1), 96-108. https://doi.org/10.1111/j.1468-2486.2010.01001.x

[38]. Drezner, D. W. (2015). Targeted sanctions in a world of global finance. *International Interactions*, *41*(4), 755-764. https://doi.org/10.1080/03050629.2015.1041297

[39]. Drezner, D. W. (2024). Global economic sanctions. *Annual Review of Political Science*, *27*(1), 9-24. https://doi.org/10.1146/annurev-polisci-041322-032240

[40]. Early, B. R. (2009). Sleeping with your friends' enemies: An explanation of sanctions-busting trade. *International Studies Quarterly*, *53*(1), 49-71. https://doi.org/10.1111/j.1468-2478.2008.01523.x

[41]. Early, B. R., & Preble, K. A. (2020). Going fishing versus hunting whales: Explaining changes in how the US enforces economic sanctions. *Security Studies*, *29*(2), 231-267. https://doi.org/10.1080/09636412.2020.1722850

[42]. Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42-79. https://doi.org/10.1162/isec_a_00351

[43]. Felbermayr, G., Kirilakha, A., Syropoulos, C., Yalcin, E., & Yotov, Y. V. (2020). The global sanctions data base. *European Economic Review*, *129*, 103561. https://doi.org/10.1016/j.euroecorev.2020.103561

[44]. Ferwerda, J., Kattenberg, M., Chang, H.-H., Unger, B., Groot, L., & Bikker, J. A. (2013). Gravity models of trade-based money laundering. *Applied Economics*, *45*(22), 3170-3182. https://doi.org/10.1080/00036846.2012.699190

[45]. Findley, M. G., Nielson, D. L., & Sharman, J. C. (2013). Using field experiments in international relations: A randomized study of anonymous incorporation. *International Organization*, *67*(4), 657-693. https://doi.org/10.1017/s0020818313000271

[46]. Fisman, R., & Wei, S.-J. (2004). Tax rates and tax evasion: Evidence from "missing imports" in China. *Journal of Political Economy*, *112*(2), 471-496. https://doi.org/10.1086/381476

[47]. Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *The Review of Financial Studies*, *32*(5), 1798-1853. https://doi.org/10.1093/rfs/hhz015

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

[49]. Fronzetti Colladon, A., & Remondi, E. (2017). Using social network analysis to prevent money laundering. *Expert Systems with Applications*, *67*, 49-58. https://doi.org/10.1016/j.eswa.2016.09.029

[50]. Galtung, J. (1967). On the effects of international economic sanctions, with examples from the case of Rhodesia. *World Politics*, *19*(3), 378-416. https://doi.org/10.2307/2009785

[51]. Gao, Z., & Ye, M. (2007). A framework for data mining-based anti-money laundering research. *Journal of Money Laundering Control*, *10*(2), 170-179. https://doi.org/10.1108/13685200710746875

[52]. Gara, M., Giammatteo, M., & Tosti, E. (2019). Magic mirror in my hand … how trade mirror statistics can help us detect illegal financial flows. *The World Economy*, *42*(11), 3120-3147. https://doi.org/10.1111/twec.12840

[53]. Gazi Yeasin, A. (2024a). Designing Trustworthy AI Output Interfaces: A UX Framework for Graceful Handling of Generative Model Uncertainty in Consumer Applications. *American Journal of Scholarly Research and Innovation*, *14*(07), 01–40. https://doi.org/10.63125/4m5fjb12

[54]. Gazi Yeasin, A. (2024b). A Quantitative Evaluation of Behavioral Design Patterns on User Engagement and Activation in Large-Scale Campus Software Products. *American Journal of Interdisciplinary Studies*, *14*(06), 01-40. https://doi.org/10.63125/x3d5k517

[55]. Gazi Yeasin, A. (2026). An AI-Integrated Multi-Agent Product Development Pipeline for Autonomous Design-To-Production Software Delivery: Architecture and Evaluation. *International Journal of Scientific Interdisciplinary Research*, *7*(1), 632-676. https://doi.org/10.63125/bq24tw25

