VISITING EXPERT'S PAPER

PREVENTING AND COMBATING MONEY-LAUNDERING AND TERRORIST FINANCING: AN OVERVIEW OF INTERNATIONAL STANDARDS, GLOBAL TRENDS AND THE ROLE OF DOMESTIC COORDINATION

*Aibek Turdukulov**

I. INTRODUCTION: THE GLOBAL FRAMEWORK AGAINST FINANCIAL CRIME

The fight against money-laundering (ML), terrorist financing (TF) and the financing of proliferation (PF) is a cornerstone of global security and economic stability. The scale of the problem is immense, with the United Nations Office on Drugs and Crime (UNODC) estimating that the amount of money laundered globally in one year is between 2 to 5 percent of global GDP, or US800 billion–US2 trillion. Criminal and terrorist networks exploit vulnerabilities in the financial system to conceal the proceeds of their activities, undermining the rule of law, fuelling corruption, distorting economic competition and threatening sustainable development.

A robust international framework, underpinned by United Nations conventions and driven by the standards of the Financial Action Task Force (FATF), provides the foundation for national efforts to combat these threats. The UNODC, through its Global Programme on Money Laundering (GPML), plays a pivotal role in supporting Member States by providing technical assistance, policy guidance and fostering international cooperation.

This paper synthesizes key concepts from the prevailing international AML/CFT regime. It will first outline the foundational standards and legal instruments, then explore the evolving nature of global ML/TF threats with a focus on Southeast Asia, and finally, examine the critical importance of effective domestic coordination as the lynchpin of a successful national strategy.

II. THE INTERNATIONAL AML/CFT STANDARDS AND LEGAL FRAMEWORK

An effective response to transnational financial crime requires a universally recognized set of standards and legal obligations. The FATF and key UN Conventions form the pillars of this global architecture.

A. The Financial Action Task Force (FATF)

The FATF is the inter-governmental body that sets the international standards for combating money-laundering and terrorist financing. Its core mandate involves:

1. **Developing the FATF Standards:** The FATF Recommendations (the "40 Recommendations") provide a complete framework of measures that countries should implement. They are not hard law but carry significant weight through the peer-review process. These standards cover the entire AML/CFT spectrum, including the crucial **Risk-Based Approach (RBA)**, requirements for **Customer Due Diligence (CDD)**, robust measures for **beneficial ownership transparency** of legal persons and arrangements, the powers and responsibilities of **competent authorities**, and mechanisms for **international cooperation**.

2. **Monitoring Compliance:** Through a rigorous process of peer-review, known as Mutual Evaluations, the FATF assesses countries' implementation of the standards. This process has two distinct components:

* Programme Officer (AML/CFT), UNODC.

- **Technical Compliance Assessment:** This evaluates whether the necessary laws, regulations, and powers exist on paper. Jurisdictions are rated on each of the 40 Recommendations as either *Compliant (C)*, *Largely Compliant (LC)*, *Partially Compliant (PC)*, or *Non-Compliant (NC)*.

- **Effectiveness Assessment:** This is a qualitative assessment of how well a country's AML/CFT system works in practice. It measures performance against 11 "Immediate Outcomes" (e.g., "IO.7: Money laundering is investigated and prosecuted," "IO.8: Proceeds of crime are confiscated"). Jurisdictions are rated as having a *High (HE)*, *Substantial (SE)*, *Moderate (ME)*, or *Low (LE)* level of effectiveness for each outcome.

3. **Identifying High-Risk Jurisdictions:** The FATF identifies jurisdictions with strategic AML/CFT deficiencies.

   - **Jurisdictions Under Increased Monitoring ("Grey List"):** These countries are actively working with the FATF to address strategic deficiencies within agreed timeframes. Being "greylisted" can result in significant reputational damage, a decline in foreign direct investment, de-risking by global correspondent banks, and increased transaction costs for businesses.

   - **High-Risk Jurisdictions Subject to a Call for Action ("Black List"):** These are countries with significant strategic deficiencies that the FATF calls on its members and all jurisdictions to apply enhanced due diligence and, in the most serious cases, countermeasures to protect the international financial system.

