Journal of Economics, Finance and Management Studies

ISSN (print): 2644-0490, ISSN (online): 2644-0504

Volume 08 Issue 10 October 2025

Article DOI: 10.47191/jefms/v8-i10-18, Impact Factor: 8.317

Page No: 6736- 6746

Laundering-As-A-Service (Laas): The Emerging Gig Economy of Financial Crime

Michele Trifiletti

Independent Researcher, https://orcid.org/0009-0004-2552-9231

ABSTRACT: The evolution of illicit finance is increasingly mirroring the dynamics of the legitimate economy, with **Laundering-as-a-Service (LaaS)** emerging as a scalable, on-demand model for outsourcing money laundering activities. This study presents LaaS as a true **structured service industry**, operating in the financial crime ecosystem. In this model, specialized, often anonymous vendors offer modular "AML circumvention packages," replicating the logic of legitimate **oftware-as-a-Service (**[1]**SaaS**) models. The clientele is extremely diverse, ranging from organized crime syndicates to individual malicious actors and terrorists.

Using a multidisciplinary research methodology that integrates **Open-Source Intelligence (OSINT**[2]**),** blockchain forensics,[3] and law enforcement case studies—including the transnational operation "Destabilise"—we map the **operational lifecycle of LaaS**. This process is divided into distinct phases: from **placement** through the creation of fictitious entities and synthetic identities (deepfakes[4], manipulated biometric data), to **complex** cross-border stratification[5] employing mixers, tumblers [6]and mule networks[7], up to **integration** illicit funds in assets with high liquidity and low risk of devaluation, such as valuable cryptocurrencies, luxury goods, and investments in real estate.

The paper analyzes the main drivers of LaaS adoption, including the anonymity offered by cryptocurrencies, the efficiency of illicit dark web marketplaces, and the increasing technological complexity of laundering methods. Its disruptive impact on **existing AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism)** regulatory and technological frameworks is discussed, highlighting regulatory gaps and investigative challenges. The work concludes by proposing a **multi-level contrast strategy** based on: 1) proactive intelligence on digital threats, 2) the application of predictive technologies and **machine learning**[8] to identify anomalous behavioral patterns and 3) a structured international cooperation between investigative agencies, public and private sectors, for a more agile and effective approach to the fight against modern financial crime.

KEYWORDS- Laundering-as-a-Service (LaaS), money laundering, cryptocurrencies, AML/CFT, dark web, financial crime, blockchain forensics, organized crime, crime economics, illicit FinTech.

[1] **Software-as-a-Service (SaaS),** or "software as a service," is a software delivery model in which a vendor makes an application available to end users over the internet, usually through a web browser.
Unlike the traditional model, where software is purchased and installed on a local computer or on a corporate ("on-premise") server, in the SaaS model, the application is hosted and managed centrally by the vendor. Users access the service through a periodic subscription (monthly or annual), without having to worry about infrastructure, maintenance or updates.

[2] **Open Source Intelligence (OSINT)** is the activity of collecting and analyzing information from public sources, such as the Internet and social media, to produce **intelligence**. Its goal is to transform open and accessible data into strategic knowledge.

[3] The **blockchain** (from the English "chain of blocks") is a technology based on a distributed and decentralized database, which allows a series of transactions to be recorded in a secure, transparent and immutable way.

[4] The term **deepfake** is a neologism composed of the English words "deep learning" and "fake". It refers to an artificial intelligence technique that generates fake and highly realistic videos, images or audio, in which the face or voice of one person is replaced with those of another.

[5] **Complex cross-border layering:** this is the phase in which money of illicit origin is "hidden". It is not just a single transaction, but a complex network of financial movements, often international (**cross-border**), which are intended to move funds away from their original source. The complexity is given precisely by the simultaneous use of different methods and jurisdictions to confuse the traces.

[6] **Mixers and Tumblers:** These are tools, typically online services or software, used in the cryptocurrency world to "mix" digital funds. A **mixer** or **tumbler** receives cryptocurrency from different sources and distributes it to multiple destinations, making it nearly impossible to trace the original provenance of the funds. It's like throwing a handful of anonymous coins into a large container and pulling out a different handful, but of the same value, making them untraceable.

[7] Financial **mules** are people who transfer money, often in small amounts, on behalf of a criminal organization. They can be recruited knowingly or unknowingly, and their job is to receive the funds in an account (often a bank account) and then withdraw or transfer them to another destination. A **network of mules** is an organized group of these people, employed to distribute money in many streams, making it difficult for the authorities to trace.

[8] **Machine Learning** (ML) is a branch of artificial intelligence that allows a computer system to learn from data, recognize patterns, and make decisions with little to no human intervention.

Laundering-As-A-Service (Laas): The Emerging Gig Economy of Financial Crime

I. INTRODUCTION

The phenomenon of **Crime-as-a-Service (CaaS)** has revolutionized the cybercrime landscape, drastically breaking down technical barriers and "democratizing" access to sophisticated tools. Phenomena such as **Ransomware-as-a-Service[9] (RaaS)** and **Phishing-as-a-Service[10] (PhaaS)** have shown that anyone, for a fee, can conduct complex operations without possessing advanced skills. Today, a similar transformation is affecting the field of money laundering. **Laundering-as-a-Service (LaaS)** emerges as the new frontier of this evolution: a criminal business model in which specialized operators offer "turnkey" services to evade the complex **Anti-Money Laundering (AML)** and **Countering the Financing of Terrorism (CFT) control systems**.

