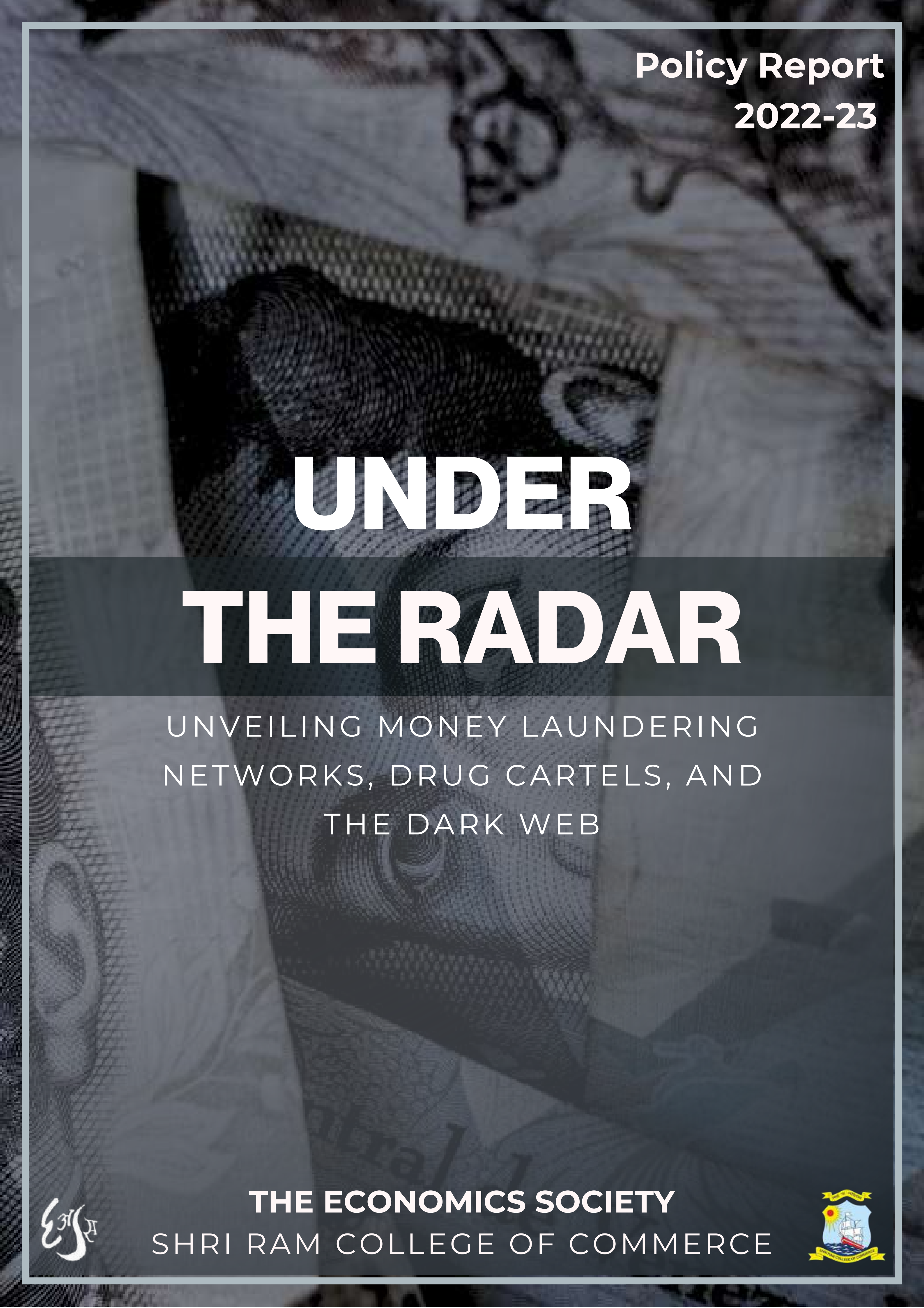


Policy Report
2022-23

# UNDER THE RADAR

## UNVEILING MONEY LAUNDERING NETWORKS, DRUG CARTELS, AND THE DARK WEB

**THE ECONOMICS SOCIETY**
SHRI RAM COLLEGE OF COMMERCE

# TABLE OF CONTENTS

Introduction 01

What is Money Laundering? 02

What is Terror Financing? 05

Organised crime and Money Laundering 17

Cryptocurrency, Dark Web, and Drug Trafficking 21

Hybrid Threats 27

Key Enforcement Agencies 32

Crisis in Sudan 41

AML and Combatting Terror Financing 46

Ransomware, DeFi, Money Laundering: Deadly Combination 55

Effect of CBDC on Money Laundering 59

An international view of Money laundering and illicit activity financing 65

Model 69

Conclusion 75

Testimonial 77

References 79

# Introduction

Raqqa, Syria in 2017 - Amidst the ruins of the city, the Islamic State of Iraq and Syria (ISIS) released a propaganda video of a 10-year-old American boy with a 7-year-old Syrian boy, threatening the erstwhile American president Donald Trump with war while using assault rifles. In October of the same year, a 12-Year-old child soldier executed Kurdish prisoners on camera for a spine-chilling propaganda video.

Travelling to Mexico, clandestine graves in the country's western region with over 30 bodies were discovered in early 2023. They were tied to a string of killings by organized crime groups whose primary business was the drug trade. Widespread violence on the streets of major cities in developing countries is all traced back to organized crime groups operating in the area.

While the events quoted above seem distant and often near fiction, the intricate nexus of all organized violent offences impacts each human life in some way or form. Crimes are not committed against a property, or a geographical area, but against the psyches of people who call themselves citizens of that area.

Whether the crime is terrorism, human trafficking, drug trade, or genocide, it all boils down to a war on the sensibilities and right to life of ordinary people.

In order to combat organized crime and terrorism, it is of foremost importance to understand where such organizations generate funds from. While attacking such organizations' main operations is necessary, it is also necessary to eliminate its main lifeline - money; in order to ensure its termination.

As time has progressed, the capabilities of terrorists and criminals have advanced with the refinements in technologies, which has proved to further exacerbate the difficulties in pinning down sources of funding for these organizations

Through this brief, we aim to understand this nexus, examine its extent, and also propose the adoption of a framework to combat illicit financial transactions being routed through the traditional banking system, through the adoption of upcoming technologies such as Artificial Intelligence and Machine Learning.

# What is Money Laundering?

The United Nations Office on Drugs and Crime has estimated that the extent of money laundering is about **2 to 5% of Global GDP**, roughly equal to **USD 800 Billion to USD 2 Trillion**. Money Laundering is a serious crime that is responsible for fueling terrorist activities, human and animal trafficking, and illicit drug trades and is the cause of shattered economies. However, what exactly is money laundering?

The **UN Vienna 1988 Convention** Article 3.1 describes Money Laundering as "t*he conversion or transfer of property, knowing that such property is derived from any offense(s), for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in such offense(s) to evade the legal consequences of his actions"*.

In simple words, Money laundering is the process of hiding the source of money obtained from illegal sources, such as illegal proceeds from drug trades, terrorist activities, gambling, arms trade, and animal and human trafficking, and converting it to a clean source, thereby avoiding prosecution, conviction, and confiscation of the criminal funds and thus converting the illegal black money into white money.

**History of Money Laundering:**

It is a common misconception that Money Laundering originated in recent centuries. A simple form of Money Laundering dates back more than a thousand years. In "Lords of the Rim", Stirling Seagrave explains how, in **China** around **4000 BC**, some of the Chinese merchants would hide their wealth from rulers to avoid paying taxes and invest it in businesses in remote provinces or even outside China.

The origin of Money Laundering in the Modern World is in the 1920s, when the US officially went dry when it banned the sale, manufacture, and transportation of Alcohol. During this time, Alphonse Gabriel Capone, an American gangster and the leader of the Chicago Outfit, would smuggle and bootleg liquor. This gang would invest the illegal proceeds into cash-heavy businesses such as the laundry business. It is where the term money laundering" was coined, and in the words of Alphonse himself, "Money laundering is called what it is because that perfectly describes what takes place: illegal, or dirty, money is put through a cycle of transactions or washed so that it **comes out the other end as legal**, or clean, money. In other words, the source of illegally obtained funds is obscured through a succession of transfers and deals in order that those same funds can eventually be made to appear as legitimate Income." Since the major investment of the proceeds was laundry, the cleaning of the money has been compared with the cleaning of the clothes in a laundry, hence the term "Money Laundering".

However, the term "Money Laundering" initially appeared in the newspaper only in 1973, during the **Watergate Scandal** in the US, which was a political scandal involving then-President, Richard Nixon's administration, and led to his resignation in 1974. In the 1980s, when the world started to take a deeper interest in the matters of Money Laundering, the term "Money Laundering" was finally used in a legal context by the United States District Courts, Southern District of Florida, in the case that was tried in 1982 United States of America, vs. Four Million Two Hundred Fifty-FiveThousand Six Hundred and Twenty-Five Dollars and Thirty-Nine Cents($4,255,625.39). (Money Laundering and its fallout, ASSOCHAM INDIA, 2013)

**Stages of Money Laundering:**
Money Laundering is not a single act but rather involves a series of stages which are:

- **Placement:** It refers to the physical disposal of bulk cash proceeds derived from illegal activity. At this stage, the launderer infuses the black money into a legitimate financial institution. This is the first step of the money-laundering process, and the ultimate aim of this phase is to remove the cash from the location of the acquisition so that it does not attract attention from the authorities. This is achieved by investing criminal money into the legal financial system by opening up a bank account in the name of unknown individuals or organizations and depositing the money in that account. This is a high-risk stage of the laundering process because large amounts of cash are pretty conspicuous, and banks are required to report high-value cash transactions.
- **Layering:** refers to the separation of illicit proceeds from their source by creating complex layers of financial transactions. It involves sending

the money through various financial transactions to change its form and make it difficult to track. It conceals the audit trail and provides anonymity, and this process consists of several bank-to-bank transfers, wire transfers between different accounts in different names in different countries, making deposits and withdrawals to continually vary the amount of money in the accounts, changing the money's currency, and purchasing high-value items to change the form of the money. Nowadays, **Electronic Funds Transfer (EFT)** has come as a boon for such layering exercises. Different techniques like correspondent banking, loans at low or no interest rates, money exchange offices, back-to-back loans, fictitious sales and purchases, trust offices, and recently, **Special Purpose Vehicles (SVPs)** are utilized to launder the money. This is the most complex step in any laundering scheme, and it's all about making the original dirty money as hard to trace as possible.

- **Integration:** Integration refers to re-injecting money into the mainstream economy. Under this process, the laundered proceeds re-enter the economy in legitimate-looking forms; they appear to have come from a legal transaction.

Launderers normally accomplish this by establishing unknown institutions in nations where secrecy is guaranteed. Under this process, a final bank transfer is made into the account of an unknown institution in which the launderer is investing in exchange for a cut of the profits. At this point, the launderer can use the money without getting caught. It is very difficult to catch a launderer during the integration stage if there is no documentation during the previous stages

# What is Terror Financing?

Bags of money changing hands, illicit transfers, huge ransoms—one thing of such instances when we talk about terror financing. But in actuality, terror financing is an extremely nuanced concept, one which is tied deeply to money laundering.

Terror financing is the fuel for one of the largest threats to humanity all across the world. For the copious amount of disaster each attack leaves in its wake, be it infrastructural, emotional, psychological, or societal, each attack tends to cost minuscule amounts. The most quoted example of this phenomenon is how **9/11 cost Al-Qaeda a total of $400,000-USD**, and wrecked a catastrophe whose economic cost is outlined in a report by "the Institute for Analysis for Global Security" (U.S. State Department, N.A.)

"Counting the value of lives lost as well as property damage and lost production of goods and services, losses already **exceed $100 billion**. Including the loss in stock market wealth—the market's estimate arising from expectations of lower corporate profits and higher discount rates for economic volatility -- the price tag approaches $2 trillion.

**Among the big-ticket items:**

The loss of four civilian **aircraft** valued at **$385 million**.

The destruction of major buildings in the **World Trade Center** had a replacement cost of from **$3 billion to $4.5 billion.**

Damage to a portion of the **Pentagon: up to $1 billion**

**Cleanup costs:** $1.3 billion.

**Property and infrastructure damage:** $10 billion to $13 billion

**Federal emergency funds** (heightened airport security, sky marshals, government takeover of airport security, retrofitting aircraft with anti-terrorist devices, cost of operations in Afghanistan): **$40 billion**

The amount of damaged or unrecoverable **property** reached **$21.8 billion**.

Losses to the **city of New York** (lost jobs, lost taxes, damage to infrastructure, cleaning): **$95 billion.**

Losses to the **insurance** industry: **$40 billion**.

Loss of **air traffic revenue: $10 billion.**

**Fall of global markets: incalculable.”** (U.S. State Department, N.A.)

To fulfil their needs, terror groups resort to the use of various avenues of raising finances:

1. Counterfeiting of goods
2. Counterfeiting of Currency
3. Drug trafficking
4. Extortion/ransom
5. Human Trafficking
6. Donations and contributions by NGOs, individuals, etc.
7. Smuggling of antiquities

**Counterfeiting of goods**

The theft of intellectual property rights through counterfeiting and pirating of consumer goods is a huge and growing criminal enterprise. It is estimated that counterfeit merchandise accounts for between **5 and 7 per cent of all the goods moved in world trade**. According to Interpol, this counterfeit merchandise is worth approximately **$460 billion annually.** According to the U.S. Trade Representative, American businesses lose as much as $250 billion each year to counterfeiters.

Popular belief outlines this as follows:
1. Counterfeiting is a victimless crime;
2. Drugs are the major source of terror financing.

**Both of these widely held perceptions are false**.

Deconstructing both points: counterfeit goods usually sell for a street price that is about 2000% inflated, whereas **drugs** only have a profit margin of **100–200%**. There have been multiple instances of terror attacks being funded through money raised from counterfeit goods. Two of the perpetrators of the **2014 Charlie Hebdo attacks** raised money by selling counterfeit trainers. Pirated music CD sales were the source of funding for the 2004 Madrid commuter train attacks, and a 2002 Al Qaeda training manual explicitly outlines how counterfeiting of goods can be used to fund terror plots.

A document by the UNODC outlines the process of laundering money raised by terror organisations via the three-step process mentioned above, namely, placement, layering, and integration.

This three-stage process, though widely cited, also has certain **blind spots** that we must address. The three-stage process assumes that the money coming in is illicit or dirty, and hence there is a need for its placement before the latter steps are undertaken. It fails to take into account that money on which **tax is not paid, which was placed in the books**, is also in need of laundering, makes up a large chunk of money laundering activity, and can also be used for terror finance. This money goes straight to stage 2 of the above-mentioned process.

While many of us willingly buy counterfeited products, not thinking beyond the probable losses the company making the original might face, **we remain largely impervious to the sinister pitfalls of supporting counterfeiting in society**. (FATF, 2015)

**Counterfeiting of Currency**

There is a thin line between financial terrorism and terror financing and counterfeiting of currency treads that particular line. The concept of the **injection of fake physical currency into an economy** is widely known to create havoc as the currency starts losing its value under the aegis of financial warfare or terrorism, but what we often discount are the steps preceding this process, which directly fund terror organizations.

**Russia:**

In a complaint brought before the US District Court for the Eastern District of Pennsylvania, the jury detailed efforts by defendants X, Y, and Z to sell the cooperating witness (CW) counterfeit United States currency for the purpose of raising funds for terrorist organisation A. In total, the conspirators provided the CW with approximately $9,800 in counterfeit US currency. From around July 2008 through to around November 2009, in the Eastern District of Pennsylvania and elsewhere, the accused conspired and agreed with others known and unknown to the grand jury to commit offences against the United States, that is, to provide “material support or resources,” including false documentation, false identification, currency, monetary instruments and financial securities, to a designated foreign terrorist organisation.

This conspiracy led the accused and others known and unknown to the grand jury to commit the following overt acts, among others, in the Eastern District of Pennsylvania and elsewhere:

Around 18 September 2008, X met with CW and stated that Country P manufactured high-quality counterfeit US currency for the benefit of terrorist organisation A and that, consequently, representatives of A would need to approve the sale of this type of counterfeit currency. Around 25 November 2008, Y met with the CW in Philadelphia to discuss the sale of counterfeit United States currency. Around 24 February 2009, Z caused his assistant ("Individual A") to deliver a sample of counterfeit EUR 200 and USD 100 notes to the CW. Around 25 April 2009, defendant X met with the CW in Florida and told the CW, among other things, that Hezbollah's representatives worked 18 to 20 hours a day counterfeiting many currencies, including those of the United States, Kuwait, Saudi Arabia and the European Union.

Around 3 September 2009, X confirmed to the CW via telephone that he had mailed a package that the CW received in Philadelphia that same day containing approximately USD 9200 counterfeit US currency hidden inside a photo album.