B. Foundational United Nations Conventions

The FATF standards are reinforced by international law, primarily through three key UN conventions that provide the legal mandate for domestic action and international cooperation:

1. **The Vienna Convention (1988):** The UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances was the first international treaty to require the criminalization of money-laundering, laying the critical groundwork for future efforts, although its scope was limited to drug trafficking proceeds.

2. **The Palermo Convention (UNTOC, 2000):** The UN Convention Against Transnational Organized Crime significantly expanded AML obligations, requiring the criminalization of laundering the proceeds of a wide range of "serious crimes". Its key contributions include Article 7, which laid out measures such as customer identification and suspicious transaction reporting, and the formal introduction of the concept of Financial Intelligence Units (FIUs). Crucially, its robust chapter on international cooperation (Article 18) provides a powerful legal basis for Mutual Legal Assistance (MLA) even in the absence of bilateral treaties.

3. **The Merida Convention (UNCAC, 2003):** The UN Convention Against Corruption is the only legally binding universal anti-corruption instrument. It established corruption offences (e.g., bribery, embezzlement) as key predicate offences for money-laundering. Its most groundbreaking feature is **Chapter V on Asset Recovery**, which establishes the return of stolen assets as a fundamental principle of international law. It obligates states to cooperate extensively in tracing, freezing, confiscating, and returning the proceeds of corruption, introducing innovative legal mechanisms like non-conviction-based asset forfeiture (Article 54) and direct recovery of property (Article 53).

Together, these instruments provide the comprehensive legal basis for countries to criminalize money-laundering, confiscate illicit assets, and cooperate effectively across borders.

III. EVOLVING GLOBAL AND REGIONAL MONEY-LAUNDERING TRENDS

The threat landscape of financial crime is not static. Criminal organizations continuously adapt their methods, exploiting new technologies and regulatory loopholes. Analysis of trends in Southeast Asia, a global

hub for such activity, reveals a dynamic and converging criminal ecosystem.

A. The Rise of Casino and Special Economic Zone (SEZ) Hubs

Across the Mekong region, a rapid and often unregulated expansion of casinos and SEZs has created a permissive environment for large-scale money-laundering. These zones, frequently located in remote border areas with limited government oversight, function as de facto extrajudicial territories and have become safe havens for transnational organized crime. Illicit actors leverage these zones to:

- **Launder Proceeds at Scale:** The commingling of vast amounts of cash from both legitimate gaming and illicit activities makes casinos a classic vehicle for laundering proceeds from drug trafficking, the primary predicate offence in the region.

- **Establish Criminal Infrastructure:** These zones house sophisticated cyber-fraud and online scam centres, often staffed by victims of human trafficking who are forced to work under brutal conditions.

- **Exploit Regulatory Gaps:** They host a proliferation of illegal and high-risk Virtual Asset Service Providers (VASPs), which operate outside of regulatory perimeters to launder funds globally.

B. Convergence of Crime and Technology

A clear and dangerous convergence of criminal activities is occurring. The vast profits from the drug trade have fuelled investment in the infrastructure needed for large-scale cybercrime. These criminal enterprises are characterized by:

- **Technological Sophistication:** An increasing reliance on technology to anonymize and expedite their operations. This includes the use of **cryptocurrencies**, laundered through mixers, tumblers and chain-hopping across different blockchains to obscure the money trail; **deepfake technology** to create fraudulent identity documents and bypass biometric KYC controls; and **advanced communications tools** like the Starlink satellite internet service, which provides resilient, hard-to-trace connectivity for criminal compounds in remote areas.

- **Professionalization and Specialization:** The growth of a criminal "as-a-service" model, where specialized groups sell hacking tools, malware, stolen data and even "Laundering-as-a-Service" (LaaS) on underground markets. This lowers the barrier to entry and increases the efficiency of criminal operations.

- **Exploitation of Data:** The proliferation of underground data markets, fuelled by "infostealer" malware that harvests credentials and personal data from victims worldwide. This stolen information is the lifeblood of modern fraud, used for victim profiling, extortion and creating mule accounts for laundering illicit funds.

On-chain analysis of cryptocurrency flows from these regional hubs shows undeniable links to global criminal activity, including North Korean sanctions evasion, proliferation financing and the laundering of funds stolen by state-sponsored hacking groups like the Lazarus Group.