A. HISTORICAL PRECEDENTS NAD PARALLELS

While LaaS is an inherently modern phenomenon, its roots lie in historical practices of organized crime. LaaS does not come out of nowhere, but represents the synthesis between consolidated recycling techniques and the logic of the **gig economy** and **fintech**.

- **Hawala**: An informal system of value transfer, based on networks of mediators and mutual trust, which operates without formal traceability. LaaS takes up the logic of anonymity and decentralization, but uses technology to make it global and instantaneous.
- **Money Mules**: Networks of nominees used to move funds, breaking the link between the illicit origin and the final beneficiary. LaaS automates and scales this model, transforming the network of mules from a manual and risky operation to a digitized service, often managed via the dark web.
- **Tax Havens**: Historic hubs for money laundering operations thanks to bank confidentiality. LaaS, through cryptocurrencies and anonymity services, extends this opacity to a digital environment, offering a virtually unassailable "jurisdiction".
- **Structured Deposits (Smurfing):** Techniques used by drug cartels to divide large sums of money into smaller, non-suspicious deposits. LaaS replicates and automates these techniques, using scripts and bots to distribute funds across hundreds or thousands of wallets or accounts, with significantly greater speed and scalability.

B. STRATEGIC IMPLICATIONS AND THESIS OF THE WORK

The central hypothesis of this work is that **LaaS is not an isolated phenomenon, but a logical evolution of financial crime towards scalable and professional business models**. Its strategic implications are profound: fragmentation **of responsibilities**, **operational decentralization** and reduction **of individual exposure** render many traditional investigation techniques ineffective. To effectively counter this threat, a reactive approach, focused on blocking individual transactions, must be abandoned in favor of a **proactive strategy** that aims to map, infiltrate and disrupt the infrastructures of criminal service providers. This paper therefore aims to define LaaS as a structured industry, track its functioning, analyze the factors that drive its adoption and evaluate its implications for current financial supervision policies.

II. LITERATURE REVIEW

The professionalization of money laundering is not a completely new concept in the literature on financial crime. Supranational bodies and intelligence agencies have long documented the importance of professional facilitators, but the phenomenon of **Laundering-as-a-Service (LaaS)** represents a digital and industrial evolution that deserves specific analysis.
The professionalization of financial crime has been observed and documented in several venues:

- **Financial Action Task Force (FATF):** The FATF's recommendations (in particular 1, 10, 15 and 24) have long emphasized the crucial role of financial facilitators, defining them as structured and increasingly sophisticated operational networks, capable of managing large volumes of illicit funds.
- **Europol**: In its *Serious and Organised Crime Threat Assessment (SOCTA),* Europol flagged the emergence of specialised providers who monetise criminal proceeds including through virtual assets, converting cryptocurrencies into fiat currency and vice versa.
- **Interpol**: You introduced the concept of **"financial crime-as-a-service,"** recognizing that specialization is becoming a norm rather than an exception in the criminal underworld.

[9] **Ransomware** is a type of malware (malicious software) that "takes hostage" a victim's files or entire system, rendering them inaccessible. The attacker demands a ransom in money to restore access to the data or the system.
[10] **Phishing** is a form of cyber fraud that uses social engineering to trick people into revealing sensitive information, such as passwords, credit card numbers, or bank details. The term derives from the English "fishing", because the attacker launches a "bait" (often an email, an SMS or a social message) to "fish" the victims.

- **United Nations Office on Drugs and Crime (UNODC):** In its reports on global money laundering, it highlighted how digitalization has reduced operational costs and increased the efficiency of recycling processes.

Despite these important recognitions, the current regulatory framework, which includes the **6th EU AML Directive (2018/1673)** and the provisions of the **Bank Secrecy Act (USA),** while attempting to adapt to the use of virtual assets and **Virtual Asset Service Providers (VASPs),** does not yet specifically contemplate the industrial, modular and "on-demand" nature of LaaS. The absence of a uniform operational definition and systematic studies that treat LaaS as an integrated phenomenon creates a gap that this work intends to fill. Our research aims to provide an in-depth analysis that defines the business model, drivers, operating cycle and specific countermeasures, going beyond the simple observation of professionalization.

III. RESEARCH METHODOLOGY

The analysis of the **Laundering-as-a-Service (LaaS)** phenomenon in this study is based on a **multi-disciplinary methodological approach** that combines qualitative and quantitative tools. The complex, transnational and technologically advanced nature of LaaS requires overcoming traditional investigative techniques, integrating three main pillars to achieve a holistic understanding of the phenomenon:

- **Open Source Intelligence (OSINT):** Collection and analysis of information available on open sources, including deep and dark web environments.
- **Blockchain Forensics**: Tracking cryptocurrency flows and rebuilding digital criminal infrastructures.
- **Case Studies**: Empirical validation through the examination of high-profile investigations.