**Source:** Charges brought before the United States District Court for the Eastern District of Pennsylvania,
United States of America v. Hassan Hodroj & Others, Date filed: November 24, 2009.

The above instance is one of many where terror groups have used the counterfeiting process to fund their core operations. While the overarching theme of counterfeiting does point towards financial terrorism, the first step, which is **printing counterfeit currency, is a crucial aspect for ensuring the continuity of a terror organisation**, which comes about from financing its operations such as procurement of goods and weapons, training of militants, propaganda, and most importantly, attacks.

This method, however, is fairly limited to certain parts of the world, with Hamas and Hezbollah being prominent organisations working in association with other organized crime groups in the border areas of Argentina, Brazil, and Paraguay. Tamil networks and Al-Qaeda also use counterfeit currency to finance their operations. (FATF, 2015)

**Drug Trafficking**

Drug trafficking is probably the most widely known source of terror financing. In recent years, with the focus on the Taliban having grown due to their seizing of power in Afghanistan, the role of the drug trade has come to the forefront, as it is one of the Taliban's major sources of funding. Reports suggest the total potential value of Afghanistan's 2006 opium harvest accruing to farmers, laboratory owners, and **Afghan traffickers reached about $US3.1 billion.**

This is a fairly lucrative source of money for terror organisations, as increased scrutiny by law enforcement agencies has led to the drying up of a large number of revenue streams. While the investment in the drug trade is low, the profits reaped are relatively high.

The two major substances traded by terror groups are opiates and cocaine. The origin of the majority of **opiates** can be traced to the **Afghanistan** region, and **cocaine** comes from **Latin America**, especially Colombia in particular. There has also been an uptick in the penetration of synthetic drugs into this market.

The nexus of drug trafficking and its links to terror financing is multifaceted in the context of where the finances flow in. Exchanges of assets as payment for drug shipments are hugely popular, particularly the use of real estate as a payment.

A large chunk of the involvement of terror groups in the drug trade on the internet comes in the following forms:

1. **Individuals** selling on discussion forums (predominantly in the Darknet)
2. **Online storefronts**, operated by one individual or group of individuals
3. **Online marketplaces**, connecting buyers and sellers but not selling anything themselves

The proceeds of the drug trade are laundered in a highly sophisticated manner through professional money laundering services. The Following case study aptly describes one such instance and the operation of such entities.

The Russian FIU (Rosfinmonitoring) detected several non-resident individuals, ethnically linked to opiate-producing and transit countries, making multiple cash deposits on their bank card accounts.

The money deposited was immediately transferred to Company A, established in the British Virgin Islands, with its accounts held in Latvian banks. The money was also transferred to companies in the **UAE, China, Turkey, Hong Kong, China, and Latvia.** A financial investigation into the heroin financing activities of the network identified further offences. The same offshore company A received money from a large construction company acting as a governmental contractor, presumably with the purpose of **embezzlement of public funds** and tax evasion. In its turn, the offshore company transferred the money to accounts of Russian companies related to the timber industry. Following a chain of transactions, the money was withdrawn in cash. The **Federal Drug Control Service** confirmed that the individuals were receiving the proceeds of opiate trafficking in cash from the dealers. (FATF, 2015)

**Extortion/Ransom**

Kidnapping and extortion are fairly easy ways to generate revenue. This stream in particular marks the direct funding of terror activities by the West.

Statistics related to kidnapping and terror financing led to the following revelations:

1. Between 2008 and 2014, Al-Qaida and its direct affiliates made at least **$125 million** in revenue from kidnappings, **$66 million** of which was collected in **2013**
2. **Abu Sayyaf Group** has participated in kidnappings where around $1.5 million in ransoms were collected by 2014, with approximately half that amount collected in 2012 and 2013
3. It is estimated that Al-Qaeda in the Islamic **Maghreb** received $75 million in ransom payments between 2010 and 2014

This method accounted for a very minor chunk of the financing of terror activities between 1970 and 2010 **(6.9%)**, but with time, there has been a marked uptick in the usage of these means for finance. As of 2016, **kidnapping alone accounted for 15.8% of all terror activity**.

The Abu Sayyaf Group (ASG) in the Philippines acts as an interesting study for this phenomenon.The Abu Sayyaf Group (ASG) in the Philippines acts as an interesting study for this phenomenon.

Although ASG was first created to advance political goals,

**Human Trafficking**

Several UN Security Council Reports underline the use of the Human trafficking nexus for terror financing. Human trafficking in itself is one of the most profitable organised crime-related activities and generates about **$150 Billion** in profits. While this nexus is difficult to demonstrate, it is a highly potent source of terror financing, and reports of several instances have proven that speculations about this nexus are both concrete and theoretical.

Strategic use of human trafficking-related activities to

➢ Spread terror and advance **ideology**

➢ **Intimidate** populations and decimate communities

➢ **Institutionalize** sexual violence and slavery

➢ **Incentivize** and bolster recruitment

Human trafficking-related activities can also constitute an opportunistic source of revenue

➢ Captives sold in open **slave markets** or through online auctions

➢ Captives used as instruments to perform support/servitude roles

➢ Captives used as means to secure ransom/rescue payments

## Case Study:

After the siege on the Yazidis on Sinjar Mountain in August 2014, Islamic State fighters separated the men from the women and children, took the young girls and abused them sexually, raped them, and committed other sexual violence against them related to the conflict; they were taken as sex slaves. The slaves were first offered to the Islamic State leaders, then to foreign buyers for thousands of dollars, and finally to Islamic State fighters for around $165. The Islamic State itself confirmed the sexual slavery of female captives in the price list of the slaves that it distributed. The list was authenticated by the Special Representative of the UN Secretary-General on Sexual Violence in Conflict, Zainab Bangura. In addition, there is evidence of attempts by the Islamic State to sell sex slaves on the Internet.

Another document published by the Islamic State concerning sexual slavery is "Questions and Answers on Taking Captives and Slaves." The article provides ideological and religious justifications for sex slavery and human trafficking and provides permission from religious scholars to take non-Muslim women captive, and to buy, sell, or gift them as slaves since they are barely property. (FATF, 2015) it has grown increasingly fond of abduction for ransom. The main focus of ASG's actions is kidnapping, and despite being repeatedly called a terrorist organisation in the Philippines throughout its existence, it has repeatedly increased its criminal activity at the expense of its terroristic, political, and ideological goals. ASG maintains connections with other terrorist groups like the Indonesian terrorist group Jemaah Islamiya and the Moro Islamic Liberation Front (MILF), which is an Islamist separatist organisation located in the Philippines.

ASG relied on training and funds from Al Qaida for a while but was cut off in the 1990s as a result of growing pressure from Philippine authorities. After this source of money was cut off, ASG turned to criminal activity, including kidnapping for ransom, which provided over 90% of its funding, to maintain its survival. The ASG relied on the money it made from abductions to recruit new members, and it learned much of its criminal tactics from other terrorist organisations.

According to **McKenzie O'Brien's 2012 research** of ASG, changes in its leadership, membership, structure, and connections to criminal and terrorist organisations were factors in the organization's transition from a terrorist to an organized crimiminal syndicate.

This case study examines ASG's dual identities as terrorists and kidnappers and, using O'Brien's methodology **makes inferences about the reasons why a terrorist cell would abandon its ideological goals in favour of the criminal enterprise's financial ambitions**. (UNODC, n.d.)

The Global Terrorism Database reports that while the number of kidnapping attacks in the Philippines has remained stable over the past few years, the number of **victims increased** by at least 70% between 2015 and 2016 (from 127 victims in 2015 to 218 in 2016), and the number continued to rise in 2017 when there were a total of 408 kidnapped/hostages in the nation (out of a total of 8,937 victims recorded worldwide). Although ASG does not engage in all abduction for ransom actions in the Philippines, it is thought that the organisation of fewer than 500 individuals is accountable for raising more than $35 million from such activities between 1992 and 2008. (FATF, 2015)

**Donations and contributions by NGOs, individuals, etc.**

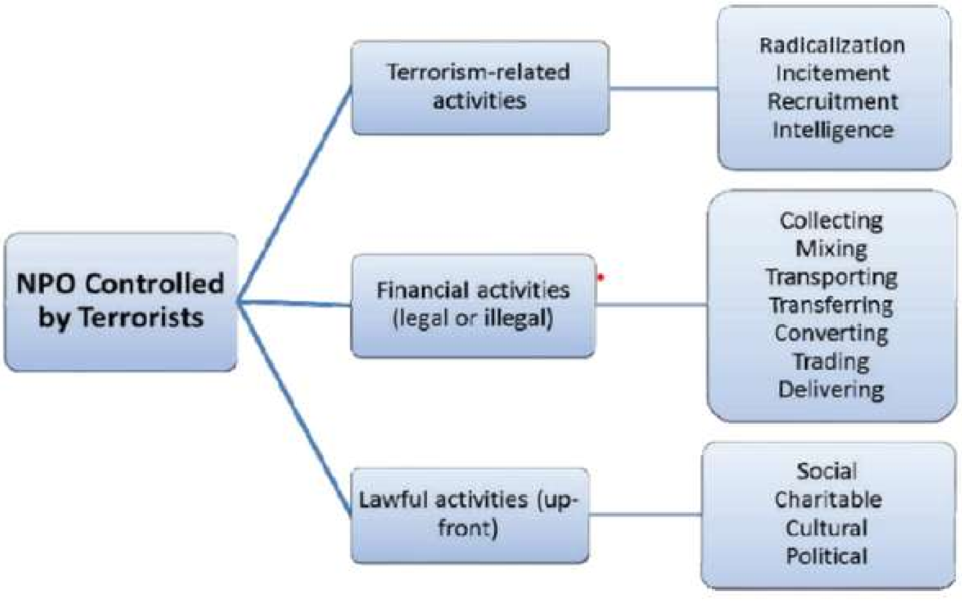
Multiple cases have been reported of individuals contributing to terror activity through donations, which primarily take place through digital currency like Bitcoin. **By using digital currencies, argues the Jihadi author under the pseudonym of Amreeki Witness, "one can prevent his 'brothers' who live outside the borders of the Caliphate from having to pay taxes to the infidels while simultaneously financing the mujahideen without exposing them to any legal risk"**.

NGOs, in the name of religious activity, have also been implicated in indoctrination and collecting funds for terror activities. An examination of the typologies of the activities related to NGOs controlled by terrorist organisations can be seen below:

This phenomenon can be better demonstrated by the following case study:

In 2008, an NPO called "Redvivir"—headed by an alleged member of the political wing of the **Marxist Terrorist Guerrilla FARC**, Jaime Cedano Roldán—was granted 81,378 euros to conduct a development project in Puerto Brasil, a rural area in Colombia. The Foundation that granted this funding—which came in turn from a Fund of the municipality of Sevilla, Spain—was "DeSevilla", a local political Foundation headed by Antonio Torrijos, a member of Spain's communist-leaning party Izquierda Unida.

In this case, in addition to a typology commonly used by terrorist-controlled NPOs — i.e. a request for funding to undertake



a development project—several red flags should have been addressed: the head of the NPO had been one of the heads of the extinct "Union Patriotica", a political wing of FARC; the development project was vaguely described and its objectives were not clearly defined; the authorities of the beneficiary area of the project, Puerto Brasil, Viotá, Cundinamarca, Colombia, were not aware of the project; the proposed development projects were not in line with usual economic activities in the region—i.e. **mostly seasonal and weekend tourism**; and finally, as of October 2010, no spending details or invoices had been provided by Redvivir or DeSevilla.

Although the case is still under investigation, it should be made clear that, contrary to the Peruvian Academy case, nowadays analysts, investigators, and prosecutors have a larger number of tools to effectively address alleged criminal activity. In addition to the international legal instruments in place and their applicable provisions, Colombia and Spain are two of the countries with the most developed counter-terrorism and counter-terrorism financing legislation in the world. Moreover, Colombia and Spain effectively cooperate and exchange information with one another, which are certainly key aspects to ensure a successful investigation and prosecution of any terrorism financing case. (FATF, 2015)

**Smuggling of Antiquities**

Smuggling invaluable antique pieces has been a prominent source of terror financing. Much of the antiquities on the international black market are being traded as a consequence of terror financing.

As a UNSC report from 2015 points out, **frequent looting of cultural heritage sites by terror organisations such as ISIL (Islamic State of Iraq and the Levant)** is a direct income stream for these organisations. A marked proliferation in the arts and antiquities black market-related activities

The United Nations Office on Drugs and Crime (UNODC) has as much as **USD 6.3 billion** in illicit proceeds that could have been laundered through or associated with the trade in cultural objects. (FATF, 2023)

Vulnerabilities Linked to the Market:

1. **Primary Market** - In the Primary Market, the risk of Money Laundering and Terrorist Financing is the least, as the artists and their representatives may prefer to choose buyers who will enhance the artist's reputation or prestige, and may avoid transacting with buyers that could create a negative perception of the work or artist.
2. **Secondary Market** - This market is more vulnerable to Money Laundering and Terror Financing as the seller lacks the incentive to scrutinise the buyer as he is not concerned with the reputation of the buyer, nor is he so keen to enquire about the source of funds, so long as he gets the required payment.
3. **Privacy of The Buyer in the Market -** The market for cultural objects has a history of privacy and discretion. This protects sellers and buyers from being targets of theft or other crimes and helps ensure that high net-worth individuals are not charged a higher price if their identities are known to the seller. This may create vulnerabilities in terms of countering the risk of Money Laundering and Terror Financing, for example, where cultural objects can be purchased anonymously in cash, it complicates the traceability of transactions. Also, The use of intermediaries and legal persons in the buying and selling process is relatively common in the market, which in certain cases can act to obscure the identity of the ultimate seller or purchaser. (FATF, 2023)

**Money Laundering threats associated with Cultural Objects:**

1. **Using Cultural Objects to Hide or Transfer Illicit Proceeds -** Pieces of high value could be used as a vehicle to transfer or hide illicit proceeds.

1. **Under or Overvaluing an art piece to pay bribes -** Sometimes, overvaluing an art piece can be a tool to launder money. A complex channel is used to mislead enforcement agencies from tracing the original possessor of the artwork. In numerous instances, the same has been used to bribe officials and compromise core government functions

1. **Forgery -** This is yet another way of laundering money,

mainly because it is difficult for the buyers to distinguish between a forged and a real painting.

A prominent example of this is the Bouvier Affair in 2016. Yves Bouvier, a Swiss art dealer, sold a forged painting to a Russian Billionaire Dmitry Rybolovlev for 118 million euros. He used a complex series of transactions to hide these illegal proceeds and to evade taxes.

provides anonymity to the buyers and sellers thus, making it more difficult for the authorities to trace it.

However, in the crypto era, **the use of cryptocurrencies is becoming increasingly common for money laundering through artworks** as it is even safer.

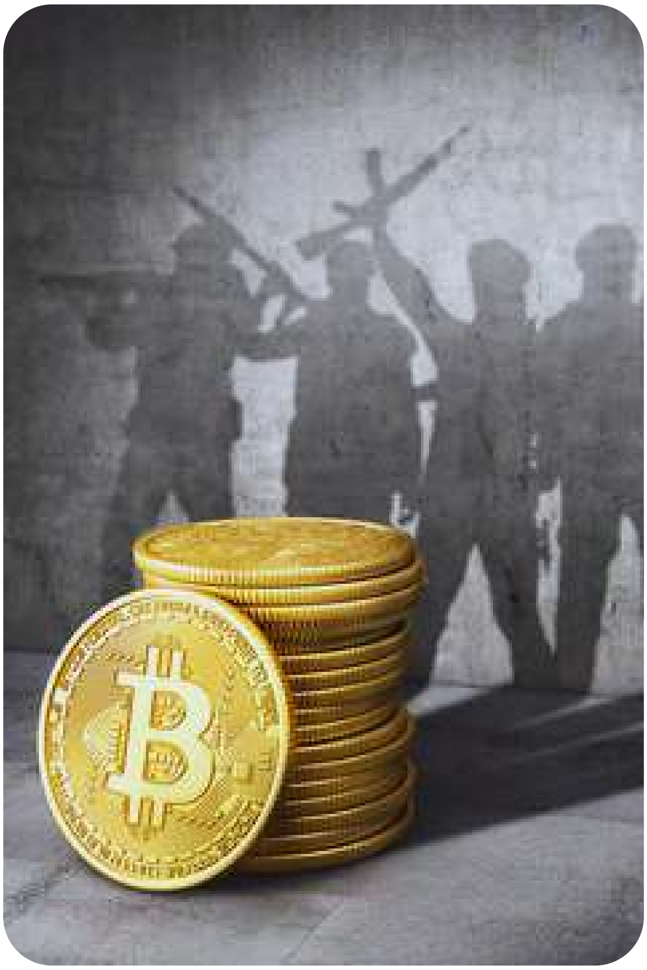
# Organised crime and Money laundering

Organised crime and money laundering are two distinct yet interdependent activities that have become increasingly prevalent in today's global society. Organised crime refers to criminal activities that are planned, coordinated, and carried out by a group of individuals, often for financial gain. Money laundering, on the other hand, involves the process of concealing the true source and ownership of funds obtained through illegal activities.