[56]. Gordon, J. (2011). Smart sanctions revisited. *Ethics & International Affairs*, *25*(3), 315-335. https://doi.org/10.1017/s0892679411000323

[57]. Gutmann, J., Neuenkirch, M., & Neumeier, F. (2021). Sanctioned to death? The impact of economic sanctions on life expectancy and its gender gap. *The Journal of Development Studies*, *57*(1), 139-162. https://doi.org/10.1080/00220388.2020.1746277

[58]. Haggard, S., & Noland, M. (2010). Sanctioning North Korea: The political economy of denuclearization and proliferation. *Asian Survey*, *50*(3), 539-568. https://doi.org/10.1525/as.2010.50.3.539

[59]. Han, J., Huang, Y., Liu, S., & Towey, K. (2020). Artificial intelligence for anti-money laundering: A review and extension. *Digital Finance*, *2*(3-4), 211-239. https://doi.org/10.1007/s42521-020-00023-1

[60]. Hataley, T. (2020). Trade-based money laundering: Organized crime, learning and international trade. *Journal of Money Laundering Control*, *23*(3), 651-661. https://doi.org/10.1108/jmlc-01-2020-0004

[61]. He, H., & Garcia, E. A. (2009). Learning from imbalanced data. *IEEE Transactions on Knowledge and Data Engineering*, *21*(9), 1263-1284. https://doi.org/10.1109/tkde.2008.239

[62]. Heupel, M. (2009). Multilateral sanctions against terror suspects and the violation of due process standards. *International Affairs*, *85*(2), 307-321. https://doi.org/10.1111/j.1468-2346.2009.00795.x

[63]. Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, *193*, 116429. https://doi.org/10.1016/j.eswa.2021.116429

[64]. Hofer, A. (2017). The developed/developing divide on unilateral coercive measures: Legitimate enforcement or illegitimate intervention? *Chinese Journal of International Law*, *16*(2), 175-214. https://doi.org/10.1093/chinesejil/jmx018

[65]. Jensen, R. I. T., & Iosifidis, A. (2023). Fighting money laundering with statistics and machine learning. *IEEE Access*, *11*, 8889-8903. https://doi.org/10.1109/access.2023.3239549

[66]. Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control*, *23*(1), 173-186. https://doi.org/10.1108/jmlc-07-2019-0055

[67]. Kazi Mohammad Khalid, A., & Sumaiya Sadmeen, M. (2022). Geospatial Artificial Intelligence for Urban Flood Susceptibility and Drainage Resilience: A Prisma 2020 Systematic Review and Bibliometric Meta-Synthesis. *Review of Applied Science and Technology*, *12*(02), 01–51. https://doi.org/10.63125/epqdvy23

[68]. Keatinge, T., & Keen, F. (2019). Social media and (counter) terrorist finance: A fund-raising and disruption tool. *Studies in Conflict & Terrorism*, *42*(1-2), 178-205. https://doi.org/10.1080/1057610x.2018.1513698

[69]. Kim, S., & Yang, S. (2024). Accuracy improvement in financial sanction screening: Is natural language processing the solution? *Frontiers in Artificial Intelligence*, *7*, 1374323. https://doi.org/10.3389/frai.2024.1374323

[70]. Kute, D. V., Pradhan, B., Shukla, N., & Alamri, A. (2021). Deep learning and explainable artificial intelligence techniques applied for detecting money laundering: A critical review. *IEEE Access*, *9*, 82300-82317. https://doi.org/10.1109/access.2021.3086230

[71]. Kynatun, M. (2025). Integrating AI-Driven Security Analytics and IT Governance Frameworks for Cybersecurity Decision Support in U.S. Financial Information Systems. *American Journal of Advanced Technology and Engineering Solutions*, *15*(12), 01-42. https://doi.org/10.63125/kzcdyz73

[72]. Kynatun, M. (2026). Artificial Intelligence Integrated MIS Framework for Proactive Cyber Threat Intelligence and Organizational Security Resilience. *American Journal of Scholarly Research and Innovation*, *16*(09), 40–78. https://doi.org/10.63125/t98tc495