A. OPEN SOURCE INTELLIGENCE (OSINT)

OSINT was the first phase of research, conducted to map the criminal market "from below". Data collection and sampling were based on the systematic monitoring of forums and marketplaces on the deep/dark web, the analysis of encrypted communication channels (e.g. Telegram, Discord) and the collection of promotional materials and public testimonials from Laas providers.

- **Business Models Observed**: Three macro-operating models have been identified that reflect the structure of a mature illicit economy:
    - **Standard/Basic**: Flat *fee* packages for money laundering of small amounts (< $10,000), ideal for minor online fraud. The processes are often automated or semi-automated.
    - **Premium/Enterprise**: Complex services for structured criminal organizations, with a **percentage commission** (10-15%). These packages are modular and include the creation of **shell companies**, the use of **synthetic identities**, and sophisticated *layering schemes*.
    - **Subscriptions/Retainers**: The most advanced model, where the customer pays a recurring fee to have continuous, on-demand access to the recycling infrastructure.
- **Trust Mechanisms**: In the absence of legal guarantees, trust has been identified as a crucial capital, built through **escrow systems** managed by marketplaces and on **public feedback** (ratings and reviews) that strengthens the provider's reputation.
- **Communication and Branding**: LaaS providers adopt marketing techniques typical of the corporate world, using professional rhetoric (e.g. **SLA** and "customer service") and creating a **brand identity**[11] to stand out and attract customers.

B. BLOCKCHAIN FORENSICS

The second pillar provided the quantitative evidence needed to track digital financial flows. Through the use of specialized software tools, the analysis focused on:

- **Service cluster identification**: Analysts group wallet addresses[12] under the control of a single entity, using heuristics such as *spending-out analysis*[13]. The goal is to identify the central nodes with sorting and *layering functions* and attribute them to real subjects by cross-referencing the blockchain data with the information collected through OSINT.
- **Obfuscation techniques**: The effectiveness of tools such as **cryptocurrency mixers** (tumblers) and **privacy coins**[14] (Monero, Zcash) was examined. The analysis made it possible to map the entry and exit points of funds and to identify the "super-users", i.e. the LaaS providers who make systematic use of these techniques.

[11] Brand **identity** is the set of visual, communicative and value elements that a company actively creates to present itself to the public. It is what the company wants to be and how it wants to be perceived.
[12] A **wallet** is, in its most general definition, a container for personal valuables, mainly money, credit cards and documents.
[13] The term "**spending-out**" refers to the act of spending money or outflowing funds.

- **Address** linking: The application of heuristics has made it possible to connect seemingly distinct addresses, providing the basis for a **graphical visualization of the network** that reconstructs the entire operational architecture of LaaS organizations.

C. CASE STUDIES

The analysis of real cases provided an empirical validation of the theoretical models that emerged from OSINT and blockchain forensics.

OPERATION DESTABILISE

This operation, conducted between 2021 and 2024 by the **UK National Crime Agency (NCA)** with the support of international agencies (FBI, Europol, FinCEN), is an emblematic example of how LaaS networks operate and can be dismantled.

- **Background**: The investigation started with the tracing of the proceeds of the Ryuk ransomware, which led to the identification of two interconnected criminal networks, **Smart** (led by Ekaterina Zhdanova) and **TGR** (led by George Rossi, Elena Chirkinyan and Andrejs Bradens).
- **Operational Structure**: These networks received cryptocurrencies from various illicit activities and converted them into **stablecoins**[15] for *layering* on DeFi platforms[16] and mixers. The funds were then exchanged for cash through couriers that combined modern *hawala* practices with blockchain techniques.
- **Investigative Methodology**: The success was the result of the integration between OSINT, blockchain forensics (identification of wallet clusters) and physical surveillance of cash deliveries. Cooperation **in over 30 countries** has been essential.
- **Results**: The operation resulted in 84 arrests, the seizure of around **£20M** and the imposition of OFAC sanctions against key players.

COMPARATIVE CASES

To further contextualize the LaaS phenomenon, historical and recent cases of recycling were examined, highlighting the evolutionary differences:

- **Historical Cases (pre-2010):** Investigations such as **Operation Virus** (France, 2012) and **Operation White Whale** (Spain, 2003-2005) were mainly based on traditional money laundering techniques (bank transfers, real estate, shell companies) with a focus on specific economic sectors.
- **Large-Scale Cases (2010-2014):** Schemes such as **Russian Laundromat** and **Azerbaijani Laundromat** have demonstrated the laundering of billions of dollars through European banks and shell companies, but still lack the technological component that characterizes LaaS.
- **Modern Cases (post-2020):** The **DEA**'s investigations against Mexican cartels show the integration of encrypted apps, *underground banking,* and *cash drops*, anticipating the hybrid models of laundering that are at the heart of LaaS.