**Interconnection between Organized Crime and Money Laundering:**

Organised crime groups often engage in illegal activities such as drug trafficking, human trafficking, arms trafficking, and financial fraud. These activities generate large amounts of cash, which cannot be deposited in a bank without attracting attention from law enforcement agencies. Therefore, organized crime groups use **money laundering techniques to "clean" their illicit proceeds**, making them appear to be derived from legitimate sources.

Money laundering techniques typically involve a **complex web of financial transactions** designed to disguise the origin and ownership of the funds. For example, funds may be transferred through a series of offshore accounts, shell companies, and trusts, making it difficult for law enforcement agencies to trace the source of the funds. The use of **cryptocurrencies and other digital assets** has also made it easier for organized crime groups to launder their illicit proceeds. (Levi, n.d.)



**Impacts of Organized Crime and Money Laundering are as follows:**

The impact of organised crime and money laundering on society is significant. These activities **undermine the rule of law and create a culture of corruption,** which erodes public trust in government institutions. They also harm the global economy, as they divert resources away from legitimate businesses and investment opportunities.

In addition, organised crime groups often engage in violent activities such as extortion, kidnapping, and murder to protect their criminal enterprises. This creates a climate of fear and insecurity, which can have a devastating impact on the communities in which they operate.

Some examples of Organised Crime and Money Laundering in order to elucidate the workings of these nexuses:

- Cybercrime - Carbanak Group:

The Carbanak Group was an international cybercrime organisation that used malware to steal millions of dollars from banks and financial institutions. The group operated for several years and used sophisticated money laundering techniques to conceal their activities. In 2018, several members of the group were arrested and charged with various offences, including money laundering.

- Fraud - Bernie Madoff:

Bernie Madoff was a financier who ran a massive Ponzi scheme. Madoff used fake investment returns to attract investors and used new investments to pay off old investors, instead of investing the money as promised. Madoff's scheme lasted for several years and resulted in billions of dollars in losses for investors. Madoff was eventually caught and sentenced to 150 years in prison for his role in the fraud and money laundering.

- Counterfeiting - Operation Bernhard:

Operation Bernhard was a Nazi counterfeiting operation during World War II. The operation involved the production of high-quality fake British pound notes, which were used to destabilise the British economy. The counterfeit notes were distributed through various channels, and the proceeds were used to fund other Nazi activities. The operation was eventually uncovered, and several members of the counterfeiting team were arrested and charged with money laundering and other offences.

- Smuggling - Zhenli Ye Gon:

Zhenli Ye Gon was a Mexican businessman who was accused of smuggling large quantities of precursor chemicals into Mexico, which were used to produce illegal drugs. Ye Gon was also accused of money laundering, and authorities seized over $205 million in cash from his home in Mexico City. Ye Gon was eventually extradited to the United States and sentenced to 25 years in prison for drug trafficking and money laundering

## FOCUS : DRUG TRAFFICKING

There is a very close connection between Money Laundering and Drug Trafficking, and it is of special importance, as drug trafficking also holds close links with terror finance operations.

Drug Trafficking is a **multi-billion dollar industry** that generates a huge amount of cash. Drug traffickers use various methods to legitimise their illicit gains and integrate them into the global financial system.

One of the most common methods used is to use front companies or shell companies. The illicit proceeds from the drug trafficking are transferred to these **shell companies** and then legitimate operations are done through these companies to launder money. One of the most famous examples of such laundering is the Mexican Drug cartel led by Trevino Morales's Brother, who would transfer the illicit drug proceeds to the bank accounts of the main shell company" Tremor Enterprises". These funds were used to buy racehorses and were sold between the shell companies themselves. All of these complex transactions gave an appearance that the business was legitimate and hence, was able to launder the drug proceeds successfully.

Another method of laundering the proceeds is to accept the drug payments in virtual currencies, such as Bitcoin and other cryptocurrencies. The transaction parties remain anonymous and as a result, it makes it difficult for the authorities to trace the source of the funds. Another way through which the funds are laundered is by purchasing **real estate** and other assets and then making a couple of complex transactions so that the money comes out “laundered”.

So, the drug dealers who use conventional methods of trafficking and selling have a lot of cash. To such an extent that even a single lone drug dealer who was not a part of any cartel was able to generate **20 to 25 million dollars** in cash. The hardest part for a lone dealer was to hide this cash from the authorities, for which they would hide it in their backyard or any place they could. To try to legalise it they would give this money to their friends and ask them to gamble in a casino, so that in the end when they receive the receipt from the casino, it's all legal. Also, they would show some money as a gift from family and relatives, because to some amount, for any gift received, you do not need to show proof of such receipt.

Also, some would invest in a **cash-intensive business**, say a salon or a clothes laundering business, so that they could show the black money as income received from that business and since it's mostly cash, they get scot-free.

Also, they would go through complex transactions such as buying a real estate property through a shell company and selling it to others, and declaring that receipt as the income of the shell company to make it appear legitimate.

Of course, these techniques have a shortcoming and if the authorities really get active, they can trace all of it, but the inefficient system that prevails just does not let that happen and as a result, a single lone drug dealer can earn millions of dollars. Such is the impact of drug trafficking and ML. (Report of the International Narcotics Report Board,2021)

# Cryptocurrency, Dark Web and Drug Trafficking

The use of cryptocurrency in dark web drug trafficking has become a growing concern for regulatory authorities. With the rise of **deep web marketplaces (DWMs)** and cryptocurrencies, many challenges have been posed to law enforcement agencies in their efforts to stop the spread of illicit substances.

Cryptocurrencies like Bitcoin are often used in these transactions due to their **anonymity and lack of regulation.** Transactions can be made without revealing the identity of the buyer or seller, making it difficult for authorities to track down those involved in illegal activities. Cryptocurrencies are not subject to government regulation, which makes them an attractive option for those looking to conduct illegal transactions.

The deep web drug marketplaces are set up in a way that allows **communication and information exchange** between interested parties, which is one of the many reasons why they have expanded into the deep web. So, it operates through closed-access forums and sites on the deep/dark web.

**How do cryptocurrency deals work on the dark web?**

The practical working of cryptocurrency is as follows :

- Buyers and sellers agree on a price for the drugs being sold, typically denominated in Bitcoin or another cryptocurrency.
- The buyer sends the agreed-upon amount of cryptocurrency to the seller's digital wallet address.
- Once the seller receives the payment, they send the drugs to the buyer through a variety of methods, such as mail or courier services.
- The transaction is recorded on a public ledger called a blockchain, which allows anyone to view the transaction history associated with a particular wallet address.
- Considering Cryptocurrencies are decentralised and not subject to government regulation, transactions can be conducted anonymously without revealing the identity of either party involved.

While this process may seem straightforward, there are many risks associated with buying drugs online using cryptocurrencies. For example, buyers may receive counterfeit or dangerous substances that can cause harm or even death. Additionally, sellers may not deliver products as promised or may scam buyers out of their money.

Cryptocurrencies have been associated with criminal activities on the dark web, but they also have legitimate uses and **potential benefits**. Let's take a closer look at some examples of both.

On the criminal side, there are several active dark markets that facilitate illegal transactions using cryptocurrencies. For example, AlphaBay was a popular dark market that allowed users to **buy and sell drugs, weapons, and stolen information using cryptocurrencies.**

In 2017, AlphaBay was shut down by law enforcement agencies in a joint operation between the US and several other countries.

The next case is the **WannaCry ransomware** attack in 2017, which demanded payment in Bitcoin from victims in exchange for unlocking their files. The attackers were able to collect over $140,000 worth of Bitcoin before being caught by law enforcement.

Another recent case involves the seizure of over **$1 billion** worth of Bitcoin by US authorities from an alleged Silk Road drug dealer. The dealer was arrested in 2020 and charged with various crimes related to drug trafficking on the Silk Road marketplace. These marketplaces offer a wide range of drugs for sale, including opioids, stimulants, and hallucinogens.

However, it is important to note that not all cryptocurrency transactions on the dark web are illegal. Some individuals and businesses use cryptocurrencies to facilitate cross-border transactions or to **avoid high transaction fees associated with traditional banking methods.** For example, some freelance workers may receive payment in cryptocurrencies from clients overseas.

Furthermore, there are legitimate cryptocurrency projects that aim to solve real-world problems and provide innovative solutions. One such project is **VeChain, which uses blockchain technology to improve supply chain management by providing transparency and traceability for products from creation to delivery**.

While cryptocurrencies have made it easier for individuals to buy and sell drugs online anonymously through DWMs, they also pose significant risks. It is important for regulatory authorities to continue to monitor these marketplaces and work to develop new technologies that can help track down those involved in illegal activities. Additionally, it is important for investors and users alike to weigh the risks and benefits before engaging in any cryptocurrency transactions or investments.

### Terror operations on the dark web :

Though the advent of the dark web is fairly recent, terror organisations have used it for conducting and primarily expanding their operations.

Recently, terror organisations have shifted to the use of encrypted platforms such as Telegram for communication purposes. However, the foundations of this method of communication lie in the advent and usage of the dark web.

Terror organisations frequently used the dark web to spread propaganda and communicate with supporters through masked means, until **encrypted messaging platforms like Telegram** came in, which allowed users to send messages to unlimited recipients at once. Terror organisations, however, continue to use the dark web to expand their functioning as they argue that it facilitates greater security and control of traffic.

The most prominent use of the dark web by terror groups though, lies in the use of **dark net currencies**. The popularity of this form of funding among such violent actors has been steadily growing since 2012. In 2014, an article titled, “Bitcoin wa Sadaqat al-Jihad” which translates to “Bitcoin and the Charity of Violent Physical Struggle,” was published online.14 The article promotes the use of Bitcoin virtual currencies as a means of facilitating economic support for jihadists and circumventing the Western banking system.

Numerous instances of these actors using digital currencies over the dark web through donations from supporters have surfaced. A case in point lies in the story of Zoobia Shahnaz of Long Island who was indicted by the Federal District Court of New York in 2017 for bank fraud and money laundering that allegedly supported terrorism. Shanhnaz was accused of having defrauded several financial entities, stealing and laundering over $85,000 of illegal returns using Bitcoin digital currency and other digital currencies which were then transferred out of the country in order to support ISIS. (RAND Corporation, 2019)

The availability of data dumps from hacks has also helped terrorists fund their operations. A jihadist group from Indonesia acquired stolen identities from the dark web, and used them on a hacked Forex trading account, hence raising $600,000 by using the points of the member. Multiple instances have led authorities to believe that the **dark web is being actively used by such violent actors and has the potency to facilitate more havoc to the world order.**

Though widely believed that the dark web masks the identities of its users, documents leaked by **Edward Snowden** in 2014 revealed that the **NSA closely monitors the users** of the TOR browser, by automatically fingerprinting them, essentially enabling the NSA to know the identity of millions of Tor users. According to a report from the German media outlet Tagesschau, there are **nine servers running Tor**, including one at the Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory. All are under constant NSA surveillance. (The Guardian, 2013)

**Dimensions of Deep Web :**

The Deep Web has various aspects and dimensions, yet we see that the social media and the media have so long portrayed it in a very negative light, which is to a great extent true, but both sides of an issue should be duly looked at if all any policy is to be implemented or enhanced.

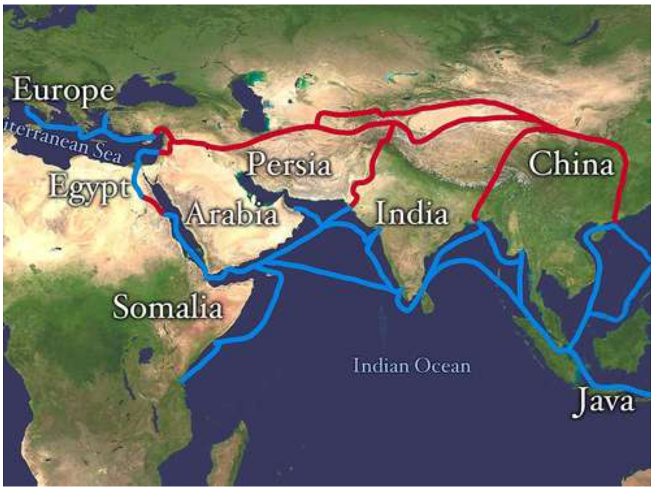
- **Social Dimension** - From a social perspective, the Deep Web is connected to important ongoing discussions about positive and negative uses of encryption and algorithms and how online anonymity can be integrated into everyday life.

- **Cultural Dimension** - From a cultural point of view, it promotes the development of new communities and practices in cyberspace.
- **Political Dimension** - From a political dimension, these technologies enable citizens, not only of authoritarian regimes but globally, to exercise civil liberties and access free information.
- **Economic Dimension** - From the economic side, crypto markets and cryptocurrencies utilise Deep Web systems and environments to propose a new trade logic.

### Abatement of Crime vs. Flourishing of Crime:

The proponents of the Dark Web believe that the illegal activities taking place through the Dark Web are actually good. Now, prima facie, it seems implausible, but an intricate analysis of the statement reveals some interesting facts. Due to online trading of illicit drugs, street-related **drug crime gets reduced** which happens due to physical trading. Although it is true that there is a positive correlation between drug use and drug abuse, there are some addicts who intake drugs because of addiction and who, on being intoxicated, do not cause any kind of violence or destruction. Other crimes such as human trafficking get abated when things are done through the web anonymously. The other side of the argument is that although the seriousness of crime is abated through the Dark Web, there is a greater **ease in committing crime.** Individuals who are new to the dark world of crime will find it easier to commit crime and also, the anonymity of users makes it even more difficult to track them. This acts as an incentive for the new people to enter the doomed world of crime.

### FOCUS: The Silk Road and The Man from Ohio



In 2011, there existed a black web market, by the name - of Silk Road, where users bought and sold practically everything — including fake passports, illegal narcotics, weapons, hacking software, and dangerous chemicals.

This website was although shut down by the FBI in 2013, with the mastermind Ulbricht, who operated on the site under the pseudonym “**Dread Pirate Roberts**,” serving a life sentence in prison since 2015. According to the government, “several thousand drug dealers” used the Silk Road to sell drugs and other illegal products to over 100,000 anonymous buyers and to launder hundreds of millions of dollars earned from those illegal sales. After the site was shut down, the FBI seized bitcoins earned through illegal transactions that the government later sold for more than **$48 million.**

Only one of the launderers could be caught, who goes by the name - **Hugh Haney** from Ohio, operated under the pseudonym “Pharmville”. He had laundered over $19 Million in cryptocurrency.

He earned millions of dollars worth of bitcoin from transactions involving illegal narcotics, including **OxyContin, Ketamine, and Fentanyl**. Haney transferred cryptocurrency proceeds worth more than $19.15 million from those transactions to an unidentified bitcoin exchange company in February 2018, and exchanged the cryptocurrency for cash that he deposited in a personal bank account. Haney told the exchange company that he had earned the bitcoin through his own “mining” of the cryptocurrency, according to the government. Federal agents subsequently seized that cash from Haney’s bank account.

The FBI later reported that the **users of the dark web cannot remain anonymous forever,** especially when they try to legitimise their proceeds.

# Hybrid Threats

Hybrid warfare is as old as conventional wars. The only difference today is that they are more complex and advanced. Conventional wars have objectives that run on the lines of causing military damage to a nation by razing through its cities or **destroying its strategic locations,** but the objectives in a hybrid war are highly tactical and have objectives such as undermining **public trust in democratic institutions**, deepening unhealthy polarisation both nationally and internationally, challenging the core values of democratic societies, gaining geopolitical influence and power through harming and undermining others, and affecting the decision-making capability of political leaders.

The idea of influence is a constant in international politics, but hybrid threats challenge this notion by using a variety of synchronised tools that create both linear and non-linear effects. They often exhibit **ambiguity** and deliberately manipulate detection and response thresholds, taking advantage of weaknesses in democratic societies and different jurisdictions. Hybrid threats also include a distraction element, diverting attention away from their true objectives.

The concept of hybrid warfare, while useful for understanding the complexities of modern conflicts, may not be the most effective policy tool for analyzing capabilities. **It can serve as a threat force multiplier**, which may support policies that do not align with the intended outcomes. This is because the concept of hybrid warfare is often associated with an existential threat that requires a strong and immediate response, potentially leading to a more aggressive or militaristic approach.