[73]. Levi, M. (2010). Combating the financing of terrorism: A history and assessment of the control of 'threat finance'. *British Journal of Criminology*, *50*(4), 650-669. https://doi.org/10.1093/bjc/azq025

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

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

[76]. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2012). Isolation-based anomaly detection. *ACM Transactions on Knowledge Discovery from Data*, *6*(1), 1-39. https://doi.org/10.1145/2133360.2133363

[77]. Lo, W. W., Kulatilleke, G. K., Sarhan, M., Layeghy, S., & Portmann, M. (2023). Inspection-L: Self-supervised GNN node embeddings for money laundering detection in bitcoin. *Applied Intelligence*, *53*(16), 19406-19417. https://doi.org/10.1007/s10489-023-04504-9

[78]. Lundberg, S. M., Erion, G., Chen, H., DeGrave, A., Prutkin, J. M., Nair, B., Katz, R., Himmelfarb, J., Bansal, N., & Lee, S.-I. (2020). From local explanations to global understanding with explainable AI for trees. *Nature Machine Intelligence*, *2*(1), 56-67. https://doi.org/10.1038/s42256-019-0138-9

[79]. Maishar Mostari, Z. (2024). Uncertainty-Calibrated Explainable AI for Cybersecurity Alert Prioritization: Improving Detection Reliability and Human Decision-Making. *American Journal of Scholarly Research and Innovation*, *14*(12), 01–40. https://doi.org/10.63125/an0pcq39

[80]. Maishar Mostari, Z. (2025). Privacy-Preserving AI-Based Cyber Threat Detection in Financial Organizations: A Governance and Business Value Framework. *American Journal of Interdisciplinary Studies*, *15*(04), 01-51. https://doi.org/10.63125/p8fct530

[81]. Maishar Mostari, Z. (2026). A Systematic Review of Machine Learning Applications in Cybersecurity Threat Detection and Classification (2018–2026). *American Journal of Data Science and Analytics*, *7*(06), 640-680. https://doi.org/10.63125/6kg7kg75

[82]. Mashfiqur, R. (2024). Anomaly Detection and Process Mining for Identifying Financial Irregularities and Strengthening Procurement Controls. *American Journal of Advanced Technology and Engineering Solutions*, *14*(09), 91-140. https://doi.org/10.63125/hmg5ta84

[83]. Mashfiqur, R., & Md Jamil, A. (2023). Machine Learning-Based Cost Variance Prediction for Early Detection of Budget Overruns in Procurement-Intensive Operations. *Review of Applied Science and Technology*, *13*(12), 142–199. https://doi.org/10.63125/7g92wd03

[84]. Masrul, H. (2025). Explainable Machine Learning for Real-Time Financial Fraud Detection and Risk-Based Transaction Monitoring in U.S. Banking and Digital Payment Systems. *American Journal of Data Science and Analytics*, *6*(10), 70-108. https://doi.org/10.63125/4h9v1876

[85]. Masrul, H., & Mashfiqur, R. (2024). Unified Analytical Modeling for Cryptocurrency Price Volatility Forecasting and Market-Manipulation Detection in U.S. Digital Asset Markets. *American Journal of Advanced Technology and Engineering Solutions*, *14*(11), 01-40. https://doi.org/10.63125/nqgh7934

[86]. Masrul, H., & Mukut Kanti, B. (2024). AI-Driven Project Portfolio and Business Analytics for Forecasting Cost Overruns, Schedule Delays, Resource Bottlenecks, and Enterprise Performance Across U.S. Industries. *Review of Applied Science and Technology*, *14*(12), 14–54. https://doi.org/10.63125/x7te4644

[87]. McDowell, D. (2021). Financial sanctions and political risk in the international currency system. *Review of International Political Economy*, *28*(3), 635-661. https://doi.org/10.1080/09692290.2020.1736126

[88]. McSkimming, S. (2010). Trade-based money laundering: Responding to an emerging threat. *Deakin Law Review*, *15*(1), 37. https://doi.org/10.21153/dlr2010vol15no1art116