IV. THE IMPERATIVE OF DOMESTIC COORDINATION

While international standards provide the blueprint, their effectiveness depends entirely on robust implementation at the national level. Effective domestic coordination is arguably the most critical element of a functional AML/CFT regime. As FATF Recommendation 2 states, countries must have national AML/CFT policies based on identified risks and ensure effective cooperation and coordination between all relevant authorities.

A. Key Domestic Players

A "whole-of-government" and societal approach is essential, involving a collaborative chain of stakeholders:

- **Financial Intelligence Unit (FIU):** The central national agency for receiving, analysing and disseminating financial intelligence. It serves as the crucial link between the private sector and law enforcement.

- **Law Enforcement Agencies (LEAs):** Police, customs and specialized financial crime units that use FIU intelligence to investigate predicate crimes and money-laundering.

- **Prosecutorial Services and Judiciary:** Responsible for prosecuting ML/TF cases, ensuring evidence is admissible, securing convictions and issuing the court orders necessary for freezing and confiscating assets while safeguarding due process.

- **Supervisory Authorities:** Central banks and other bodies that regulate and supervise financial institutions and DNFBPs. Their role is to ensure the private sector effectively implements its AML/CFT obligations, including the RBA and CDD.

- **Policy-Making Ministries:** Ministries of Finance, Justice and Foreign Affairs that provide political will, oversee the legal and policy framework, and manage international cooperation.

- **Private Sector:** Financial institutions and designated non-financial businesses and professions (DNFBPs) are the gatekeepers of the financial system and the first line of defence, responsible for implementing preventive measures and reporting suspicious activity to the FIU.

B. Models for Coordination and Information Sharing

Effective coordination must occur at both the policy and operational levels. Common mechanisms include:

- **High-Level Coordination:** National AML/CFT Committees, often chaired by a senior figure from a ministry of finance or justice, are essential for setting national policy. Their primary tasks include conducting the **National Risk Assessment (NRA)**, developing a national strategy based on its findings, and ensuring the allocation of adequate resources and political will.

- **Operational Coordination:** This involves hands-on collaboration through multi-agency **task forces** focused on specific threats (e.g., cyber-fraud, wildlife trafficking), **joint investigation teams** for complex cases and the **secondment of staff** between agencies to build trust, share expertise and break down cultural silos.

- **Public-Private Partnerships (PPPs):** These are increasingly vital. Formal platforms, like the UK's Joint Money Laundering Intelligence Taskforce (JMLIT), allow the FIU, law enforcement and major private sector entities to exchange strategic intelligence and typologies in a trusted environment, dramatically improving the quality and utility of suspicious transaction reports.

The fuel for all coordination is **information sharing**. Legal frameworks must provide clear "gateways" that permit or mandate the timely and proactive sharing of operational and strategic intelligence, moving from a reactive "need to know" culture to a proactive "need to share" paradigm. The failure to share information creates silos where crucial pieces of the puzzle are missed, leading to failed investigations and allowing illicit funds to dissipate.

V. CONCLUSION AND KEY TAKEAWAY

Combating money-laundering and terrorist financing is a complex, enduring challenge that requires sustained commitment and adaptation. The key takeaways from this overview are clear:

1. **A Strong Foundation is Essential:** Adherence to the global standards set by the FATF and the legal obligations within the UNTOC and UNCAC is the non-negotiable price of entry for any country seeking to protect its financial system and participate in the global economy.

2. **Threats are Dynamic and Converging:** Criminals are agile, technology-driven and operate transnationally. The convergence of cybercrime, fraud and traditional predicate offences like drug trafficking presents a formidable, borderless challenge that requires an equally agile and collaborative international response.

3. **Domestic Coordination is Key:** A national AML/CFT framework is only as strong as the collaboration between its constituent parts. Breaking down institutional silos and fostering seamless, real-time information sharing between the FIU, law enforcement, prosecutors, supervisors and the private sector is the single most critical factor for success.

4. **Public-Private Collaboration is Crucial:** The private sector is the first and most important line of defence. Empowering financial institutions and DNFBPs with the actionable intelligence and collaborative frameworks they need to identify and report illicit activity is a force multiplier that is indispensable in the fight against financial crime.