To effectively address hybrid threats, it may be more fruitful to develop old techniques in new ways or approach them from different contexts, rather than simply adopting and combining different types of tools. This approach may also serve as a challenge for developed and well-prepared countries to reassess their strategies. Ultimately, it is crucial to analyse and understand the new forms of influence that may arise from hybrid threats, as they can have self-harming consequences for a country, which may prove to be detrimental to the stability of the government of that. Hybrid threats are characterized by the utilization of multiple synchronized tools, enc-

-ompassing both linear and non-linear strategies, primarily leveraging non-military means to achieve their objectives. The following points explain the characteristics of hybrid threat:

- It creates **ambiguity** and hides the real intent behind the actions. This is often done through covert and plausible deniability tactics.
- It also exhibits **deliberate threshold manipulation** when it comes to detection and response. This means that they manipulate the threshold at which a response is triggered, making it difficult for authorities to detect and respond to their actions.
- Furthermore, it exploits the **means of a democratic society** as well as between different jurisdictions. They take advantage of any gaps or weaknesses in these systems to achieve their objectives.
- Finally, Hybrid Threats often include a **distraction element**, such as action in one place while targeting something or someone else somewhere else. This helps them divert attention away from their true objectives.

Now, we shall take a deeper look at hybrid threats by breaking its elements into simpler parts.

**ELEMENTS**

There are four main pillars to be considered for the analytical framework of hybrid threats. They are: Actors, Tools, Domains, and Phases.

1. Actors

a. State actors
b. Non-State actors

2. Tools:

a. Foreign direct investment
b. Cyber espionage
c. Armed force operations
d. Diplomatic sanctions

3. Domains:

a. Infrastructure
b. Cyber
c. Military
d. Political & Public administration

4. Activity:

a. Interference
b. Influence (through priming)
c. Operation(destabilisation)
d. War / Warfare (Coercion)

The major aim of such Activity is to target and undermine the decision-making capability of the target through the above-mentioned activities, particularly in different domains through the tools and the actors.

The actors involved in hybrid threats typically employ diverse combinations of linkages, tailored to specific countries, in order to

maximize their effectiveness in achieving their objectives.
The linkage can be understood by:

Hybrid threats involve a combination of conventional and unconventional tactics used by state and non-state actors to achieve their objectives. Within hybrid threats, the cyber domain plays a critical role, with cyber espionage, interference, and manipulation often employed as tactics. State actors are often the primary actors involved in hybrid threats, using hybrid warfare tactics to gain strategic advantage, undermine sovereignty, or create instability. Effective strategies to counter hybrid threats require **collaboration** between government agencies, private companies, and international organisations to develop comprehensive approaches that address the underlying causes of conflict and promote peaceful outcomes.

**Types of Actors:**
In hybrid warfare, both the state as well as non-state actors are engaged with the motive of furthering their own strategic interests. The **state actors include states like Russia, China, Iran, and North Korea** among others and some examples of non-state actors include **Al Qaeda, ISIS, and Hezbollah**.

There is another classification of actors in hybrid warfare given by Ronald O’Rourke - revisionist powers, rogue states, and transnational threat organisations. The revisionist power includes states like China and Russia. The rogue states include states like Iran and North Korea, while the last category includes jihadist terrorist organisations.
All of these actors differ in their approach, and magnitude while trying their best to compete across political, economic, and military arenas, and use technology and information to accelerate these contests in order to shift regional balances of power in their favour.

Let us take a deeper look at all of these actors, their modus operandi, and why these actors behave so.

1. **State Actors-** These state actors have an underlying objective to challenge the principles of democracy. The reason for the same is not hard to discern. These states are mainly authoritarian and want to hold on to the power they enjoy in their state. However, there is an underlying weakness with the authoritarian system and that is, the transition of power should take place within the regime and hence, a quintessential need to preserve the power. This is what differentiates an authoritarian state from a democratic one. To further their motives, the authoritarian states use coercive methods which may include censorship of media, or other measures such as quashing dissent and maintaining their influence within their respective countries. These states often view the democratic states as a threat to their power position and hence, they always try to undermine and weaken the democratic states. The authoritarian states maintain strict control over the media and scarcely is there any scope for any check or criticisms from anybody, while the opposite is the case for the democratic countries

Thus, these differences in the ideologies, and approaches, between the two kinds of states, impel the authoritarian states to act against the democratic states, and for this, they adopt hybrid warfare as a means.

An in-depth look at the strategies and thinking of some individual state actors yields the following:

The Russians use Reflexive Control, which is deeply rooted in their strategic thinking. What this basically means is using information and communication to manipulate an adversary's perception and decision-making processes, Russia uses various techniques, such as in the field of information warfare, psychological operations, and cyberattacks.

For example, in the 2014 Crime Invasion, Russia reportedly used disinformation campaigns and propaganda to create a narrative that Ukraine was a failed state on the brink of collapse, and that the Russian-speaking population in Crimea was in danger of being persecuted. By framing its actions as a humanitarian intervention, Russia was able to justify its annexation of Crimea to the international community.

The Chinese strategies and its ambitions are well reflected in its official documents. For instance, the declaration of becoming a sea power nation as its national strategic objective is very evident in the statements of Chinese Leaders. How are they a hybrid warfare threat? This question is answered by the **Chinese Three Warfare Concept.**

**Psychological Warfare-** It is achieving political and military aims by influencing targets' psychology and behaviour by distributing specific information. Some of the methods are deterrence, coercion, deception, instigation, seduction, bribery, inducement, and confusion

**Public Opinion Warfare-** is defined as operations to influence both domestic and international support by the use of selective information delivered through different media.

**Legal Warfare** is used to describe the technique of manoeuvring to gain legal superiority by using or modifying domestic and international law to gain political initiative or military advantage

The main state actors - Russia and China, thus use these methods posing threats to NATO, EU.

2. **Non-State Actors-** It is sometimes underestimated by researchers, but as a matter of fact, the first-ever concept of hybrid warfare emanates from the actions of a non-state actor and it dates back to 1994, Chechen War, where the major non-state actors included the Chechen Rebels who used a variety of tactics such as guerilla warfare, propaganda to fight the Russian military.

The non-state actors play a major role in international politics and even without having any institution with any State, have the power to interfere in the matters of democratic states and exert huge pressure on their governments.

# Key Enforcement Agencies

In a world with multifarious threats, there is a need for international cooperation in order to ward off these threats, while also containing them, this leads us to an examination of the key agencies working towards these objectives.

**FATF**

The Financial Action Task Force (FATF) is an inter-governmental body that was established to set standards and promote effective implementation of **legal, regulatory, and operational measures** for combating money laundering, terrorist financing, and other related threats to the integrity of the international financial system. It is a policy-making body that works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

**Role of FATF in combating terrorism financing:**

- The FATF monitors the progress of its members in implementing necessary measures and reviews money laundering and terrorist financing techniques and countermeasures.
- In collaboration with other organizations, The FATF is the global standard-setter for combating money laundering, terrorist financing, and the financing of proliferation of weapons of mass destruction (WMD).
- The role of the FATF is to protect the integrity of the financial system and enhance its transparency, which contributes towards global security.
- The FATF conducts and publishes expert operational and strategic studies on risks, trends, and methods; develops and sets global policies, standards, best practices, and guidance.
- It evaluates FATF member countries and oversees in close cooperation with the FATF-style regional bodies.

- Zonal stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.
- The FATF has developed a series of recommendations that are recognised as the international standard for combating money laundering the financing of terrorism and the proliferation of weapons of mass destruction. They form the basis for a **coordinated response** to these threats to the integrity of the financial system and help ensure a level playing field.

**Effectiveness of FATF:**

- Over a period of time the FATF has gained perceptible credibility as a professional organisation, which has succeeded in not only increasing awareness regarding the challenges being faced by the global financial system, but also human security issues like terrorism.
- It has gained considerable influence over the financial regulatory frameworks that make it less likely to be exploited by profiteers and terrorists.
- The FATF has been at the forefront of international efforts to fight money laundering and combating finance to terrorism. Its efforts have been **in conjunction with relevant resolutions of the United Nations Security Council (UNSC)**.
- Terrorist financing investigation and prosecution ensures that terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.
- FATF has become one of the major factors for countries like Pakistan being pressured to take requisite action against terrorists operating from its soil. Terrorist financing preventive measures and financial sanctions require that terrorists, terrorist organisations, and terrorist financiers are prevented from raising, moving and using funds across the globe and from abusing the not-for-profit sector of their respective states, thus curtailing the spread of terrorism.

.

- The naming and shaming policy of the FATF has a corrective underlying principle. A country can be placed on a list and then removed thereafter on receipt of assurance from the highest political authority, along with a judgement on the progress made to implement the guidelines, has ensured an improvement in the overall CFT standards.

Thus FATF played an important role of acting as a standard body to put pressure on terrorism funding and money laundering. Any blacklisting of a country cuts the lifeline of terrorist activity supported by the state through blockage of funds. Thus, FATF acts as a pressure group helping in combating terrorism and money laundering.

**Counter Terrorism Committee**

The Counter-Terrorism Committee (CTC) was established by the United Nations Security Council in the wake of the 9/11 attacks to coordinate international efforts to combat terrorism. The committee is responsible for monitoring the implementation of Security Council Resolution 1373, which requires all states to take measures to prevent and suppress terrorist acts.

One of the key strengths of the CTC is its ability to bring together representatives from different countries and international organisations to share information and best practices. This cooperation helps to identify and address emerging threats, and also helps to build the capacity of less developed countries to combat terrorism.

Another important aspect of the CTC's work is its focus on preventing the financing of terrorism. The committee works closely with the Financial Action Task Force (FATF) to monitor the flow of funds to terrorist groups and to develop strategies to disrupt their financing networks.

The CTC has undertaken several programs to combat terrorism and prevent violent extremism. These programs include:

- **Capacity building:** The CTC provides technical assistance to countries to enhance their capacities to prevent and combat terrorism. The committee helps countries develop legal frameworks and institutions to investigate and prosecute terrorist acts, and also provides training for law enforcement officials and judicial authorities.

**Combating terrorist financing:** The CTC works closely with the (FATF) to prevent the financing of terrorism. The committee provides guidance to countries on how to implement international standards to detect and disrupt the flow of funds to terrorist organisations.

**Information sharing:** The CTC facilitates information sharing between countries and international organisations to identify and disrupt terrorist networks. The committee also promotes cooperation and coordination among law enforcement agencies to investigate and prosecute terrorist acts.

**Research and analysis:** The CTC conducts research and analysis on emerging terrorist threats and trends. The committee provides regular updates to the Security Council on these issues, and also publishes reports and briefings for the broader public.

Overall, the CTC's programs aim to enhance international cooperation and coordination to prevent and combat terrorism, as well as to address the underlying factors that contribute to violent extremism.

The Counter-Terrorism Committee (CTC) has been highly active in several instances, particularly in response to major terrorist attacks. Here are a few examples:

**9/11 Attacks:** The CTC was established by the United Nations Security Council in the aftermath of the September 11, 2001 terrorist attacks on the United States. The committee was tasked with monitoring the implementation of Security Council Resolution 1373, which required all countries to take measures to prevent and suppress terrorist acts.

**2004 Madrid train bombings:** Following the Madrid train bombings in 2004, the CTC held an emergency meeting and urged countries to take swift action to prevent and combat terrorism. The committee also emphasised the need for international cooperation and information sharing to identify and disrupt terrorist networks.

**2015 Paris attacks:** In the wake of the November 2015 terrorist attacks in Paris, the CTC held an emergency meeting to discuss ways to enhance international cooperation and coordination to combat terrorism. The committee urged countries to share information and intelligence, and also emphasised the importance of preventing the financing of terrorism.

**2019 Sri Lanka Easter bombings:** In response to the Easter Sunday bombings in Sri Lanka in 2019, the CTC emphasised the need for countries to address the root causes of terrorism, such as social exclusion and marginalisation. The committee also called for greater international cooperation to prevent the financing of terrorism and disrupt the activities of terrorist organisations.

Overall, the CTC has been highly active in response to major terrorist attacks, and has played an important role in promoting international cooperation and coordination to combat terrorism.

The Counter-Terrorism Committee (CTC) and anti-money laundering efforts are closely linked, as terrorist organisations often rely on illicit financial flows to finance their activities.

The CTC has played a key role in promoting international cooperation and coordination to prevent the financing of terrorism, and works closely with the Financial Action Task Force (FATF) to develop and implement international standards for combating money laundering and terrorist financing.

The CTC and FATF have developed a number of initiatives to prevent the financing of terrorism, including:

**Risk assessments:** The CTC and FATF work with countries to conduct risk assessments to identify vulnerabilities in their financial systems that could be exploited by terrorists. This allows countries to develop targeted measures to prevent and detect suspicious transactions.

**Enhanced due diligence:** The CTC and FATF promote the use of enhanced due diligence measures to prevent the financing of terrorism. This includes measures such as identifying and verifying the identity of customers, monitoring transactions, and reporting suspicious activities.

**Information sharing:** The CTC and FATF facilitate information sharing between countries and financial institutions to detect and disrupt the flow of funds to terrorist organisations. This includes the sharing of financial intelligence and the development of common reporting standards.

**Sanctions and asset freezing:** The CTC and FATF work with countries to impose sanctions and freeze the assets of individuals and organisations involved in terrorist financing. This can help disrupt their financial networks and prevent them from accessing the resources they need to carry out terrorist activities.

Overall, the CTC and FATF's efforts to prevent the financing of terrorism have been critical in the global fight against terrorism. However, there is still much work to be done to identify and disrupt the complex networks that terrorists use to finance their activities, and to ensure that financial systems are not exploited for illicit purposes.

The Counter-Terrorism Committee (CTC) has played an important role in promoting international cooperation and coordination to prevent and combat terrorism. However, there are also some criticisms of the committee's effectiveness and approach. Here are some critical analyses of the CTC:

- **Security-focused approach:** One criticism of the CTC is that it has a narrow, security-focused approach to counterterrorism that emphasises law enforcement and military responses. This approach can be effective in disrupting terrorist networks and preventing attacks, but it does not address the root causes of terrorism such as political grievances, poverty, and social exclusion.

- **Limited effectiveness:** Despite its efforts, the CTC's effectiveness in preventing and combating terrorism has been limited in some cases. For example, some countries have been reluctant to share information or cooperate fully with international efforts to combat terrorism. Moreover, some critics argue that the committee's focus on security measures has not been sufficient to address the underlying factors that contribute to terrorism.

- **Balancing human rights and security:** The CTC's focus on security measures has also been criticised for potentially infringing on human rights and civil liberties. Some critics argue that measures such as mass surveillance and indefinite detention without trial can be counterproductive and may fuel resentment and radicalization.
- **Lack of accountability:** Another criticism of the CTC is the lack of accountability and oversight mechanisms. Some observers argue that the committee lacks transparency and accountability, and that its decisions are not subject to sufficient scrutiny.

Overall, while the CTC has made important contributions to the global fight against terrorism, there is still much work to be done to address the underlying factors that contribute to terrorism and to strike a balance between security measures and respect for human rights and civil liberties.

**UNODC**

Money laundering is a pervasive global problem that threatens the integrity of financial systems and undermines economic development. The United Nations Office on Drugs and Crime (UNODC) has developed a comprehensive framework for combating money laundering, which includes five key components. However, while this framework provides a solid foundation for addressing money laundering, there are several areas where improvements can be made to ensure its effectiveness in a constantly evolving landscape.

- **Legal Framework-** The first component of the UNODC framework is the establishment of a legal framework that criminalises money laundering and provides for effective investigation, prosecution, and punishment of offenders. While many countries have laws criminalising money laundering, penalties are often inadequate to deter potential offenders. Therefore, countries need to strengthen their legal frameworks and ensure that the penalties for money laundering are severe enough to act as a deterrent.

- **Financial Intelligence Unit (FIU)-**The second component of the framework is the establishment of a Financial Intelligence Unit (FIU) to receive and analyse suspicious transaction reports and disseminate the information to the appropriate authorities. The FIU plays a critical role in identifying and tracking suspicious transactions and is essential to the success of any anti-money laundering (AML) program. However, FIUs must be adequately resourced and staffed to ensure they can effectively fulfil their mandate.

- **Know Your Customer (KYC)-** The third component is the implementation of effective (KYC) procedures to verify the identity of customers and monitor their transactions. KYC procedures help financial institutions to identify high-risk customers and detect suspicious transactions. However, KYC procedures can be burdensome for customers and can create significant compliance costs for financial institutions. Therefore, regulators need to strike a balance between KYC requirements and the need to ensure a seamless customer experience.

- **Suspicious Transaction Reporting-** The fourth component of the framework is the requirement for financial institutions to report suspicious transactions to the FIU. This reporting is critical to identifying potential money laundering activity and ensuring that appropriate action is taken. However, reporting requirements can be overly burdensome, and financial institutions may be hesitant to report suspicious transactions for fear of damaging their reputation. Therefore, regulators need to work with financial institutions to streamline reporting requirements and provide appropriate incentives to encourage reporting.