[89]. Md, F., & Kynatun, M. (2023). A Quantitative Assessment of Cybersecurity Risk Scoring Models for Enterprise Database Systems in Cloud-Native Environments. *Review of Applied Science and Technology*, *13*(12), 50–103. https://doi.org/10.63125/gk2krm47

[90]. Md Hasinur, R. (2024). Human in the Loop Artificial Intelligence for Loan Document Verification and Credit Risk Reporting: A Bibliometric and Science Mapping Analysis. *American Journal of Interdisciplinary Studies*, *14*(06), 41-71. https://doi.org/10.63125/8x359j95

[91]. Md Hasinur, R. (2025a). Machine Learning for Nonperforming Corporate Loan Recovery: A Systematic Review and Meta-Analysis of Predictive Performance. *American Journal of Scholarly Research and Innovation*, *4*(01), 1174–1202. https://doi.org/10.63125/a7v6f533

[92]. Md Hasinur, R. (2025b). Present and Future of Digital Banking Services in Bangladesh. *Review of Applied Science and Technology*, *4*(02), 725-749. https://doi.org/10.63125/k7tgr183

[93]. Md Hasinur, R. (2026). Explainable Machine Learning for Loan-Delinquency Prediction in U.S. Community Banks: A Quantitative Study Using Gradient Boosting and SHAP. *American Journal of Data Science and Analytics*, *7*(01), 280-316. https://doi.org/10.63125/mfv3c059

[94]. Md Maksudul, H. (2024). Supplier-Risk Scoring and Procurement Resilience for Distributed Athletic-Apparel and Equipment Supply Networks. *American Journal of Advanced Technology and Engineering Solutions*, *14*(09), 44-90. https://doi.org/10.63125/a9fmgj50

[95]. Md Maksudul, H. (2025). Data-Driven Fulfillment Optimization for Time-Sensitive Teamwear and Sporting Goods Distribution. *American Journal of Scholarly Research and Innovation*, *4*(01), 1120–1173. https://doi.org/10.63125/rpezfz61

[96]. Md Maksudul, H. (2026). Generative AI Decision Support for Procurement, Inventory, And Operational Planning in U.S. Sports Businesses. *American Journal of Interdisciplinary Studies*, *16*(04), 01-55. https://doi.org/10.63125/ngtzw226

[97]. Md Maksudul, H., & Md Takbir Hossen, S. (2023). Predictive Inventory Optimization for Reducing Stockouts and Excess Inventory in U.S. Sports and Apparel Operations. *Review of Applied Science and Technology*, *13*(12), 104–141. https://doi.org/10.63125/8djn1j48

[98]. Md Maksudul, H., & Md Tazul Islam, C. (2022). Machine Learning-Based Cash-Flow Forecasting for Improving Financial Planning in U.S. Small and Mid-Sized Businesses. *International Journal of Scientific Interdisciplinary Research*, *12*(12), 01–38. https://doi.org/10.63125/w3pgjx97

[99]. Md Mohsin, B. (2024). Artificial Intelligence for Medication Safety and Nursing Documentation in Emergency Departments: A Bibliometric Analysis. *American Journal of Interdisciplinary Studies*, *14*(10), 01-34. https://doi.org/10.63125/2krdb618

[100]. Md Mohsin, B. (2026). Nurse-Led Triage Protocols in Emergency and Trauma Care: A PRISMA-Guided Systematic Review. *American Journal of Health and Medical Sciences*, *16*(09), 01–40. https://doi.org/10.63125/21k00924

[101]. Md Mohsin, B., & Jannatul, F. (2021). Emergency Nursing Triage and Timely Escalation of Care: A Quantitative Clinical Audit. *International Journal of Scientific Interdisciplinary Research*, *11*(07), 01–33. https://ijsir.org/index.php/IJSIR/article/view/138