TABLE 1 – CASES

CASE	PERIOD	ESTIMATED VOLUME	TECHNIQUES	BENEFICIARIES
Operation Destabilise	2021 2024	Hundreds of millions	Crypto, cash courier, OSINT, blockchain	Cybercrime, oligarchs, espionage
Russian Laundromat	2010 2014	$20–80B	Shell companies, banks	Russian elites
DEA Network	2021 present	$50M (shown)	Cash drops, encrypted apps	Drug trafficking cartels

SOURCE AUTHOR: *Analysis of sector data and representative values present in the text*

D. METHODOLOGICAL SUMMARY

The integration of **OSINT,** blockchain forensics**,** and **case study analysis** ensures a comprehensive, three-dimensional view of LaaS. This approach combines the "bottom-up" perspective of the illicit market with the "top-down" perspective of judicial

[14] Privacy **coins** are a category of cryptocurrencies that are specifically designed to make transactions anonymous and untraceable.
[15] A **stablecoin** is a cryptocurrency designed to maintain a stable value, usually pegged to a real asset such as a fiat currency (dollar, euro) or a commodity (gold).
[16] **DeFi** (**Decentralized Finance**) is a movement that aims to create an open and global financial system, an alternative to the traditional one, which does not rely on intermediaries such as banks, brokers or central institutions.

evidence, confirming that LaaS operates as an organized crime industry that integrates advanced digital technologies and traditional money laundering strategies in a global context.

IV. OPERATIONAL MODEL OF LAAS

The Laundering-as-a-Service (LaaS) **operating model** is not the result of random actions, but a modular and scalable structure that faithfully reflects the money laundering value chain. LaaS providers behave like professional criminal enterprises, offering a catalog of services that covers the entire life cycle of illicit money, from its generation to its full integration into the legitimate economy. This architecture consists of three key phases, supported by specialized delivery channels and standardized pricing models.

A. SERVICE STRUCTURE: The Three Stages of Recycling

The LaaS model reproduces the three canonical phases of recycling: placement, layering and integration. Each step is a link in a sophisticated chain, designed to maximize anonymity and minimize the risk of detection by authorities.

- **Entry Phase – Positioning**: The goal is to introduce illicit funds into the financial system, making them appear legitimate. The methods used are diversified and increasingly sophisticated:
    - **Creation of *shell companies***: Shell companies are established in low-transparency jurisdictions such as the British Virgin Islands, Seychelles or Belize. These fictitious entities, often with no real commercial activity, serve to mask the real beneficiaries of the funds.
    - **Synthetic identities**: Fake but credible profiles, created by combining real and fictitious data, to open offshore accounts or *wallets* on non-KYC (Know Your Customer) exchanges. This technique makes it extremely difficult for detective agencies to identify criminals.
    - **Pre-paid and gift cards**: Illicit funds are loaded onto prepaid cards to be spent or resold, often in different currencies or countries. This method fragments money into smaller, less obvious streams.
- **Core Laundering Phase – Stratification**: This is the most complex phase, the "heart" of the service. Its purpose is to break the traceability of illicit money through a network of processed transactions.
    - **Multiple fiat/crypto conversions**: Repeated switching between traditional and digital currencies to obfuscate origin.
    - **Trade-Based Money Laundering (TBML):** Issuance of false invoices and packing slips to justify movements of funds as fictitious commercial payments.
    - **Use of DeFi platforms:** Instant swaps, *liquidity pools*, and *flash loans* are leveraged o increase transactional volume in a very short time, making it difficult for forensic analysts to reconstruct.
    - **Mixers and *tumblers***: Services that aggregate and scramble cryptocurrencies from many different sources, breaking the link between sender and receiver.
    - ***Digital smurfing***: Fragmentation of sums into micro-transactions across multiple platforms to evade automated AML checks, which are only triggered beyond a certain transaction threshold.
- **Exit Phase – Integration**: The "cleaned" money is injected back into the legitimate economy. The methods used are designed to make funds indistinguishable from those of legal origin.
    - **Luxury goods**: Purchase of watches, works of art, fine cars and jewelry. The nature of these assets, which are often at low risk of obsolescence, makes them an excellent investment for recycling.
    - ***Real estate***: Real estate investments through conduit companies or front men.
    - **Alternative assets**: gold, precious metals, collectibles, and most recently, **NFTs**.
    - **Money mule *networks***: Split cash withdrawals from ATMs or ATMs, often with cards linked to foreign accounts.

B. DELIVERY CHANNELS

LaaS providers use multiple operating channels to ensure efficiency and anonymity.

- **Marketplaces on the dark web**: They function as real criminal *e-commerce*, with service showcases and prices exposed. They offer **escrow *systems*** to protect both parties and a **feedback and review** system to measure the reputation of suppliers.
- **Encrypted chats and closed channels**: Platforms such as Telegram, Discord or Session are used for direct and private communication. They allow quick negotiation and sending of encrypted documentation (PGP, OTR).

- **Physical brokers and "trusted" intermediaries**: Professionals infiltrated in legitimate sectors (consultants, lawyers, real estate agents) who act as a bridge between the digital world of LaaS and the real economy, managing the transition from digital funds to physical assets or *fiat cash*. They sometimes operate as modern *hawaladars*, handling parallel transactions without physically transferring the money.

C. PRICING MODELS

The pricing structure of LaaS is strikingly similar to that of a legitimate service industry, with pricing that reflects the risk and complexity of the operation.