- **Law Enforcement and Prosecution**-The final component of the framework is the effective investigation, prosecution, and punishment of money laundering offenders. While the legal framework is essential, enforcement is equally critical to ensure that money laundering is effectively deterred. However, money laundering cases can be complex and require significant resources to investigate and prosecute.

Therefore, law enforcement agencies need to be adequately resourced and trained to effectively investigate and prosecute money laundering cases.

Improvements to the Framework

- **Strengthening Legal Framework:** Many countries still lack a robust legal framework for combating money laundering, and those that do have laws often have inadequate penalties. Therefore, countries need to strengthen their legal frameworks and ensure that the penalties for money laundering are severe enough to deter potential offenders.

- **Enhancing International Cooperation:** Money laundering is a global problem that requires international cooperation. Countries need to work together to share information and cooperate in investigations and prosecutions.
- Improving Technology: Money launderers are increasingly using technology to hide their activities. Therefore, countries need to invest in technology to better detect and prevent money laundering
- Addressing Emerging Trends: Money laundering techniques are constantly evolving, and regulators need to be proactive in addressing emerging trends, such as the use of cryptocurrencies.

- **Increasing Awareness:** Finally, countries need to raise awareness among financial institutions and the public about the dangers of money laundering and the importance of reporting suspicious transactions.

**(United Nations Office on Drugs and Crime, 2011)**

# Crisis in Sudan

Of late, the media has been rife with images and articles from Northeast Africa, of a country in turmoil. The Republic of Sudan is currently witnessing a unique conflict - with two military factions battling on the streets of the country to grasp power when the citizens of the country were the closest they have ever been to establishing democracy.

To understand this issue, we must go back to the year 2019, during the reign of the erstwhile autocratic president, Omar Al-Bashir. A plot to topple his regime was carried out by the coming together of two politically ambitious figures at the top of Sudan's military ecosystem - The leader of the Sudanese Army **Abdel Fattah al-Burhan** and the leader of the paramilitary Rapid Support Forces Mohammed **Hamdan Dagalo**, also known as **Hemedti**. (Gbadamosi, 2023)

The 2019 upheaval led to the establishment of a Transitional Military Council, which took upon itself the onus of overseeing the restoration of normalcy and transition of power in Sudan post the coup. This move was widely protested by the pro-democracy movement which then led to the formation of a Sovereign Council, which was meant to be a blend of the military council and a civilian administration. The power-sharing structure was defined as such:

*The military council would oversee the country's leadership for the first 21 months while the civilian administration would rule the council over the following 18 months.*

While this did keep the pro-democracy movement happy initially, it was soon clear that this alliance was at best - shaky. In 2021 things came to a head when the Sudanese army, in collaboration with the RSF conducted a military coup by dissolving the power-sharing structure. Al-Burhan was quoted saying the agreement with civilian members of the country's transitional sovereign council "became a conflict" over the past 2 years "threatening peace and unity" in Sudan. (Reuters, 2023).

### A History of the Rapid Support Forces

The Rapid Support Forces are one of the two most pivotal characters in this conflict. A history of the group suggests that it was born out of Sudan's Darfur conflict of the early 2000s where he headed the notorious Janjaweed forces which have been implicated in human rights violations. This conflict, born out of environmental degradation and fierce competition over fairly limited resources, led to communal conflicts.

Later, in 2013 Bashir created the RSF a paramilitary group which was led by Dagalo, which played a pivotal role in trying to quash the pro-democracy sit-ins in Khartoum post which Dagalo turned against President Bashir and joined forces with the Sudanese armed forces. (Sikainga, 2023)

## Why Has the Power Struggle Arisen?

This conflict has originated from an agreement signed on the 5th of December 2022, calling for the absorption of the RSF into the ranks of the Sudanese military. While the Army wishes the process to take place over a span of 2 years, the RSF has vehemently opposed that and proposed a period of 10 years for the same. This agreement was a part of the series of processes aimed at creating a civilian government by the 11th of April, 2023. The clash was further deepened by the proposal to elevate Hemedti to a position equal to Burhan. A communal undertone can be sensed concerning this facet, as the powerful Islamists of Sudan – an Arabic-speaking elite class – have come out in support of Burhan as he has been strategically reincorporating people from this community into the government.

This power struggle has taken the form of violence on the streets of Khartoum and various other parts of Sudan, creating a threat of a prolonged humanitarian crisis.

## The Plot Thickens – International Actors in the Crisis

While this does seem like a grave national conflict on the face of it, its ramifications on the world become clear when we take a step back to look at Sudan's position in the geo-political sphere. Several international actors with vested economic interests in Sudan not only complicate the issue but also reveal another potential facet of the conflict – State-sponsored terror activities and financing. Sudan is particularly well placed and coveted by numerous powers, due to its strategic location on the Red Sea and vast gold repositories in addition to its access to the Nile River. It is also a major pathway for oil in the oil trade. Both warring factions have close ties with numerous regional and international powers, which we must examine closely.

## THE SUDANESE ARMED FORCES – INTERNATIONAL ALLIES:

1. **Egypt:** Hemedti has accused the country of supplying the Army with Fighter jets and colluding with Burhan. These allegations have been blatantly denied by Egypt, who maintain the stance that their forces were in Sudan for a joint military exercise. Their economic interests lie in the strong trade of low-priced consumer goods with Sudan.

Their most notable interest lies, however, in the opposition to the Great Ethiopian Renaissance Dam on the river Nile, which threatens Egypt's water supply gravely. (The Guardian, 2023)

2. **Israel:** This nation has had close ties with the military government, as they are trying to normalise relations between the two countries.

3. **China:** The country has invested copious amounts of money, including $6 Billion in loans. It is also worth noting that Burhan controls an estimated 250 companies in the Sudanese economy, making it clear that countries with over-arching trade-related interests have a vested interest leaning towards the Armed forces. (Al-Jazeera, 2023)

## THE RAPID SUPPORT FORCE – INTERNATIONAL ALLIES:

1. **UAE:** While the Emirates does have a vested interest in Burhan's faction as well due to its investments in Sudanese port infrastructure, it also has close ties to the RSF, which was hired as a mercenary organisation to fight on their behalf in Yemen.

2. **Russia:** A private military company with a record of advancing Moscow's political, and economic interests has close ties with the RSF head Hemedti, who derives most of his wealth from the gold-mining industry. In addition to

supporting Bashir, they also supported the 2021 coup which strengthened Russia’s ties with Sudan.

The gold-mining aspect is particularly pivotal, as the proceeds from mining and adjacent smuggling activities have largely cushioned the blow of sanctions imposed on Russia in the aftermath of the Invasion of Ukraine.

Russia is also looking to establish a strategic naval base in the Red Sea, and Sudan is an ideal location for the same.

**3. Libya:** Khalifa Haftar, a **Libyan warlord** who heads the militia controlling eastern Libya is a close ally of the **RSF**, and has reportedly sent a plane of military supplies in support of the group. (Al-Jazeera, 2023).

## How does this tie in with AML and terror Financing?

Years of internal tensions, starting from the South Sudan conflict, and the Darfur Conflict and extending up to the current crisis have led the nation to be economically weak. Indicators of human development confirm this, with the **total fertility rate being 6, life expectancy being at 59, and the per capita income** amounting to an estimated $750-$800.

In such dire conditions, the ongoing conflict has already caused a shortage of essentials such as food and water. Historical trends show that there is a strong likelihood of ethnic groups being pitted against each other as a result of the competition for scarce resources. The economic pressure on an already highly fragmented society will lead to the prolonging of the war, and the creation of militarised factions by ethnic groups, which are extremely likely to take the form of terrorist organisations, as seen in various examples across the globe.

The threat of an extended humanitarian conflict and terrorism arises most primarily, however, out of the involvement of foreign powers. One must also keep in mind the definition of terrorism as given by the Oxford Dictionary, in order to lucidly grasp the gravity of the situation – “the unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims.”

Both sides are looking to their regional allies as well for supplies and ammunition for the conflict. Sudan is in a troubled neighbourhood, with many of the countries grappling with bilateral problems, making Sudan a probable ground for proxy wars and terror groups funded by these nation-states for the sole purpose of the fulfilment of their own political and economic interests.

Gold mining in Sudan with its adjacent smuggling trade ecosystem, is unique in the sense that it purportedly works to fund two conflicts currently taking place – the Sudanese conflict and the Ukrainian Conflict. Until now, it has helped to prop up the involvement of the Wagner group (and by extension Russia) in Ukraine and will play a pivotal role in supporting the atrocities being inflicted on millions of civilians in Sudan by the RSF.

Money Laundering carried out by Sudan's major industries, many of which are controlled by Burhan's army can appropriate funds to fuel the conflict. As the Arab elites or Islamists are in support of the Sudanese Armed Forces, and the scope for raising money from donors as well as rallying the support of Non-State Violent Actors is a probable move, taking into consideration anecdotal evidence from various conflicts over the past century.

The funding of ethnicity-based factions has a strong potential to extrapolate into ethnic cleansing and related terror activity. The funding of these groups will primarily come from the two fundamental players in this battle – the Sudanese Army and the RSF in order to rally their support, and additionally from foreign players with vested interests and looking to fight proxy wars in Sudan.

The conflict, if not nipped in its infancy, will have far-reaching ramifications, especially with regard to the terror financing ecosystem, organised crime, and money laundering.

# AML AND COMBATTING TERROR FINANCING

In order to understand the basics of combating money laundering, we turn to the European Union's AML Directives.

The EU has issued many anti-money laundering directives, with **AML Directive 6** being the most recent. These directives follow or even exceed the recommendations and guidelines issued by the Financial Action Task Force, which is responsible for setting AML Standards at the global level. The AMLDs have expanded the scope of obligated entities subject to AML supervision by tightening the definitions of money laundering offences and making them more effective in combating the problem of Money Laundering.

The current AMLD Framework on Money Laundering:

The framework has two parts

1. The first one is the small, lower-capacity jurisdictions in individual European nations, which act as the **first line of defence** against illicit financial practices. The efforts of these individual jurisdictions are based on three pillars:

1.1 T**he AML Supervisors or administrative authorities** that examine the entities for adherence to the jurisdiction's AML regime typically have the power to impose fines for noncompliance.

1.2 The next pillar is the **Financial Intelligence Units**, which collect, analyse and disseminate the reports that the entities submit under the AML Program requirements.

1.3 The last pillar is the **law enforcement agencies** and the justice system, concerned with the persecution of individuals involved in crimes pertinent to money laundering.

2. The second part of the framework is the authority at the European level. These include three European Supervisory Authorities to help foster convergence at the EU Level. These authorities are namely, the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets

Authority (ESMA). They mainly investigate cases of breaches of union laws and their rulings override the decisions of the individual jurisdictions at the national level.

There is a joint committee that facilitates coordination among the three ESAs, the AML Committee (AMLC).

**Limitations of the framework:**

The first and foremost limitation is that the coexistence of integrated enforceable single financial market policy with the national structure of AML Supervision implies that any weakness in one EU State can invite money laundering to enter that country and potentially gain access to the entire single market. The reason for the weak national structure is that national-level authorities are susceptible to political influence and regulatory capture. Their acting as the first line of defence would encourage criminals to seek out weak links and take advantage of them.

Although it might seem that even though Money Launderers manage to pass through the individual state's jurisdiction scot-free, **they will be punished by the ESAs, this is not the case**. The ESAs generally do not investigate unless a large failure has already occurred and if the launderers pass through an individual state scot-free, they have low chances of being caught. As a result, this framework of coexistence generates national vicious circles, which tend to be self-perpetuating rather than self-correcting.

**The current conflict regarding the choice between Two-tier versus Unitary architecture**

The European Union faces a choice between two models:

1. Enhancing a **two-tier model** under which the ultimate responsibility of AML would still remain at the **national level** but an EU authority would be empowered to oversee national AML Supervisors.

   - This also has many drawbacks,

as this model is still based on the previous model.

**2. Unitary Model-** Under this model, a European Agency would have the ultimate AML Supervisory responsibility, which can be exercised through a network that involves national agencies and other European-level bodies. However, it has several drawbacks, such as adding an extra burden at the central level. Also, it is practically impossible for a large authority to oversee the entire European Union and as a result, the lower-level branches of the EU Central Authority will still have some level of autonomy that can be exploited by launderers. (Joshua Kirschenbaum and Nicolas Véron, 2018)

## The New MODEL: EAMLA

The creation of a new European AML Authority emerges as the best response to the current challenges of AML supervision in the European Union.

## Money laundering: Risk of DeFi and cryptocurrency

Money laundering is a serious problem that affects societies worldwide. Criminals use various methods to launder their illicit proceeds, including traditional financial systems and more recently, cryptocurrencies. The rise of decentralised finance (DeFi) has brought new challenges in the fight against money laundering, as it offers a new way for criminals to move and hide their funds. In this context, **it is important to understand the risks associated with DeFi and cryptocurrency and how they can be addressed**.

A report by the US Justice Department's cyber-digital task force states that criminals of all types are increasingly using cryptocurrency to launder their illicit proceeds. Another problem is that transnational criminal organisations, including drug cartels, may find cryptocurrency especially useful to hide financial activities and move vast sums of money efficiently across borders without detection. Additionally, **Janet Yellen**, US Treasury Secretary, has described the misuse of cryptocurrencies as a growing problem. However, it is worth noting that most money launderers do not need cryptocurrencies to be successful and can use traditional methods such as mixing illicit funds into trade flows or investing them in assets such as property or art.

Cryptocurrencies can be transferred quickly and easily cross borders without intermediaries such as banks, which can reduce transaction costs and increase speed. Additionally, it can be used anonymously or pseudonymously, which makes it harder to trace the source of funds or identify the parties involved. These features make cryptocurrencies an attractive option for money launderers who want to hide their activities from law enforcement and regulatory authorities.

A bevvy of analytical firms has emerged to help detect illicit activity in the industry. These watchdogs take advantage of the fact that blockchain transactions are public and gather data to identify suspicious patterns of activity or addresses. Focusing on this kind of "cryptocurrency native" crime, Chainalysis, a leading crypto forensics firm, estimates **illicit activity represented 0.34 per cent of cryptocurrency transaction volume in 2020, down from 2.1 per cent in 2019, as the overall level of crypto activity increased this year**. Therefore, it seems that increased monitoring and analysis of blockchain transactions may be one way to reduce money laundering in the cryptocurrency industry.

According to Chainalysis, bad actors such as drug traffickers are using cryptocurrency to launder their ill-gotten funds by converting them into cryptocurrency and sending them around the world. However, it is harder to investigate this activity in individual cases or to ascertain the size of it in the aggregate because such funds move into cryptocurrency directly from fiat rather than from known illicit addresses on blockchains, leaving no trace of how the money was originally made. Therefore, money laundering in cryptocurrency can be difficult to detect and prevent.

There have been several high-profile cases of money laundering using cryptocurrencies in recent years. For example, in 2019, the US Department of Justice charged two Chinese nationals for laundering more than $100 million worth of cryptocurrency stolen by North Korean hackers. In another case, a Russian national was arrested in Greece for allegedly laundering $4 billion through a Bitcoin exchange. Additionally, the infamous dark web marketplace Silk Road was shut down by US authorities in 2013 after it was found to be facilitating drug sales and money laundering using Bitcoin. These cases highlight the potential for cryptocurrencies to be used for illicit activities such as money laundering and the need for increased monitoring and regulation of the industry.

Mexican-based narcotics dealers are increasingly looking to cryptocurrency as a means to obscure illicit business transactions, as well. At the same time, federal agencies have been moving to track the illegal use of cryptocurrency - once touted as untraceable - and how closely they work with exchanges like Binance to track organised crime.

There are also opportunities for **innovation** in the fight against money laundering, such as the use of blockchain technology to create more transparent and secure financial systems. It is essential that governments, regulators, and industry stakeholders work together to develop effective strategies for combating money laundering in the digital age. By doing so, we can protect communities from criminal activity and promote economic stability and growth.

The use of cryptocurrency in money laundering has both pros and cons. **On the one hand, the anonymity and decentralisation offered by these systems make it easier for criminals to launder their illicit proceeds without detection.** This has led to growing concerns among regulators and industry stakeholders about the potential for cryptocurrency to be used for criminal activities.

On the other hand, there are also potential benefits to using cryptocurrency to combat money laundering. For example, blockchain technology can be used to create more transparent and secure financial systems that are less vulnerable to fraud and corruption. Additionally, blockchain analytics tools can help identify suspicious activity on decentralised blockchains and promote compliance with anti-money laundering regulations.