[102]. Md Mohsin, B., & Mst Kaniz, F. (2023). AI-Enabled Clinical Decision Support for Standardized Nurse-Led Emergency Care Pathways: A Multisite Mixed-Methods Implementation Study. *Review of Applied Science and Technology*, *13*(08), 01–33. https://doi.org/10.63125/ac09sa31

[103]. Md Momen Shahriar, J. (2025). Viscoelastic Creep Characterization of LDPE Under Multilevel Stress and Temperature Using Time-Temperature Superposition and Constitutive Modeling. *American Journal of Scholarly Research and Innovation*, *15*(11), 01–38. https://doi.org/10.63125/2edstd86

[104]. Md Momen Shahriar, J. (2026). Physics-Informed Machine Learning for Long-Term Polymer Performance Prediction from Extrusion Parameters, Material Properties, and Creep Data. *American Journal of Interdisciplinary Studies*, *16*(05), 01-41. https://doi.org/10.63125/8gk5c668

[105]. Md Saddam, H. (2026). Explainable Machine Learning for Inventory Shrinkage and Stockout Prediction in U.S. Retail Supply Chains: A Quantitative Study using Gradient Boosting and SHAP. *American Journal of Advanced Technology and Engineering Solutions*, *16*(10), 01-29. https://doi.org/10.63125/6hzy9c10

[106]. Md Tazul Islam, C. (2024). Explainable AI For Financial and Operational Decision Support: Improving Transparency and Managerial Trust. *American Journal of Advanced Technology and Engineering Solutions*, *14*(12), 01-38. https://doi.org/10.63125/kwfvzw68

[107]. Md Tazul Islam, C. (2025). Business Intelligence and Data-Quality Frameworks for Improving Evidence-Based Decisions across Multi-Source Enterprise Data. *American Journal of Scholarly Research and Innovation*, *15*(07), 01–41. https://doi.org/10.63125/qhh6ka59

[108]. Md. Mainuddin, F. (2024). Quantitative Structural Retrofit Assessment Models for Strengthening Existing Steel Buildings Under Increased Load Demands. *Review of Applied Science and Technology*, *3*(04), 325–366. https://doi.org/10.63125/yyqnte84

[109]. Md. Mainuddin, F. (2026). AI-Enabled Performance-Based Structural Optimization of Steel Truss and Mezzanine Systems for Industrial Facilities. *American Journal of Data Science and Analytics*, *7*(02), 01-38. https://doi.org/10.63125/enhzbm16

[110]. Md. Mamunur, R. (2024). Predictive Analytics for Cloud Service Reliability A Comparative Evaluation of System Performance and Disaster-Recovery Metrics. *Review of Applied Science and Technology*, *14*(12), 55–91. https://rast-journal.org/index.php/RAST/article/view/171

[111]. Md. Mamunur, R. (2025). AI-Driven Quantitative Cybersecurity Risk Assessment of Identity and Access Management in Hybrid Cloud Environments. *American Journal of Interdisciplinary Studies*, *15*(10), 01-37. https://doi.org/10.63125/1yc7ee20

[112]. Md. Mamunur, R., & Md, A. (2023). Cloud Migration Readiness and Operational Risk in U.S. Organizations: A Quantitative Analysis of Infrastructure and Business Continuity Indicators. *American Journal of Scholarly Research and Innovation*, *13*(07), 01-27. https://doi.org/10.63125/28jkj206

[113]. Morgan, T. C., Syropoulos, C., & Yotov, Y. V. (2023). Economic sanctions: Evolution, consequences, and challenges. *Journal of Economic Perspectives*, *37*(1), 3-29. https://doi.org/10.1257/jep.37.1.3

[114]. Morse, J. C. (2019). Blacklists, market enforcement, and the global regime to combat terrorist financing. *International Organization*, *73*(3), 511-545. https://doi.org/10.1017/s002081831900016x

[115]. Naheem, M. A. (2015). Trade based money laundering: Towards a working definition for the banking sector. *Journal of Money Laundering Control*, *18*(4), 513-524. https://doi.org/10.1108/jmlc-01-2015-0002