- ***Flat Fee***: A fixed fee for limited amounts, typical of "Basic" packages.
- **Percentage fee**: A charge of **10-15%** on the amount recycled, justified by the high risk and complexity of "Premium" operations.
- **Subscription (*retainer*):** A monthly or annual fee for unlimited access to laundering capacity, reserved for high-profile customers or large criminal organizations.

D. EVOLUTION AND EMERGING TRENDS

The LaaS model is constantly evolving, adapting to evade survey methods.

- **Bot automation**: Some providers offer **Telegram APIs and bots** that allow customers to initiate recycling processes automatically.
- **Asset tokenization**: Conversion of funds into *private security tokens* or *stablecoins*, making tracking and traceability more complex.
- **Integration with *cybercrime-as-a-service***: "All-in-one" packages are becoming more prevalent that include not only money laundering, but also services such as *hacking*, *phishing*, and immediate monetization of proceeds.
- **Mandatory geo-diversification**: The distribution of passages across multiple countries and jurisdictions to reduce the risk of internationally coordinated investigations.

V. ADOPTION DRIVERS OF LAAS

The expansion of **Laundering-as-a-Service (LaaS)** is not a random phenomenon, but the result of a combination of structural, technological and behavioral factors. These factors make LaaS an extremely attractive solution for a wide range of criminal actors, from individual cybercriminals to complex transnational organizations. These "drivers" explain not only the rapid growth of the phenomenon, but also its ability to adapt and thrive in different legal and technological contexts.

A. REMOVAL OF THE TECHNICAL BARRIER AND SKILLS

Traditionally, money laundering was a highly specialized activity, requiring advanced skills in finance, a deep understanding of banking procedures, and trusted contacts in specific industries such as real estate or law. LaaS has removed this barrier, democratizing access to recycling and making it available to a much wider customer base, including:

- **Beginner hackers** or *script kiddies* who do not possess the skills to independently launder the proceeds of their attacks.
- **Small online scammers** who operate with small volumes of money, resulting from fraud or *scams*.
- **Local actors** with no previous experience in recycling who can now outsource the process to professionals.

The OSINT **analysis** revealed that many marketplaces on the dark web offer "Starter Packs" for recycling, complete with tutorials, step-by-step guides, and even a dedicated "customer support" service, breaking down all barriers to entry.

B. SCALABILITY AND FLEXIBILITY

LaaS providers efficiently manage variable cash flows, offering a flexible solution that adapts to the customer's needs, whether it's small amounts or large amounts of capital.

- **Micro-laundering**: Services dedicated to laundering proceeds deriving from *phishing* fraud or *romance scams*.
- **Macro-laundering**: "Enterprise" packages designed to manage large volumes of money, such as those generated by drug cartels, *ransomware networks* or arms trafficking.

The **modularity** of LaaS packages allows the process to be adapted according to several variables: the volume of money, the perceived risk, the timing required by the customer and the jurisdictions involved. This flexibility eliminates the need for criminals to build and maintain their own laundering infrastructure, reducing operational costs and risks.

C. ADVANCED ANONYMITY AND TECHNOLOGICAL RESILIENCE

The technologies employed by LaaS providers are specifically designed to circumvent tracking systems and dramatically reduce the possibility of tracing funds and identities.

- **Privacy coins** such as Monero and Zcash, which mask the sender, recipient and amount of transactions.
- **Mixers and *tumblers*** that break the direct link between the entry and exit of cryptocurrencies.
- **Encrypted communications** on platforms such as Telegram or Session, with end-to-end encryption and timed messages (*self-destruct messages*).

The emerging trend shows an increasing use of **anonymous DeFi platforms** and **cross-chain bridges** to "jump" between different blockchains, adding an extra layer of complexity and making rebuilding money flows an extremely difficult task for law enforcement.

D. SOCIAL FAACTORS: Community and Reputation

LaaS is not just a market of services, but a closed social ecosystem that is based on mechanisms of trust and *community building*, similar to those found in legal markets.

- ***Mentoring***: More experienced suppliers mentor new customers or affiliates, creating an informal apprenticeship system that ensures the continuity of the criminal network.
- ***Gamification***: Some marketplaces use public provider rankings, with scores based on reliability, speed, and recycled volumes. This system encourages competition and loyalty.
- ***Internal networking*** Customers don't just buy a service, they become part of a network of contacts that may include other specialized criminals (e.g. *hackers*, producers of false documents), creating an integrated and interconnected black market.

This reputation and community system creates barriers to entry for new players and strengthens trust among participants, making the network more resilient.

E. LEGAL RISK REDUCTION AND RISK FRAMING[17]

LaaS allows criminals to fragment and outsource the laundering process, isolating the end customer from the riskiest and most complex phases.

- **Customer isolation**: The provider manages the riskiest part (stratification and conversions), while the customer receives funds that have already been "cleansed" or converted into assets, reducing their direct exposure to money laundering crimes.
- **Complication of investigations**: This model makes the work of law enforcement extremely difficult, as they have to investigate in fragmented environments spread across multiple jurisdictions, with digital evidence dispersed across different blockchains and encrypted communication channels.