Ultimately, the use of cryptocurrency in money laundering is a complex issue that requires careful consideration of both its potential benefits and risks. While there are challenges associated with regulating these systems, there are also opportunities for innovation in the fight against money laundering. By working together, we can develop more effective strategies for combating money laundering in cryptocurrency while promoting innovation and growth in this emerging technology.

## LIMITATIONS :

- It is primarily related to the complexity and constantly

- evolving nature of the DeFi and cryptocurrency landscapes. Due to the decentralised and rapidly changing nature of these systems, it can be difficult to develop a comprehensive model that accurately captures all of the potential risks associated with money laundering.
- Additionally, there is a lack of standardisation in the DeFi and cryptocurrency industries, which makes it challenging to develop a one-size-fits-all model for identifying and mitigating money laundering risks. Different platforms may have different risk profiles, making it difficult to apply a uniform approach across the entire industry.
- Another limitation is the lack of data available for analysis. Many transactions on decentralised blockchains are anonymous or pseudonymous, making it difficult to trace them back to their source. This can make it challenging to identify patterns or trends that may indicate money laundering activity.
- Finally, there is also a risk that regulatory efforts could stifle innovation in the DeFi and cryptocurrency industries.

While there is a need for greater oversight and regulation in this space, overly burdensome regulations could discourage investment and innovation in these emerging technologies. (Silverman G., 2021).

## LIBRA PROJECT

Cryptocurrencies have been a hot topic in the financial world for several years now, with Bitcoin being the most well-known example. However, the emergence of stablecoins, which are cryptocurrencies pegged to a stable asset like a fiat currency or commodity, has raised new concerns for regulators and governments worldwide.

One of the most high-profile **stablecoin** projects is Libra, which Facebook announced in June 2019. The project aimed to create a global digital currency that could be used for online transactions and remittances. However, almost immediately after its announcement, regulators and politicians began expressing concerns about the potential impact of Libra on financial stability and monetary policy.

In reality, the Libra Project works as follows:

1. Users can purchase Libra Coins through authorised exchanges or by using a credit card or bank transfer.
2. Once users have purchased Libra Coins, they can store them in digital wallets provided by third-party companies or through Facebook's own wallet app called Calibra.
3. Users can then send and receive Libra Coins through their digital wallets using blockchain technology. Transactions are processed quickly and at a low cost compared to traditional payment methods.
4. To ensure the security of transactions and user data, the Libra Project uses advanced encryption techniques and other security measures like multi-factor authentication and biometric verification.
5. The value of the Libra Coin is pegged to a basket of stable assets like fiat currencies and government bonds, which helps to ensure that its value remains stable over time.
6. The governance structure of the Libra Project is designed to be decentralised and democratic, with each member of the association having an equal vote on important decisions related to the project's development.
7. The Libra Association is committed to complying with all applicable laws and regulations related to anti-money laundering (AML) and counter-terrorist financing (CTF). This includes complying with international standards set by organisations like the Financial Action Task Force (FATF) and implementing measures to prevent sanctions evasion.

The G7 and G20 both expressed concerns about global stablecoins like Libra, with particular emphasis on risks to financial stability. The **Financial Stability Board (FSB)** and the **Financial Action Task Force (FATF)** also began working on regulatory issues related to stablecoins.

There are various types of stablecoins such as fiat-collateralized stablecoins, crypto-collateralized stablecoins, algorithmic stablecoins, commodity-backed stablecoins and hybrid stablecoins. However, the Libra project initially proposed a single global currency that would be backed by a basket of fiat currencies. In response to regulatory concerns, the project has shifted towards a more decentralized approach with multiple stablecoins backed by different fiat currencies. Facebook revised its Libra concept as "Libra 2.0" which includes several new features designed to address regulatory concerns and make it easier for people to use Libra as a means of payment.

One of the key features of Libra 2.0 is the introduction of single-currency stablecoins in addition to the multi-currency Libra Coin (LBR). The network would start with stablecoins for USD, EUR, GBP, and SGD, with the LBR being made up of these single-currency coins using a smart contract.

It is worth noting that while Libra's stablecoins are backed by fiat currencies, they are not necessarily categorised as **fiat-collateralized stablecoins.** This is because the Libra Association has committed to holding reserves in a variety of low-risk assets in addition to fiat currencies, such as government bonds and bank deposits. This diversified reserve portfolio is intended to help maintain the stability of Libra's stablecoins even in times of market stress. (Read & Schäfer, 2020).

## EU FRAMEWORK:

The European Commission has proposed a new legal framework for crypto-assets, including stablecoins, which are digital rrencies that maintain a stable value relative to a specific asset or basket of assets. The proposal aims to establish a clear regulatory framework for these types of digital assets, which are becoming increasingly important in the global economy.

The proposed framework includes principles of authorization, disclosure, investor protection, market integrity, and supervision. **Issuers of crypto-assets would need to obtain authorization** from national authorities before offering their assets to investors or consumers. Issuers would also be required to provide clear and comprehensive information about their assets, including their value, performance, risks, and fees, in a standardised format that is easily accessible to investors and consumers. Investors in crypto-assets would have certain rights, including the right to receive information about the asset's value and performance, as well as the right to redeem their assets for cash or other assets.

Overall, the proposed legal framework for crypto-assets is designed to promote investor protection and financial stability while also ensuring that these assets can be used safely and securely by consumers around the world. The proposal is part of a broader effort by the European Union to regulate the digital economy and ensure that it operates in a safe and transparent manner. (FSA, 2022)

# Ransomware, DeFi, Money Laundering: Deadly Combination

Ransomware has become one of the most significant threats to businesses and individuals alike. It is a type of malware that encrypts files on a victim's computer, rendering them inaccessible until a ransom is paid. The **ransom is usually demanded in cryptocurrency**, which makes it difficult to trace the money flow. This anonymity has made ransomware an attractive option for cybercriminals looking to make a quick profit.

However, once the ransom is paid, the criminals need to launder their ill-gotten gains. Money laundering is the process of making illegally obtained money appear legitimate by passing it through various financial transactions. Criminals use money laundering to hide their illegal activities and avoid detection by law enforcement agencies.

Cryptocurrency has made money laundering easier than ever before. *Cryptocurrency mixers* are one of the most popular methods used by criminals to launder their money. These mixers take cryptocurrency from multiple sources and mix them together before sending them back out in different amounts to different addresses. This makes it difficult for law enforcement agencies to trace the flow of funds.

One of the most popular methods used by cybercriminals to launder their money on DeFi platforms is **through liquidity pools**. Liquidity pools are pools of funds that are used to facilitate trades on DeFi platforms. Cybercriminals can deposit their ill-gotten gains into these pools and then withdraw them as different cryptocurrencies or fiat currencies.

Another method used by cybercriminals is **through flash loans**. Flash loans are a type of loan that allows users to borrow funds without collateral as long as they repay the loan within a single transaction block. Cybercriminals can use flash loans to move large sums of money quickly and anonymously across different DeFi platforms.

Multiple cryptocurrency exchanges

are another method used by criminals to launder their money. They can buy and sell cryptocurrencies on these exchanges, making it difficult for law enforcement agencies to track the source of the funds.

Criminals also use various tricks to conceal the final beneficiaries of their ill-gotten gains. One such trick is called "**smurfing**", where they break up large sums of money into smaller amounts and deposit them into multiple accounts at different banks or financial institutions.

The consequences of ransomware attacks can be devastating for businesses and individuals alike. Not only do they lose access to their data, but they may also face reputational damage if sensitive information is leaked or stolen during the attack.

Money laundering adds another layer of complexity to an already dangerous situation. It allows criminals to profit from their illegal activities while avoiding detection by law enforcement agencies. This, in turn, encourages more cybercriminals to engage in ransomware attacks, leading to a vicious cycle of criminal activity.

To combat this problem, law enforcement agencies around the world are working together to track down and prosecute those responsible for ransomware attacks. They are also working with financial institutions to identify suspicious transactions and freeze accounts linked to criminal activity.

To prevent ransomware attacks, businesses should regularly back up their data and store it securely, while also educating employees on how to identify and avoid phishing emails - a common ransomware delivery method. Alongside this, governments must collaborate with the private sector to develop new technologies and tools that can detect and prevent money laundering in cryptocurrency transactions.

By being aware of the risks associated with ransomware and taking appropriate measures to protect themselves, businesses can safeguard their operations and minimise the impact of potential attacks. This includes implementing robust cybersecurity measures and regularly backing up their data. By prioritising these steps, businesses can help ensure their continued safety and operational resilience in the face of a ransomware threat.

Ransomware and money laundering are two interconnected issues that pose significant risks to financial systems and consumers. The rise of cryptocurrency has made it easier for cybercriminals to carry out ransomware attacks and launder their ill-gotten gains, making it crucial for governments and private sectors to work together to address these challenges.

To specifically address the issue of ransomware and money laundering, it is essential to recognize that paying ransom only fuels the growth of this criminal activity. Instead, governments and private sectors must work together to develop better defences against ransomware attacks and implement regulations that make it harder for cybercriminals to launder their ill-gotten gains.

By prioritising the regulation of cryptocurrency exchanges, preparing for the possibility that ransomware actors might move on to another cybercrime like cryptocurrency fraud and theft, and working closely with law enforcement authorities, we can reduce the problem of ransomware and prevent cyber criminals from moving on to other areas of cybercrime.

Furthermore, it is crucial to continue investing in better defences against ransomware attacks, international law enforcement chasing bad actors, and imposing sanctions on ransomware gangs and service providers that facilitate money laundering. By doing so, we can ensure a lasting effect on reducing the problems caused by ransomware attacks and money laundering.

**LIMITATIONS :**

- Ransomware attacks can be difficult to execute successfully, as they often require sophisticated technical knowledge and social engineering tactics.
- The use of cryptocurrency in ransomware attacks can be traced through blockchain analysis, making it easier for law enforcement agencies to identify and prosecute those involved in these crimes.
- The high-profile nature of ransomware attacks means that law enforcement agencies are more likely to investigate and prosecute those involved in these crimes, making it riskier for cybercriminals to attempt these attacks.
- The increasing regulation of cryptocurrency exchanges and

- other financial institutions makes it harder for cybercriminals to move large sums of money without being detected.

Overall, while ransomware attacks can still be lucrative for cybercriminals, there are significant limitations that make

other financial institutions make it harder for cybercriminals to move large sums of money without being detected. Overall, while ransomware attacks can still be lucrative for cybercriminals, there are significant limitations that make

# Effect of CBDC on Money Laundering

The blockchain and cryptocurrency markets are evolving around the world to be explored and exploited. Cryptocurrency's significance surpasses evolving technologies via decentralization, security, and transformation potential. Despite its advantages of accessibility and fast and cheap transactions, it also poses limitations in terms of volatility, criminal activity and traceability if it gets misused.

Cryptocurrency gives root to the problem of money laundering. Since there is no proper government body for the regulation of digital technologies, money launderers misuse the advantages of digital currency. With crypto, they may move the illicit funds through hundreds of wallets before depositing the funds and cashing them out at a crypto exchange. Unlike bank accounts, thousands of wallets may be opened without proof of identity within seconds. This poses more problems for financial inclusion and creates chaos like economic instability, disruption of financial markets, reduction of tax revenue, etc.

Central banks dislike private money like bitcoins because they can't get control of it. And it also threatens the sovereignty of the national currency. Hence, numerous central banks around the world are working on their state issues through CBDC.

**CBDC (Central Bank Digital Currency)** is a digitised version of domestic currency that's equal to physical cash or the reserves created by the central bank. It would be curious to think that this term sounds similar to digital transactions made using payment apps. But that's not the truth. Digital transactions using a payment app involve transactions between two commercial banks. But CBDCs are a **direct liability of the central banks.** They are mostly token-based which is represented by blockchains.

Unlike public blockchains like Bitcoin or Ethereum, where the information recorded is available to all, CBDCs are private or **permissioned blockchains** to which only central banks and the parties they choose have access.

CBDCs have the potential to provide

greater transparency, traceability, and accountability in financial transactions, which can help reduce the opportunities for money laundering in an economy. However, it is important to note that CBDCs are not a panacea and must be designed and implemented carefully to ensure that they are effective in reducing money laundering and other illicit activities. Some of them are:

1. Investigation of e-krona (Riksbank) (Central bank of Sweden)
2. Digital Yuan or Digital Currency Electronic Payment (DCEP) [ People Bank of China]
3. Dcash (Eastern Caribbean Central Bank)
4. e-Dinar (Central Bank of Tunisia)

**DCEP (Digital Currency Electronic Payment) : (CHINA)**

China's central bank digital currency, known as DCEP, has the potential to address some financial governance challenges, such as money laundering. DCEP is a digital version of China's fiat currency, the renminbi (RMB), and is issued and backed by the **People's Bank of China** (PBOC).

DCEP transactions are processed through a centralised system that allows for real-time settlement. The system uses a two-tiered approach, with the PBOC issuing DCEP to commercial banks, which then distribute it to customers. Transactions can be conducted using mobile devices or other digital platforms.

The PBOC has stated that DCEP will be designed with anti-money laundering (AML) and counter-terrorism financing (CTF) measures in mind. For instance, a real-name wallet would be required for any large transaction, which could help prevent anonymous transactions that are often used in money laundering schemes.

One instance where DCEP could help prevent money laundering is **online gambling**. In China, online gambling is illegal but still prevalent. Criminals often use anonymous payment methods to launder their profits from online gambling sites. With DCEP's real-name wallet requirement for large transactions, authorities could more easily track and monitor these transactions.

Another instance where DCEP could help prevent money laundering is in **cross-border transactions.** Criminals often use cross-border transactions to move illicit funds across borders and evade detection. With DCEP's centralised system and real-time settlement capabilities, authorities could more easily track these transactions and prevent criminals from moving illicit funds across borders.

A third instance where DCEP could help prevent money laundering is in **corruption cases**. In recent years, China has cracked down on corruption by targeting officials who have used their positions for personal gain. DCEP's real-name wallet requirement could help prevent officials from using anonymous payment methods to move illicit funds.

Finally, DCEP could also help prevent money laundering in the **real estate sector.** In China, real estate is a popular way for criminals to launder money. With DCEP's centralized system and real-time settlement capabilities, authorities could more easily track and monitor transactions in the real estate sector and prevent criminals from using it as a means of laundering money.

**IMPACT :**

The impact of DCEP is that it could *reduce the use of physical cash in China*. With DCEP's real-time settlement capabilities and ability to be used for small transactions, it could become a popular alternative to physical cash. This could have implications for China's monetary policy, as it would make it easier for the PBOC to track and monitor financial transactions.

Another potential impact of DCEP is that it could *disrupt existing online payment mechanisms* in China. Currently, mobile payment platforms like **Alipay and WeChat Pay dominate the online payment market in China**. However, with DCEP's real-time settlement capabilities and ability to be used for small transactions, it could become a popular alternative to these platforms.

Furthermore, DCEP has the potential to create new business opportunities for companies that are involved in digital payments. For instance, companies that provide digital wallets or other payment-related services could potentially partner with banks or other financial institutions to offer DCEP-related services.

Overall, while DCEP has the potential to disrupt existing online payment mechanisms in China and reduce the use of physical cash; it also has the potential to create new business opportunities for companies involved in digital payments.

### HOW CAN A REDUCTION IN PHYSICAL CASH THROUGH CBDC REDUCE MONEY LAUNDERING?

1. **Reduction in cash-based businesses:** Cash-based businesses, such as street vendors and small shops, are often used to launder money. With DCEP's real-time settlement capabilities and ability to be used for small transactions, it could become a popular alternative to physical cash. This could make it more difficult for criminals to launder money using cash-based businesses.

For instance, Demonetization in India reduced the use of physical cash in real estate transactions, making it harder for criminals to launder money through cash-based businesses like shell companies or fake property deals. The government promoted digital payments in the real estate sector and required transactions above a certain threshold to be conducted digitally. This shift made it easier for authorities to track and monitor transactions, reducing the risk of money laundering.

- **Increased monitoring of financial transactions:** DCEP has the potential to increase the monitoring of financial transactions by providing greater visibility into financial flows. For instance, Sweden's BankID system lets users access digital services and online banking securely. With over 7 million users, it helps banks monitor transactions for potential money laundering or financial crimes. If someone makes large, unusual transactions, alerts can be triggered for further investigation. This shift towards digital payments in Sweden has made it harder for criminals to launder money anonymously.

- **Greater transparency in charitable donations:** Charitable organizations are often used as a front for money laundering activities. With DCEP's real-time settlement capabilities and ability to be used for small transactions, it could become a popular alternative to physical cash donations. This could make it more difficult for criminals to launder money through charitable organizations.

For instance, Charities can be used to launder money from foreign sources in the US, and a popular method is through "**donor-advised funds" (DAFs)**. These allow donors to make large charitable donations while remaining anonymous, making it hard for authorities to track the source of the funds.