[116]. Neuenkirch, M., & Neumeier, F. (2015). The impact of UN and US economic sanctions on GDP growth. *European Journal of Political Economy*, *40*, 110-125. https://doi.org/10.1016/j.ejpoleco.2015.09.001

[117]. Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science*, *366*(6464), 447-453. https://doi.org/10.1126/science.aax2342

[118]. Oztas, B., Cetinkaya, D., Adedoyin, F., Budka, M., Aksu, G., & Dogan, H. (2024). Transaction monitoring in anti-money laundering: A qualitative analysis and points of view from industry. *Future Generation Computer Systems*, *159*, 161-171. https://doi.org/10.1016/j.future.2024.05.027

[119]. Pape, R. A. (1997). Why economic sanctions do not work. *International Security*, *22*(2), 90-136. https://doi.org/10.1162/isec.22.2.90

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

[121]. Pavlidis, G. (2023). The dark side of anti-money laundering: Mitigating the unintended consequences of FATF standards. *Journal of Economic Criminology*, *2*, 100040. https://doi.org/10.1016/j.jeconc.2023.100040

[122]. Peksen, D. (2009). Better or worse? The effect of economic sanctions on human rights. *Journal of Peace Research*, *46*(1), 59-77. https://doi.org/10.1177/0022343308098404

[123]. Peksen, D. (2019). When do imposed economic sanctions work? A critical review of the sanctions effectiveness literature. *Defence and Peace Economics*, *30*(6), 635-647. https://doi.org/10.1080/10242694.2019.1625250

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

[125]. Portela, C. (2016). Are European Union sanctions "targeted"? *Cambridge Review of International Affairs*, *29*(3), 912-929. https://doi.org/10.1080/09557571.2016.1231660

[126]. Punnaiah Chowdary, R. (2021). GC-MS Strategies for Identification of Trace Impurities in Active Pharmaceutical Ingredients. *American Journal of Advanced Technology and Engineering Solutions*, *11*(05), 01-35. https://ajates-scholarly.com/index.php/ajates/article/view/131

[127]. Punnaiah Chowdary, R., & Md, A. (2020). Practical HPLC Method Validation Under ICH Q2(R2) and Q14: An Analytical Quality Framework. *International Journal of Business and Economics Insights*, *10*(03), 01–36. https://ijbei-journal.org/index.php/ijbei/article/view/73

[128]. Punnaiah Chowdary, R., & Md Jamil, A. (2020). Risk-Based Lifecycle Management of Chromatographic Methods for Generic API Quality: A Systematic Review. *Review of Applied Science and Technology*, *10*(09), 01–41. https://doi.org/10.63125/r0xnar90

[129]. Rocha-Salazar, J.-d.-J., Segovia-Vargas, M.-J., & Camacho-Miñano, M.-d.-M. (2021). Money laundering and terrorism financing detection using neural networks and an abnormality indicator. *Expert Systems with Applications*, *169*, 114470. https://doi.org/10.1016/j.eswa.2020.114470

[130]. Rodríguez, F., Rendón, S., & Weisbrot, M. (2025). Effects of international sanctions on age-specific mortality: A cross-national panel data analysis. *The Lancet Global Health*, *13*(8), e1358-e1366. https://doi.org/10.1016/s2214-109x(25)00189-5

[131]. Romaniuk, P., & Keatinge, T. (2018). Protecting charities from terrorists … and counterterrorists: FATF and the global effort to prevent terrorist financing through the non-profit sector. *Crime, Law and Social Change*, *69*(2), 265-282. https://doi.org/10.1007/s10611-017-9755-6

[132]. Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, *1*(5), 206-215. https://doi.org/10.1038/s42256-019-0048-x

[133]. Sadia, A. (2025). Privacy-Aware Personalization: Machine Learning, Model Validation, And Consumer Trust in AI-Mediated Marketing. *American Journal of Scholarly Research and Innovation*, *4*(01), 1081–1119. https://doi.org/10.63125/j7tfr242

[134]. Sadia, A. (2026). A Data-Science Decision-Support Framework for Responsible AI-Enabled Marketing, Visualization, And Consumer Engagement in The United States. *American Journal of Interdisciplinary Studies*, *7*(02), 277-311. https://doi.org/10.63125/e67w9e54