As a result, the risk of an arrest or judicial investigation is perceived as lower than the option of laundering money independently, further fueling the adoption of these services.

VI. IMPACTS ON AML/CFT FRAMEWORKS

Laundering-as-a-Service (LaaS) represents a structural and growing challenge for current **anti-money laundering (AML)** and **countering the financing of terrorism (CFT)** regulatory and technological frameworks. Unlike traditional forms of recycling, which relied on complex but straightforward operations, LaaS leverages automation, fragmentation, and decentralization, rendering many of the detection and intervention mechanisms in use today inadequate. This requires a deep reflection and an urgent updating of prevention and repression strategies.

A. FRAGMENTATION OF ENFORCEMENT AND INTERNATIONAL COOPERATION

LaaS operations are inherently multi-jurisdictional, leveraging the speed of data transfer to circumvent physical and legal boundaries. Illicit financial flows can cross dozens of countries in minutes, taking advantage of regulatory differences and legal response times.

- **Procedural incompatibilities**: International cooperation is often slowed down by slow requests for legal assistance and divergent **KYC (Know Your Customer)** standards. This allows criminals to move funds before authorities can intervene.
- **Exploitation of jurisdictions**: Exchanges and payment service providers in countries with weak AML oversight become strategic entry and exit points for criminal networks.
- **Example**: Operation **Destabilise** highlighted this issue. Coordination between more than 30 jurisdictions was necessary to reconstruct the money flows, with delays due to differences in evidentiary requirements and legal procedures, which greatly complicated the investigation.

[17] Framing is a concept that refers to the way in which information is presented to influence a person's interpretation, perception, and decisions.

B. REGULATORY ASYMMETRY AND REGULATORY ARBITRAGE

The cycle of criminal innovation in LaaS is significantly faster than regulatory compliance. New techniques spread on a large scale before they are considered by regulators, creating regulatory "gray areas" that criminals exploit to their advantage.

- **Criminal innovation**: New technologies such as **DeFi platforms,** cross-chain swaps*,* [18] and unregulated *stablecoins* can be used for large-scale laundering before regulatory agencies have understood and regulated them.
- **Absence of responsible entities**: Decentralized services such as *crypto bridges* [19]operate without a responsible legal entity, making it nearly impossible to issue warrants or penalties.
- **Regulatory arbitrage**: LaaS providers choose jurisdictions with minimum registration requirements or ineffective *enforcement*. Stricter **AML/CFT** regulations in one country can push criminals to move their activities to another, more permissive jurisdiction.

C. LIMITATIONS OF CURRENT PATTERN ANALYSIS

Traditional AML systems, based on predefined rules and algorithms, are designed to detect anomalies at the individual transaction level. This approach is ineffective against the multi-step, distributed layering techniques typical of LaaS.

- **Lack of time correlation**: Current detection engines struggle to identify suspicious transaction sequences in a short but crucial time frame.
- **Confusion with legitimate activities**: Layering techniques on blockchain, which involve a high frequency of transactions, can be indistinguishable from legitimate *trading* or algorithmic finance operations.
- **Automated LaaS "signing"**: However, specific indicators have been identified. Automated LaaS operations tend to leave a unique "signature":
    - **High-frequency micro-transactions**: Tens or hundreds of small transactions made in a matter of minutes.
    - **Fast cross-chain *passages*** through *unregulated* bridges.
    - **Recurring patterns of fractional amounts**, for example, slightly varied amounts to circumvent AML filters based on fixed thresholds.

D. STRATEGIC IMPLICATIONS FOR THE FUTURE

To effectively adapt to the LaaS threat, AML/CFT frameworks must evolve proactively. Supervisory agencies and financial institutions must:

- **Integrate OSINT and blockchain forensics**: These tools must become a key part of supervisory and investigation procedures.
- **Centralize *cross-border*** data: Mechanisms need to be developed that allow for faster transnational data sharing and analysis, overcoming fragmentation.
- **Update risk models**: Risk models should be updated to include LaaS-specific indicators, shifting the focus from individual transactions to more complex patterns of behavior.
- **Driving rapid international standards:** Real-time regulatory alignment *is essential to prevent criminals' competitive advantage from thriving in an outdated regulatory environment.*

VII. COUNTERMEASURES AND RECOMMENDATIONS

To effectively counter **Laundering-as-a-Service (LaaS),** a multi-layered approach is needed that integrates advanced technological tools, targeted legislative reforms, and real-time international cooperation. The traditional reactive model, based on the subsequent identification of suspicious transactions, has proven insufficient in the face of the speed and resilience of LaAS networks. The response must be **proactive, adaptive, and integrated**.

A. INTELLIGENCE & MONITORING: A Paradigm Shift

The paradigm must shift from passive detection of illicit activity to continuous, **predictive monitoring** of criminal infrastructure.

- **Proactive monitoring of criminal infrastructure:** Authorities should not only react, but should conduct systematic observation of forums, dark web marketplaces, and encrypted communication channels (e.g., Telegram, Discord, Session). The goal is not only to intercept ongoing operations, but **to map LaaS providers in advance**, identify their

[18] A **cross-chain swap** (or "chain swap") is an operation that allows cryptocurrencies residing on two different blockchains to be directly exchanged, without having to go through a centralized intermediary such as a traditional exchange.