DCEP, a digital currency, could help prevent this by providing increased transparency and monitoring capabilities. With DCEP, authorities could more easily track transactions and prevent criminals from using charitable organizations like DAFs to launder money. This could be achieved by triggering alerts for further investigation if someone suddenly starts making large donations through a DAF using DCEP.

The evolution of central bank digital currency (CBDC) has the potential to transform financial transactions and improve market efficiency. However, as with any new technology, there are also risks to consider. One such risk is the potential for money laundering and terrorist financing.

It is important for regulators and financial institutions to work together to ensure that CBDC is implemented in a way that minimizes these risks while still allowing for the benefits of digital currencies. This may involve implementing robust anti-money laundering and counter-terrorist financing measures, as well as developing new technologies to detect and prevent illicit activities.
Overall, while there are challenges to overcome, the potential benefits of CBDC are significant. By improving efficiency in financial transactions and reducing counterparty risk, wholesale CBDC has the potential to revolutionize debt capital markets in any country. As we continue to explore this technology, it will be important to balance innovation with responsible regulation in order to ensure a safe and secure financial system for all.

**LIMITATIONS :**

1. Lack of physical presence: While the lack of physical presence of CBDC can make it difficult to trace and track, it can also limit the ability of criminals to launder large amounts of cash. This is because CBDC transactions are **typically recorded** on a distributed ledger, which makes it easier for

law enforcement agencies to track illicit activities.

- **Increased transparency**: CBDC transactions are typically more transparent than traditional currency transactions, as they are recorded on a distributed ledger. This increased transparency can make it more difficult for criminals to launder money without being detected.
- **Smart contract limitations**: While smart contracts offer technical solutions for interoperability and risk reduction, they may also have limitations when it comes to enforcing anti-money laundering regulations. For example, smart contracts may not be able to detect or prevent certain types of illicit activities.
- **Cybersecurity risks**: As with any digital technology, CBDC is vulnerable to cyber-attacks and other forms of online fraud. This could potentially make it easier for criminals to launder money or engage in other illicit activities.
- **Financial privacy**: CBDC systems may offer a certain degree of financial privacy, which could potentially be exploited by criminals for illicit activities.
- **Centralized nature**: The centralized nature of CBDC means that there is a single point of control for the system, which could potentially make it easier for criminals to exploit vulnerabilities or corrupt individuals within the central authority.

- **Strong privacy protections and security measures**: It is important to ensure that CBDC systems are designed with strong privacy protections and security measures in place, such as encryption, multi-factor authentication, and regular audits to detect and prevent fraudulent activities.
- **Clear regulatory frameworks**: It may be necessary to establish clear regulatory frameworks for CBDC systems to ensure that they are used responsibly and safely. This could include requirements for anti-money laundering and know-your-customer (KYC) checks, as well as penalties for individuals or institutions found to be engaging in illicit activities. (ESM, 2023)

# An International view of Money laundering and illicit activity financing

**MONEY LAUNDERING: JAPAN**

Japan has been facing challenges in the form of money laundering (ML) and terrorist financing (TF) risks. As technology advances, financial transactions become more complex and globalized, and the risks faced by financial institutions (FIs) in ML/TF and proliferation financing (PF) also change. The COVID-19 pandemic has further highlighted the risks of non-face-to-face transactions, which are easier to falsify and impersonate than face-to-face transactions. In response to these challenges, Japan has implemented various policies and initiatives to strengthen its AML/CFT/CPF regime.

One of the challenges faced by Japan is the need to continuously improve its ML/TF risk control framework in response to changes in ML/TF risks. To address this, the government of Japan published the **National AML/CFT/CPF Action Plan,** which outlines the necessary legislative actions for the next three years. The plan emphasizes the need for both the public and private sectors to work together to enhance the AML/CFT/CPF regime.

Another challenge is the evolving criminal methods used in the ML/TF environment. Japan has identified the main perpetrators of ML crime as members of boryokudan, specialized fraud crime groups, and crime groups consisting of foreign nationals in Japan. To combat this, Japan has established and revised guidelines for risk identification and assessment, **Customer Due Diligence (CDD)**, transaction monitoring and filtering, and cross-border remittances. The Financial Services Agency (FSA) has also implemented inspections focusing on AML/CFT/CPF measures and strengthened inter-agency cooperation.

Japan has also recognized the importance of utilizing new technologies to improve risk assessment and management, speed up and improve the accuracy of large-scale data analysis, reduce costs, and improve the quality of suspicious transaction reporting.

However, there are challenges in utilizing new technologies, such as regulatory and operational challenges, avoiding unintended consequences (e.g., privacy breaches), assessing the effectiveness of solutions and addressing residual risks. Additionally, Japan has implemented measures such as freezing the assets of parties related to terrorist groups like the Taliban, ISIL, and Al-Qaida in accordance with the UNSC Resolution.

To address these challenges, Japan has established the **Blockchain Governance Initiative Network (BGIN)**, which is developing blockchain technology in line with the multi-stakeholder approach. Japan has also conducted a proof-of-concept project for data sharing and collaborative analytics, aiming at the use of AI. However, it is also necessary to ensure consistency with data protection and privacy regulations.

In conclusion, Japan has implemented various policies and initiatives to strengthen its AML/CFT/CPF regime in response to the challenges of ML/TF risks. The government of Japan has published the National AML/CFT/CPF Action Plan to work steadily on necessary legislative actions. Japan has also established and revised guidelines, implemented inspections, and strengthened inter-agency cooperation to combat evolving criminal methods. Furthermore, Japan recognizes the importance of utilizing new technologies, such as blockchain and AI, to improve risk assessment and management, but also acknowledges the challenges in utilizing these technologies. Japan's initiatives demonstrate its commitment to combating ML/TF risks and strengthening its AML/CFT/CPF regime.(FSA, 2022)

## RECOMMENDATION BY BRITISH COLUMBIA

Money laundering is a significant problem worldwide, with an estimated $1.6 trillion laundered annually. The issue is particularly acute in British Columbia, where a recent report found that billions of dollars in illegal funds were being laundered through the province's real estate market. To combat this problem, policymakers are exploring innovative tools like **Unexplained Wealth Orders (UWOs)**, which allow law enforcement agencies to investigate and potentially seize assets that are suspected to be the proceeds of criminal activity.

The Final Report of the Commission of Inquiry into Money Laundering in British Columbia recommended the implementation of UWOs as part of a wider approach to combat money laundering and proceeds of crime in the province. However, the implementation of unexplained wealth orders (UWOs) can help combat money laundering by allowing law enforcement agencies to investigate and potentially seize assets that are suspected to be the proceeds of criminal activity. By inquiring individuals to explain the source of their wealth, UWOs can help deter money laundering and increase transparency in financial transactions.

UWOs can be used not only to target individuals suspected of money laundering but also those who may have received assets from such individuals. This means that UWOs can help disrupt the entire chain of illicit financial flows, from the initial act of money laundering through to the eventual use of those funds.

In addition, UWOs can help to promote transparency in financial transactions by requiring individuals to provide a clear explanation for their wealth. This can help to identify suspicious transactions and prevent further instances of money laundering.

The analysis provides valuable insights into the feasibility and potential impact of implementing UWOs in British Columbia. The Final Report of the Commission of Inquiry into Money Laundering in British Columbia urged the government to legislate UWOs as part of a wider approach to counter the prevalence of money laundering and proceeds of crime in the province.

Implementing unexplained wealth orders (UWOs) efficiently requires global regulatory policymakers to take the following steps:

- **Establish a clear legal framework**: The government should establish a clear legal framework for UWOs, including guidelines for their use and appropriate due process protections.
- **Allocate adequate resources**: The agency responsible for applying UWOs should be allocated adequate resources and capabilities to do so effectively.
- **Foster collaboration between stakeholders**: Collaboration between law enforcement agencies, financial institutions, and other stakeholders is crucial for effectively implementing UWOs and combating money laundering more broadly. Policymakers should work to foster collaboration between these groups by sharing information and expertise.

- **Develop public awareness campaigns**: Raising public awareness about the existence and potential impact of UWOs can help to deter money laundering by increasing transparency in financial transactions.
- **Establish appropriate safeguards**: Appropriate safeguards must be put in place to protect individual rights and prevent abuse of power when implementing UWOs. This includes establishing clear guidelines for their use, ensuring that they are accompanied by appropriate due process protections, and fostering transparency in their implementation.
- **Monitor effectiveness**: Policymakers should monitor the effectiveness of UWOs over time to ensure that they are achieving their intended goals and making a meaningful impact on combating money laundering.

By taking these steps, global committees can implement UWOs efficiently as part of a broader strategy to combat money laundering and proceeds of crime.

Overall, UWOs represent an important tool for combating money laundering and proceeds of crime. By working collaboratively across sectors and putting appropriate safeguards in place, policymakers can effectively implement UWO. (Basel University, 2022)

# Model

Money laundering is a serious threat to the global financial system and the stability of nations. It facilitates various crimes such as terrorism, drug trafficking, human trafficking, corruption, and tax evasion. It also undermines the rule of law and erodes public trust in institutions. Therefore, it is imperative to devise effective strategies and policies to combat money laundering and its associated risks.

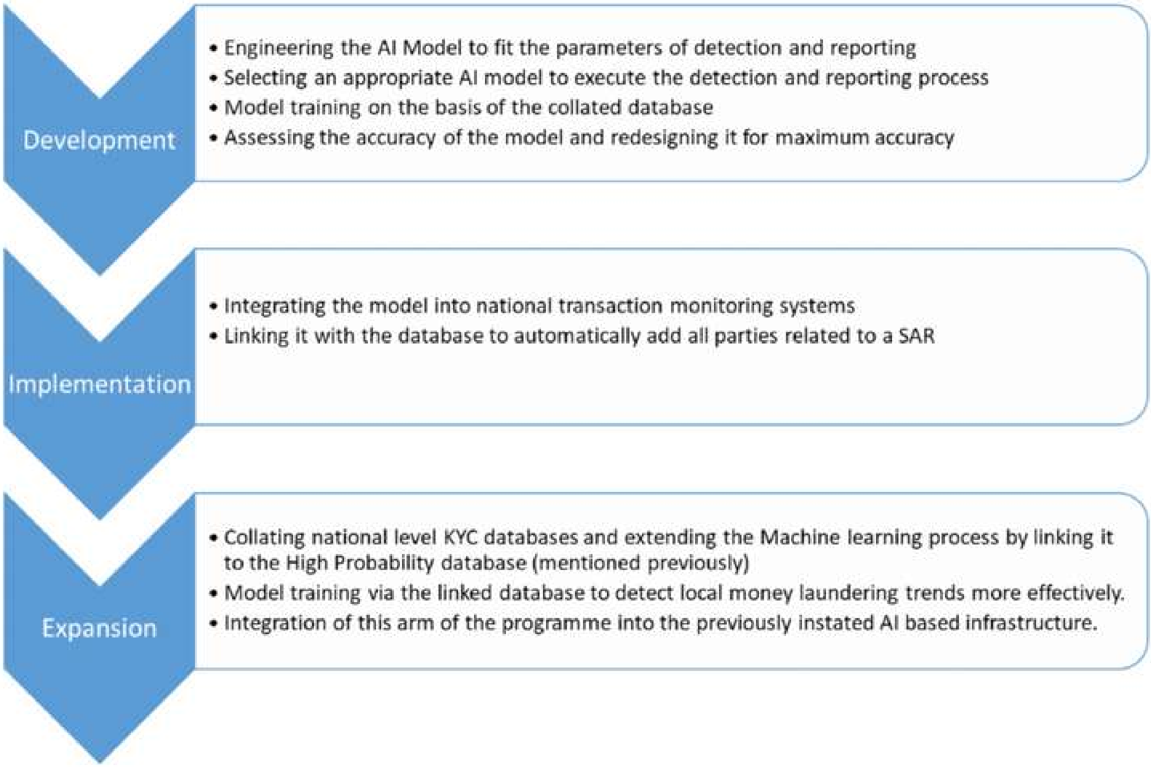
In this policy brief, we propose a novel anti-money laundering model that aims to enhance the detection and prevention of money laundering activities across different domains and platforms. The model consists of two main components: a database of high-risk individuals and organizations that are prone to money laundering, and a dark web crawler that can track and analyze illicit transactions on the dark web and crypto markets. The model also leverages artificial intelligence and machine learning techniques to improve the accuracy and efficiency of risk assessment and flagging of suspicious transactions.

**Some Statistics**

The model is based on the latest data and trends on money laundering and its impact on the global economy and security. According to the Financial Times, global fines for failing to prevent money laundering and other **financial crimes surged more than 50% in 2022, reaching almost $5 billion.** However, this amount is still a fraction of the estimated **value of money laundered worldwide, which according to the United Nations is between 2% and 5% of the global GDP, or $800 billion to $2 trillion. (Financial Times, 2023)**

The model also recognizes that money laundering is evolving and adapting to new technologies and platforms, such as the dark web and crypto markets, which pose new challenges and risks for the anti-money laundering domain. According to Chainalysis, a blockchain analysis company, **$1.7 billion worth of cryptocurrency was stolen** or laundered in 2018. Another study by CipherTrace, another blockchain analysis company, estimated that $4.5 billion worth of cryptocurrency was lost to fraud and theft in 2019.

The model aims to address these challenges by using various tools and techniques to enhance the identification and prevention of money laundering activities across different domains and platforms. The model uses a database of high-risk individuals and organizations that are prone to money laundering, based on various criteria such as their criminal records, financial profiles, geographic locations, and business activities. The database can be integrated with an **AI system to flag suspicious transactions** based on predefined rules and patterns. The model also uses a **dark web crawler** that can track and analyze illicit transactions on the dark web and crypto markets, using natural language processing and machine learning techniques to extract relevant information and generate risk scores.



Development

- Engineering the AI Model to fit the parameters of detection and reporting
- Selecting an appropriate AI model to execute the detection and reporting process
- Model training on the basis of the collated database
- Assessing the accuracy of the model and redesigning it for maximum accuracy

Implementation

- Integrating the model into national transaction monitoring systems
- Linking it with the database to automatically add all parties related to a SAR

Expansion

- Collating national level KYC databases and extending the Machine learning process by linking it to the High Probability database (mentioned previously)
- Model training via the linked database to detect local money laundering trends more effectively.
- Integration of this arm of the programme into the previously instated AI based infrastructure.

## COMPONENTS OF INSTATING AND USING THE AI/ML PROGRAMME

The components of instating and using the AI/ML program as analytical tools involve the implementation and utilization of artificial intelligence and machine learning techniques in the fight against money laundering. These tools encompass various stages, including data integration, model development, model evaluation, and ongoing monitoring. By leveraging AI/ML, the program aims to enhance the detection and prevention of money laundering activities by analyzing high-risk individuals and organizations, tracking illicit transactions on the dark web and crypto markets, and improving risk assessment and flagging of suspicious transactions. These analytical tools provide a data-driven approach to strengthen the financial system and fortify the battle against money laundering.

Components of Instating and Using the AI/ML Program in Anti-Money Laundering:

- **Model Development**: This stage involves the use of analytical tools such as data mining, predictive analytics, and network analysis to develop an AI model for detecting and reporting money laundering activities. Machine learning algorithms like decision trees, neural networks, or support vector machines are employed to train the model using labeled historical data.
- **Model Evaluation**: The accuracy of the AI model is assessed in this stage using separate data to evaluate its performance. Metrics like precision, recall, and F1 score are used to measure the model's accuracy. If necessary, the model can be redesigned by adjusting parameters, selecting different features, or using alternative machine learning algorithms.

- **Data Integration**: Analytical tools facilitate the integration of the anti-money laundering model with national transaction monitoring systems. This integration enables real-time access to transaction data from various financial institutions and platforms.
- **Database Linking**: The model is linked to a database that contains information about high-risk individuals and organizations susceptible to money laundering. Regular updates to this database are shared with relevant institutions. When the model identifies a suspicious transaction, the parties involved can be automatically added to Suspicious Activity Reports (SARs), which are reports filed by financial institutions to report potentially illicit activities.

- **Automated SAR Generation**: Through analytical tools, the process of generating SARs can be automated. When the model detects a suspicious transaction, it automatically generates a SAR, including relevant details of the flagged transaction and the parties involved. This automation streamlines the reporting process and ensures timely reporting of suspicious activities.

- **Monitoring and Alerting**: The integrated system continuously monitors transactions in real time, applying the anti-money laundering model to identify potentially suspicious activities. If a transaction meets the predefined suspicion criteria,alerts are generated to notify relevant authorities or compliance officers for further investigation.