[135]. Sadia, A., & Md. Mosheur, R. (2023). Consumer Trust, Perceived Authenticity, and Personalized Digital Marketing: A Quantitative Decision-Science Study. *International Journal of Scientific Interdisciplinary Research*, *4*(2), 252–295. https://doi.org/10.63125/cajkqt60

[136]. Saenz, M., & Lewer, J. J. (2023). Estimates of trade based money laundering within the European Union. *Applied Economics*, *55*(51), 5991-6003. https://doi.org/10.1080/00036846.2022.2141444

[137]. Saito, T., & Rehmsmeier, M. (2015). The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets. *PLOS ONE*, *10*(3), e0118432. https://doi.org/10.1371/journal.pone.0118432

[138]. Shabbir, A. (2025). Physics-Based Failure Prognostics for Preventing Pressure-System Degradation and Unplanned Industrial Shutdowns. *American Journal of Scholarly Research and Innovation*, *14*(09), 01–41. https://doi.org/10.63125/3asd0053

[139]. Sharman, J. C. (2008). Power and discourse in policy diffusion: Anti-money laundering in developing states. *International Studies Quarterly*, *52*(3), 635-656. https://doi.org/10.1111/j.1468-2478.2008.00518.x

[140]. Sharmin, A. (2025). Transferable Patient-Centered Communication Models: A Multisite Implementation Study. *American Journal of Scholarly Research and Innovation*, *15*(09), 01–32. https://doi.org/10.63125/j5p8bm56

[141]. Sharmin, A., & Mst Kaniz, F. (2023). "My Pain Was Not Taken Seriously" Medical Gaslighting As an Expectancy Violation in Women's Healthcare. *American Journal of Health and Medical Sciences*, *13*(06), 55–85. https://ajhmsjournal.com/index.php/ajhms/article/view/20

[142]. Sharmin, A., & Nishat, J. (2023). Communication Accommodation and Patient Trust in Healthcare and Chronic Illness Care. *Review of Applied Science and Technology*, *13*(08), 34–72. https://doi.org/10.63125/6p0xwb79

[143]. Singh, K., & Best, P. (2019). Anti-money laundering: Using data visualization to identify suspicious activity. *International Journal of Accounting Information Systems*, *34*, 100418. https://doi.org/10.1016/j.accinf.2019.06.001

[144]. Songeta, D. (2024). Human-In-The-Loop Artificial Intelligence for Account Reconciliation and Financial-Reporting Transparency: A Bibliometric and Science-Mapping Analysis. *American Journal of Scholarly Research and Innovation*, *14*(12), 41–72. https://doi.org/10.63125/jamadx91

[145]. Songeta, D. (2025). Machine Learning for Retail Sales and KPI Forecasting: A Systematic Review and Meta-Analysis of Predictive Performance. *American Journal of Advanced Technology and Engineering Solutions*, *15*(08), 01-36. https://doi.org/10.63125/xan6v087

[146]. Songeta, D. (2026). Machine Learning for Financial-Statement Anomaly Detection in U.S. Small and Mid-Sized Enterprises: A Quantitative Study Using Gradient Boosting and SHAP. *American Journal of Interdisciplinary Studies*, *16*(08), 94-127. https://doi.org/10.63125/61wry195

[147]. Stewart, I. J., Viski, A., & Brewer, J. (2020). Combating the financing of proliferation: Challenges and new tools. *Journal of Financial Crime*, *27*(4), 1107-1121. https://doi.org/10.1108/jfc-06-2019-0082

[148]. Sumaiya, M. (2024). Hospital Wastewater as A Reservoir of Antimicrobial Resistance Genes: Implications for Public Health and Genomic Surveillance in The United States. *Review of Applied Science and Technology*, *3*(04), 448–508. https://doi.org/10.63125/ahvas976