[19] A **crypto bridge** is a protocol that connects two separate blockchains, allowing the transfer of assets and data between them. Since blockchains are closed ecosystems that cannot communicate with each other natively, bridges are crucial to ensure **interoperability** and keep liquidity flowing between different networks.

business models, repeat customers and the operational innovations they introduce. This intelligence-driven approach can provide an "early warning" of future threats.

- **Advanced blockchain analytics**: Blockchain **forensics** tools must evolve from a single-address approach to one based on **networks and service clusters**. The use of **graph analytics** and **entity resolution** techniques makes it possible to identify the central nodes of recycling, visualize complete flow architectures and identify "super-users" and recurring patterns of **cross-chain** transactions. For example, proactive real-time tracking of **DeFi** transactions can spot *flash loan laundering* schemes before funds are integrated into the financial system.

B. LEGAL AND POLICY INSTRUMENTS: Harmonization and Timeliness

Technology alone is not enough; A harmonised and up-to-date legal framework is needed to fill regulatory gaps and allow for effective action.

- **LaaS-specific criminalization**: It is crucial to introduce regulations that explicitly define and penalize the offer and use of "as-a-service" recycling infrastructure. This would make it possible to prosecute not only the final beneficiaries of the illicit money, but also the **facilitators and providers** of these services, hitting the crucial link in the criminal chain.
- **Transparency of corporate registers**: The implementation of public and real-time registers of **beneficial ownership**, with the obligation of transparency also extended to offshore jurisdictions, is essential. This would drastically reduce the possibility for criminals to disguise real owners behind **shell companies**.
- **Rapid international cooperation**: Financial **Intelligence Units (FIUs)** and channels such as the **Egmont Group** need to be strengthened for secure and immediate data exchange, overcoming the bureaucratic slowness of traditional international letters rogatory. The creation of **permanent multi-jurisdictional task forces** dedicated to digital financial crimes can ensure faster and more coordinated intervention.

C. TECHNOLOGICAL INNOVATION: Leveraging AI and Data

The public and private sectors must co-innovate, sharing tools and expertise to create a more robust and dynamic defensive system.

- **Machine Learning and Predictive AI**: AI models can be trained to recognize typical LaaS **service patterns**, such as high-frequency micro-transactions, fast cross-chain steps, and fractional amounts. Unlike fixed rules, these systems dynamically adapt to new criminal strategies.
- **Privacy-preserving data sharing**: It is possible to create secure platforms for data sharing between banks, crypto-exchanges, and law enforcement, using techniques such as **homomorphic encryption**[20] or **federated learning**[21]. This allows you to extract actionable insights for investigations without violating privacy regulations such as GDPR**.**
- **SupTech for real-time supervision**: Supervisory authorities (suptech, or **supervisory technology**) should adopt live analytical dashboards that integrate banking, OSINT, and blockchain data. This would allow for the automated generation of **Suspicious Activity Reports (SARs)** and timely interventions before funds complete the integration phase.

D. SYNERGY APPROACH: a global response

The effectiveness of countermeasures depends on a **simultaneous combination** of these elements. In the absence of an integration between technological prevention, regulatory updating and operational cooperation, LaaS will continue to thrive, exploiting the gaps and asymmetries between different legal and technological frameworks. The response must be comprehensive, coordinated and capable of evolving at the same speed as the threat.

CONCLUSION

The emergence of **Laundering-as-a-Service (LaaS)** represents a crucial turning point in the evolution of financial crime. Similar to the *gig economy*, criminal networks have industrialized and democratized access to advanced laundering techniques. What was once a niche business, run by specialized criminal elites, is now a scalable, modular and resilient industry, available "on-demand" on a global market.

To effectively counter this phenomenon, a **cultural and operational change in** AML/CFT **frameworks** is indispensable. You can no longer rely on a reactive approach based on the single suspicious transaction, which has proven inadequate in the face of the speed and complexity of LaaS. A proactive approach must be taken, focused on identifying, monitoring and dismantling criminal

[20] Homomorphic encryption is a form of cryptography that allows you to perform mathematical operations on encrypted data, without it having to be decrypted. The result of the operation, once deciphered, will be identical to the result that would have been obtained by performing the same operation on the original unencrypted data.

[21] **Federated learning** is a **machine learning** technique that allows an algorithm to be trained on a vast amount of decentralized data, without the data ever leaving the device on which it was generated.

infrastructures themselves. Only by integrating **technological intelligence** and **international cooperation** will it be possible to strike at the heart of the criminal business model and bring the strategic advantage back into the hands of the institutions.

FUTURE PROSPECTS: a rapidly changing landscape

Over the next 5–10 years, the money laundering environment will undergo a technological acceleration driven by two main macro-trends that will redefine the digital arms race between *enforcement* and crime.

CENTRAL BANK DIGITAL CURRENCIES (CBDCs)

The introduction of **CBDCs** opens up double-edged scenarios.