- **Data Collation:** Analytical tools such as data mining and text analytics are employed to collate a national-level Know Your Customer (KYC) database. This database contains information about individuals and organizations, including their identity, financial profile, and transaction history. Additionally, the database can be linked to a high-probability database that holds information about known money laundering activities and patterns. This linked database helps identify local money laundering trends and patterns not apparent in the national-level database alone.

- **Model Training:** Using the linked database, analytical tools such as predictive analytics and machine learning train the anti-money laundering model. The model analyzes the data in the linked database to detect local money laundering trends and patterns. Various machine learning algorithms like decision trees, neural networks, or support vector machines are utilized to train the model. The model is designed to identify suspicious transactions based on parameters such as transaction amount, frequency, and location.

## Discussion

Throughout the formulation of this policy brief, we have analyzed and presented different aspects and domains of money laundering, its impact, and its gravity in the real world. However, we believe that merely stating the problem and its effect is useless unless it is backed by a feasible and pragmatic solution that could help ameliorate the situation. So we present an anti-money laundering model to help in the effective tracking and persecution of money launderers bringing about a substantial reduction in money laundering activities.

| ACTION | WHAT IT ENTAILS | EFFECT | FEASIBILITY | RELEVANT STAKEHOLDER AND ITS ROLE | LIMITATIONS | OVERCOMING LIMITATION |
|---|---|---|---|---|---|---|
| Dark Web Crawlers | Develop sophisticated web crawling tools specifically designed for the dark web. These tools can scan hidden services, forums, and marketplaces to identify suspicious transactions, money laundering networks, and emerging trends. By continuously monitoring the dark web, law enforcement agencies can proactively respond to evolving money laundering techniques. | Dark web crawlers enable early detection of money laundering activities, identification of key players, and the mapping of dark web networks. They help in gathering evidence, initiating investigations, and disrupting criminal operations. Timely intervention can deter money launderers and protect the integrity of the financial system. | Governments can collaborate with cybersecurity firms to develop advanced web crawling tools tailored for the dark web. Regular updates and maintenance of the tools are essential to keep up with the evolving nature of the dark web. Close cooperation between law enforcement agencies and dark web crawler developers is crucial for information sharing and technology improvements. | Government agencies: Collaborate with cybersecurity firms to develop dark web crawling tools and establish partnerships for information sharing.<br>Cybersecurity firms: Develop and maintain dark web crawling tools, ensuring they remain effective in monitoring hidden services and marketplaces.<br>Law enforcement agencies: Utilize dark web crawling tools to gather intelligence, detect suspicious transactions, and initiate investigations. | Dark web crawlers may face limitations, such as limited access to certain hidden services and marketplaces that require authentication or invitations. The dynamic nature of the dark web poses challenges in consistently tracking and monitoring illicit activities. | Collaboration with international partners and intelligence agencies can provide broader access to the dark web and assist in overcoming authentication challenges. Continuous research and development can help enhance dark web crawler capabilities and ensure adaptability to changing dark web landscapes. |
| Artificial Intelligence in Risk Scoring | Leverage artificial intelligence and machine learning algorithms to develop risk scoring models for financial transactions related to the dark web. These models can assess the risk associated with specific transactions or customers, flagging those that exhibit characteristics of potential money laundering. | Artificial intelligence-based risk scoring enhances the accuracy and efficiency of identifying high-risk transactions and customers on the dark web. It streamlines compliance processes for financial institutions and assists authorities in focusing resources on investigations with a higher probability of detecting money laundering activities. | Governments can collaborate with financial institutions and technology companies to develop AI-powered risk scoring models specifically tailored for dark web money laundering. Data sharing frameworks can be established to facilitate information exchange between financial institutions and authorities. Regular updates and fine-tuning of risk scoring algorithms are necessary to adapt to evolving money laundering techniques. | Government agencies: Collaborate with financial institutions and technology companies to develop AI-powered risk scoring models specifically tailored for dark web money laundering.<br>Financial institutions: Implement AI-based risk scoring models in their transaction monitoring systems to flag high-risk transactions and customers.<br>Technology companies: Provide the necessary infrastructure and expertise to develop AI algorithms and integrate them into financial institutions' systems. | Developing accurate risk-scoring algorithms requires large and diverse datasets, and biases can inadvertently be introduced during the training process. Criminals may adapt their techniques to avoid detection, rendering risk scoring less effective in certain cases. | Governments should invest in data sharing initiatives, encouraging financial institutions to collaborate and share transaction data to improve risk scoring accuracy. Continuous monitoring of risk scoring models and regular audits can help identify and address biases. Close cooperation with technology companies can enable the development of innovative risk scoring methodologies. |
| Using blockchain technology for AML compliance | Creating and sharing customer information on a distributed ledger that can be accessed by multiple parties | Enhancing the verification and detection of customer information and transactions on blockchain-based platforms | Moderate: The technology is available and has potential benefits, but there are also challenges and risks that need to be addressed. | Financial institutions: Provide and use customer information on blockchain platforms; collaborate with industry associations and SROs; offer training and certification programs. | Privacy and security concerns; lack of standardization and interoperability; regulatory uncertainty. | Developing best practices and guidelines for data privacy and security; adopting common standards and protocols; engaging with regulators and policymakers |
| Targeting identity management node | Disrupting the creation and use of fake identities or identity theft within the cryptolaundering system | Reducing the anonymity and concealment of individuals involved in the laundering process | High: The methods are proven and effective, and there is a strong incentive to implement them. | Government agencies: Implement stricter identity verification processes; use biometric data to verify identities; require additional forms of identification; develop technology to detect fraudulent identities. | Sophisticated methods of identity theft or fraud; resistance from privacy advocates; cost and complexity of implementing new technologies | Improving the coordination and cooperation among different agencies; raising awareness and education among the public; leveraging existing technologies and platforms. |
| Using blockchain technology for financial services | Increasing transparency, reducing fraud, and improving traceability in financial transactions and processes | Improving the efficiency, security, and accountability of financial services | Low: The technology is still nascent and faces many technical and regulatory barriers. | Government agencies: Provide clear and consistent regulatory frameworks for blockchain-based financial services; support innovation and experimentation in the sector.<br>Financial institutions: Adopt blockchain technology for financial services; collaborate with other stakeholders to develop common standards and solutions. | Interoperability, scalability, and performance issues; regulatory uncertainty and complexity; lack of trust and awareness among customers and stakeholders. | Developing interoperable, scalable, and high-performance blockchain platforms; engaging with regulators and policymakers to address regulatory challenges; educating customers and stakeholders about the benefits and risks of blockchain technology. |

The first part of our model is concerned with identifying individuals and organisations prone to money laundering by creating a database of such individuals or organisations and sharing it with different institutions. The database can be integrated with an AI system to flag suspicious transactions. With the rise of the dark web and crypto, there has been a significant increase in money laundering and illicit activities over the dark web. The next part of the model focusesn such activities by using a unique tool - Dark Web Crawler- to map and identify the dark web networks and transactions. Artificial intelligence can be used to develop risk-scoring models to help improve the efficiency and accuracy of the identification of high-risk transactions.

For the building of this model, feasibility and effectiveness have been given priority over sophistication and abstraction. The model entails the use of various different tools and methods to counter money laundering effectively.

# Conclusion

Over the course of this brief, we have traversed the various facets of the intersection of money laundering and the financing of illicit activity. Our exploration of various topics under this ambit includes examining traditional sources of funding and laundering, along with the advent of new-age methods and mechanisms – with a special emphasis on cryptocurrency.

One finds from these descriptions and glimpses into the real-world situation, the fragility of the global financial system, with respect to illicit activity. From varied regional patterns and processes to penetration and effectiveness of legal frameworks, continuous attempts to prevent such activities, while being fruitful, have been extremely tedious to curb. With the proliferation and increased accessibility to technology, criminals, and terrorists are able to get away with illicit activity much more efficiently. Our observations yield that while international organizations have been working towards incorporating these rapid changes, their effectiveness is minuscule due to its largely theoretical nature as of now.

We have recognized one of the foremost issues in battling such activity to be a lack of systematic global cooperation towards this objective. While organizations such as the FATF and the UNODC have succeeded at bringing these issues to the forefront of global attention and promoting regional cooperation, a lack of structure and a duplication of efforts stand as an impediment to the same. To address these issues, we have developed a framework to combat issues related to money laundering through cryptocurrency, the banking system, and illicit activity via the dark web – which calls for a streamlined structure to be put in place in collaboration with existing grass root organizations and the points of origination for such illicit activity, while also promoting global cooperation and intelligence sharing. Our model also accounts for the changes in technology with time, by using Artificial Intelligence and Machine Learning models for combating the same.

In the end, it can be reasonably inferred from the various conclusions drawn throughout the course of this policy brief, that the rapid shift in the methods of Money laundering, Crime, and Terror Financing serve as a major impediment to the global order, both in terms of security and development, and it is of paramount importance that greater global cooperation and efficient development of new technologies and methods is undertaken in order to curb this destructive phenomenon.

# Testimonial

The Policy Report 2022-23 “Under the Radar: Unveiling Money Laundering Networks, Drug Cartels and the Dark Web” of the Economics Society, Shri Ram College of Commerce is co-authored by Mithraeye E., Raghav Singhal, Satakshi Akanksha and Sneha Mishra (under the guidance of Pratul Malthumkar). It is a well-researched and informative paper that aims to understand the nexus between these three clandestine activities and proposes adoption of a framework to combat this menace through the adoption of upcoming technologies.

The authors explain the three activities, though clearly the central focus is money laundering. They provide a comprehensive overview of the history, causes, and consequences of the functioning of the organisations and means which are at the centre of most of the illegal activities in the world at present. They bring out that money laundering networks, drug cartels, and the dark web are all interconnected phenomena that pose serious challenges to law enforcement, security, and human rights.

They explain that Money Laundering is the process of concealing the origin, ownership, or destination of illegally obtained money by moving it through legitimate businesses or financial institutions. As they rightly bring out money laundering is a process.

On the other hand, Drug Cartels are organised criminal groups that produce, transport, and distribute illicit drugs. Obviously, the profits earned by selling drugs—which are huge—have to be ‘laundered’.

The Dark Web, a part of the internet that is not indexed by standard search engines and requires special software to access, links the above two activities and facilitates them. As the brief brings all ‘dark’ operators like drug cartels, terrorists and criminals, use the Dark Web for illegal activities, especially in buying and selling drugs, weapons, stolen data, and other contraband. But more than all that it is the best environment for drug laundering especially in crypto currencies which ironically have potential benefits.

The Brief covers the major aspects of the complex and multifaceted problem associated with money laundering and drug cartels such as:

- Financial facilitators which include some banks who are linked in extensive money laundering networks, which vary in their area of expertise, such as real estate or offshore banking.
- Counterfeiting of goods and currency.
- How dubious financial institutions offer their services to multiple clients, charge fees, specialise in certain techniques, and use legal professionals or intermediaries.
- The types and sources of drugs that the cartels traffic including synthetic drugs and how they affect the world's security, health, and economy.
- The offices of the UN engaged in combating the spread of drugs and cartels.
- How international cooperation can help and be improved to combat this menace.
- The Dark Web, and how it is used for illegitimate purposes especially as it relates to money laundering.
- Potential methods of government intervention on the Dark Web.

The Brief is based on credible sources quoted in the references. It studies one conflict ridden area in detail i.e., Sudan, to understand terror financing and how the key enforcement agencies such as the FATF function. The brief is written in a clear, concise, and engaging manner, and it offers a balanced and nuanced perspective on three controversial and interrelated topics. The article is a valuable resource for anyone interested in learning more about the world's long war on drugs and its implications for regional stability and human rights. It contributes to the literature on money laundering and organised crime, as it provides empirical evidence and insights on a phenomenon that is often hidden and difficult to investigate. The paper also has important implications for policy and practice, as it concludes with a table giving out a comprehensive and tabulated anti-money laundering model. This will be valuable for those dealing with public policy, scholars, practitioners, journalists and the general public. It deserves to be widely read and cited by researchers.

**Lieutenant General GS Katoch, PVSM, AVSM, VSM (Retd)**
**MS in Defence Analysis (Irregular Warfare) from NPS, Monterey, California**
**Ex Director General Perspective Planning, Army HQ,**
**Ex Director Centre of Anti-Terrorism Studies NSG**
**Distinguished Fellow, USI of India**

# References

"Anti-Money Laundering, Counter Financing of Terrorism, and Counter-Proliferation Financing" Current Status and Challenges. www.fsa.go.jp. https://www.fsa.go.jp/en/news/2022/20221007/20221007.pdf.

"Anti-Money Laundering, Counter Financing of Terrorism, and Counter-Proliferation Financing" Current Status and Challenges. www.fsa.go.jp. https://www.fsa.go.jp/en/news/2022/20221007/20221007.pdf.

Burke, J. (2023, April 20). Sudan: up to 20,000 flee violence as rival leaders refuse to negotiate. The Guardian. https://www.theguardian.com/world/2023/apr/20/egyptian-soldiers-captured-by-sudanese-paramilitary-return-home

FATF (2023), Money Laundering and Terrorist Financing in the Art and Antiquities Market, FATF, Paris, France, https://www.fatf-gafi.org/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-ArtAntiquities-Market.html

Gbadamosi, N. (2023, April 19). Sudan Descends Into Conflict as Rival Generals Clash. Foreign Policy. https://foreignpolicy.com/2023/04/19/sudan-conflict-generals-burhan-hamdan-hemeti-rsf/

The Dark Side of the Internet: A study about Representations of the Deep Web and the Tor Network in the British Press, Thais Sarda, 2020) https://core.ac.uk/download/pdf/327067368.pdf

Hybrid Warfare: The Changing Nature of Conflict, Institute for Defence Studides and Analyses, Vikrant Deshpande) https://www.idsa.in/system/files/profile/book-chapter-hybrid-warfare-kkkhera.pdf

https://www.incb.org/documents/Publications/AnnualReports/Thematic_chapters/English/AR_2021_E_Chapter_I.pdf Report of the International Narcotics Report Board for 2021)

# References

Silverman G., (2021-09-15). Cryptocurrency: rise of decentralised finance sparks? dirty money? fears. Financial Times. https://www.ft.com/content/beeb2f8c-99ec-494b-aa76-a7be0bf9dae6.

A Better European Architecture to Fight Money Laundering, Peter Institute for International Economics, Joshua Kirschenbaum and Nicolas Véron, 2018) https://www.piie.com/sites/default/files/documents/pb18-25.pdf

Money Laundering and its fallout, ASSOCHAM INDIA, 2013 https://www.resurgentindia.com/pdf/1210062877Money-Laundering-and-its-fallout.pdf

In- Depth Evaluation of the United Nations Global Programme against Money Laundering, Proceeds of Crime and the Financing of Terrorism, United Nations Office on Drugs and Crime, 2011) https://www.unodc.org/documents/evaluation/indepth-evaluations/Indepth_evaluation_of_the_United_Nations_Global_Programme_against_Money_Laundering_Proceeds_of_Crime_and_the_Financing_of_Terrorism.pdf

Levi, Mike ORCID: Soudijn, Melvin 2020. Undestanding the laundering of organized crime money. Crime and Justice 49,pp .579-631.10.1086/708047file

Libra Project: Regulators Act on Global Stablecoins - Intereconomics. www.intereconomics.eu. https://orca.cardiff.ac.uk/id/eprint/128331/1/Levi

Origins. (n.d.). Origins.
https://origins.osu.edu/article/worlds-worst-humanitarian-crisis-understanding-darfur-conflict?language_content_entity=en

The Near and Far Future of Ransomware Business Models. documents.trendmicro.com.
https://documents.trendmicro.com/assets/white_papers/wp-the-near-and-far-future-of-ransomware.pdf.

# References

View of Working Paper 41: Targeting unexplained wealth in British Columbia. eterna.unibas.ch. https://eterna.unibas.ch/bigwp/article/view/1196/1338.

(n.d.). FATF Terrorist Financing Typologies Report. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Fatfterroristfinancingtypologiesreport.html

Wholesale central bank digital currency – the safe way to debt capital market efficiency European Stability Mechanism. www.esm.europa.eu. https://www.esm.europa.eu/publications/wholesale-central-bank-digital-currency-safe-way-debt-capital-market-efficiency.

## RESEARCH AND POLICY DIRECTOR

Pratul Malthumkar

## TEAM MEMBERS

Mithraeye E.

Raghav Singhal

Satakshi Akanksha

Sneha Mishra

## DESIGN TEAM

Arshiya Chaudhary

Divyansh Gupta

Ishita Gambhir

## Contact Us

☎

**Pratul Malthumkar**
+91-63014-97329

**Keshav Khemka**
+91-62893-69919

www.ecosocsrcc.com

✉ contact@ecosocsrcc.com

The Economics Society, SRCC

THE ECONOMICS SOCIETY

SHRI RAM COLLEGE OF COMMERCE

ecosocsrcc.com

contact@ecosocsrcc.com