[149]. Sumaiya Sadmeen, M. (2025). Spatiotemporal Graph Neural Networks and Digital Twins for Urban Drainage Networks: Predictive Inundation, Critical-Node Detection, And Infrastructure Prioritization. *American Journal of Scholarly Research and Innovation*, *15*(12), 01-40. https://doi.org/10.63125/awvjew66

[150]. Sumaiya Sadmeen, M., & Kazi Mohammad Khalid, A. (2023). Multi-Source Remote Sensing and Dem-Derived Hydrogeomorphic Indicators for High-Resolution Urban Flood Susceptibility Mapping: A Spatial Cross-Validation Framework. *Journal of Sustainable Development and Policy*, *13*(07), 01-46. https://doi.org/10.63125/z4xt7k38

[151]. Tahmedur, R. (2024). Machine-Learning-Assisted Project Cost Estimation for Technology-Intensive Engineering Programs. *International Journal of Scientific Interdisciplinary Research*, *14*(12), 01–54. https://doi.org/10.63125/7gfgm030

[152]. Tahmedur, R. (2025). Development of a Decision-Support Model for Agile Hybrid Engineering Project Delivery in Technology Driven Organizations. *Review of Applied Science and Technology*, *4*(04), 339–381. https://doi.org/10.63125/v7jjv448

[153]. Takáts, E. (2011). A theory of "crying wolf": The economics of money laundering enforcement. *Journal of Law, Economics, and Organization*, *27*(1), 32-78. https://doi.org/10.1093/jleo/ewp018

[154]. Tasneem, S., Courtot, H., Fullowan, K., & Hall, P. (2026). Bias evaluation in large language model summaries using financial crimes data. *Mathematics*, *14*(11), 1795. https://doi.org/10.3390/math14111795

[155]. Unger, B., & den Hertog, J. (2012). Water always finds its way: Identifying new forms of money laundering. *Crime, Law and Social Change*, *57*(3), 287-304. https://doi.org/10.1007/s10611-011-9352-z

[156]. Vanhoeyveld, J., Martens, D., & Peeters, B. (2020). Customs fraud detection: Assessing the value of behavioural and high-cardinality data under the imbalanced learning issue. *Pattern Analysis and Applications*, *23*(3), 1457-1477. https://doi.org/10.1007/s10044-019-00852-w

[157]. Walker, J., & Unger, B. (2009). Measuring global money laundering: "The Walker gravity model". *Review of Law & Economics*, *5*(2), 821-853. https://doi.org/10.2202/1555-5879.1418

[158]. Watterson, C. J., Osborne, S., & Grant, S. (2020). Open registries as an enabler of maritime sanctions evasion. *Marine Policy*, *119*, 104090. https://doi.org/10.1016/j.marpol.2020.104090

[159]. Weiss, T. G. (1999). Sanctions as a foreign policy tool: Weighing humanitarian impulses. *Journal of Peace Research*, *36*(5), 499-509. https://doi.org/10.1177/0022343399036005001

[160]. Wertz, D. (2013). The evolution of financial sanctions on North Korea. *North Korean Review*, *9*(2), 69-82. https://doi.org/10.3172/nkr.9.2.69

[161]. Wolsing, K., Roepert, L., Bauer, J., & Wehrle, K. (2022). Anomaly detection in maritime AIS tracks: A review of recent approaches. *Journal of Marine Science and Engineering*, *10*(1), 112. https://doi.org/10.3390/jmse10010112

[162]. Wronka, C. (2022). Digital currencies and economic sanctions: The increasing risk of sanction evasion. *Journal of Financial Crime*, *29*(4), 1269-1282. https://doi.org/10.1108/jfc-07-2021-0158

[163]. Zdanowicz, J. S. (2009). Trade-based money laundering and terrorist financing. *Review of Law & Economics*, *5*(2), 855-878. https://doi.org/10.2202/1555-5879.1419

[164]. Zhang, Y., & Trubey, P. (2019). Machine learning and sampling scheme: An empirical study of money laundering detection. *Computational Economics*, *54*(3), 1043-1063. https://doi.org/10.1007/s10614-018-9864-z