- **Opportunity**: CBDCs could offer native and immutable traceability of transactions, making it easier to identify illicit capital flows and facilitate investigations.
- **Risks**: Without harmonized international standards, regulatory discrepancies between jurisdictions will create new spaces for criminal arbitrage. LaaS providers could leverage less regulated CBDCs as "cleaning hubs" in *cross-border recycling chains*.

GENERATIVE ARTIFICIAL INTELLIGENCE

AI will become a determining factor for both parties.

- **For authorities**: Artificial intelligence will enable real-time predictive analysis, the identification of service *patterns* never observed before and the automatic correlation of data from disparate sources (OSINT, blockchain, traditional databases), enhancing the effectiveness of detection systems.
- **For criminals**: LaaS providers will use generative AI to create highly believable business documents and synthetic identities. Sophisticated algorithms will automate layering steps, simulating legitimate economic behavior to evade AML checks. AI will make crime more adaptive and difficult to predict.

TOWARDS A WINNING STRATEGY: A Holistic Approach

The challenge against LaaS will not only be played out in the technological field, but will require a holistic strategy based on three pillars:

1. **Speed of response**: Countermeasures must be adapted in weeks, not years. The regulatory and investigative response must be agile, capable of reacting in real time to criminal innovations.
2. **Multi-Actor Collaboration**: A secure and immediate data sharing ecosystem between law enforcement, financial institutions, digital service providers, and intelligence agencies is essential.
3. **Cultural prevention**: Legitimate economic actors need to be made aware of how LaaS can infiltrate seemingly harmless sectors and how to recognise warning signs.

LaaS is set to remain a stable player in the global criminal economy, with rapid and adaptive evolution driven by technology. Victory will not come from a single tool or a single operation, but from a **multi-layered defense ecosystem** where technology, intelligence and *global governance* act as one, anticipating the moves of crime instead of chasing them.

REFERENCES

1) Aldridge, J. and Décary-Hétu, D. 2015. *Cryptomarkets and the future of illicit drug markets*. EMCDDA / Internet and Drug Markets, EMCDDA Insights 21, pp. 23-30. DOI: 10.2810/324608.
Available:
https://www.researchgate.net/publication/296008837_Cryptomarkets_and_the_future_of_illicit_drug_markets
2) Associated Press. 2024. *UK dismantles massive money laundering operations tied to Russian oligarchs and cybercriminals.* AP News, March 6.
Available:https://apnews.com/article/britain-money-laundering-network-russia-crypto-drug-crime-0ccbf95cf4bb0f9dd20c8aa3ea1e1ef2
3) European Union. 2018. *Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law.* Official Journal of the European Union, L 284, 22–30.
4) Europol. 2021. *Serious and Organised Crime Threat Assessment (SOCTA) 2021.* The Hague: Europol.
5) Fanusie, Y. J. and Robinson, T. 2018. *Bitcoin laundering: An analysis of illicit flows into digital currency services.* Foundation for Defense of Democracies (FDD), January 12.

Available: https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf

6) Financial Action Task Force (FATF). 2019. *Guidance for a risk-based approach to virtual assets and virtual asset service providers.* FATF / OECD.
7) Foley, S., Karlsen, J. R. and Putniņš, T. J. 2019. *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?* Review of Financial Studies, 32(5), 1798–1853. DOI: 10.1093/rfs/hhz015.
Available via Oxford / Research repository: https://academic.oup.com/rfs/article-abstract/32/5/1798/5427781
8) Möser, M., Böhme, R. and Breuker, D. 2013. *An inquiry into money laundering tools in the Bitcoin ecosystem.* In: 2013 APWG eCrime Researchers Summit. IEEE.
9) Organized Crime and Corruption Reporting Project (OCCRP). 2014. *The Russian Laundromat.*
Available: https://www.occrp.org/en/laundromat/
10) Organized Crime and Corruption Reporting Project (OCCRP). 2017. *The Azerbaijani Laundromat.*
Available: https://www.occrp.org/en/azerbaijanilaundromat/
11) Organized Crime and Corruption Reporting Project (OCCRP). 2019. *The Troika Laundromat.*
Available: https://www.occrp.org/en/troikalaundromat/
12) Royal United Services Institute (RUSI). 2024. *Operation Destabilise: Russia, organised crime and illicit finance.* RUSI Commentary, March 7.
13) Schmidt, A. 2024. *Impacts of money laundering and terrorism financing: Final report.* Australian Institute of Criminology.
14) United Nations Office on Drugs and Crime (UNODC). 2020. *Global Report on Money Laundering 2020.* Vienna: UNODC.
15) U.S. Department of the Treasury – Financial Crimes Enforcement Network (FinCEN). 2021. *Advisory on ransomware and the use of the financial system to facilitate ransom payments.* October.
16) Wikipedia contributors. 2023. *Operation Virus.* In Wikipedia, March 15.
(Link: https://en.wikipedia.org/wiki/Operation_virus)
17) Wikipedia contributors. 2024. *Operation Destabilise.* In Wikipedia, December 20.
(Link: https://en.wikipedia.org/wiki/Operation_Destabilise)
18) WIRED. 2025. *An $8.4 billion Chinese hub for crypto crime is incorporated in Colorado.* Wired, February 19.