CHAPTER 4

THE MONEY LAUNDERING OFFENCES AND ITS NEXUS WITH CRIMINAL ACTIVITIES

4.1 MONEY LAUNDERING AND GLOBALIZATION:

The money laundering and the related offences include within their definition “money obtained not only through drug trafficking but also the proceeds of other criminal acts including terrorist activities”. Whenever criminological aspects of money laundering are discussed, it is not possible to make any meaningful distinction between the concepts of 'organized crime' and 'terrorism'. Drug trafficking has become a natural source of financing for both phenomena\(^1\). Due to globalization of economy criminal organizations are not a local issue. They have become international, operating globally:

Criminals are now taking advantage of the globalization of the world economy by transferring funds quickly across international borders. Rapid developments in financial information, technology and communication allow money to move anywhere in the world with speed and ease. This makes the task of combating money laundering more urgent than ever.

The deeper "dirty money" gets into the international banking system, the more difficult it is to identify its origin. Because of the clandestine nature of money laundering, it is difficult to estimate the total amount of money that goes through the laundry cycle. Estimates of the amount of money laundered globally in one year have ranged between $500 billion and $1 trillion. Though the margin between those figures is huge, even the lower estimate underlines the seriousness of the problem governments have pledged to address.

\(^1\) Bosworth-Davies & Salt marsh, 1994:26
There have been a number of developments in the international financial system during recent decades that have made the three F's—finding, freezing and forfeiting of criminally derived income and assets—all the more difficult. These are the "dollarization" (i.e. the use of the United States dollar in transactions) of black markets, the general trend towards financial deregulation, and the progress of the Euro market and the proliferation of financial secrecy havens.

Fuelled by advances in technology and communications, the financial infrastructure has developed into a perpetually operating global system in which "megabyte money" (i.e. money in the form of symbols on computer screens) can move anywhere in the world with speed and ease.

Now Mafia does not operate only in Italy and US; the Yakuza is active not in Japan only; Triads Tongs are not confined only to Hong Kong or US. The jurisdictional boundaries of criminal organizations have expanded globally more because of the disintegration of Soviet Union, the growth of capitalism in China, the enactment of NAFTA (North Atlantic Free Trade Agreement, a regional trade block), and the lowering of controls of European Customs, currency, passport, and other such events. Now Colombian drug cartels operate in Western Europe, Russian gangsters operate in Eastern Europe, US and Asia; the Chinese Triads dominate Asia and the west coast of US; and the Mexican criminal organizations dominate the world methamphetamine trade.²

In addition to their global operations, they form intentional alliances with each other, with crook governments, and with terrorist organizations. These crime groups therefore are more in the nature of international criminal organization (ICO) (or transnational criminal organization, TCO) and today their strategic alliances are the dominant problems to be tackled by local, national and international law enforcement.³ They run their operations more like a multinational corporation (MNC) and use modern business management models. In

this context *Ajit Ninan's cartoon* (Fig. II.i)\(^4\) graphically presents Indian underworld figure Dawood's interests, activities and operations, which are conducted more, like that of a global conglomerate.

![Fig. II.i: Indian Underworld Don Dawood's Areas of Operations](image)

### 4.2 NEXUS OF CRIMINAL ACTIVITIES WITH MONEY LAUNDERING:

The links between money-laundering and organized crime can be found in the reasons why organized criminal groups would engage in this practice. The processes to launder money or property can be expensive and are in themselves not free of risk. An organized criminal group will not go to the trouble of laundering the profits of its crimes unless there are external factors making it necessary to do so. There are mainly three reasons why organized criminal groups engage in money-laundering.

\(^4\) Source: *India Today*, 1998 "Centre stage by Ajit Ninan" *India Today* 23rd November, XXIII (47)
The first reason relates to the criminal organization’s ability to continue its activities. The primary purpose of an organized criminal group is to make profits. Just like a legitimate business, the members of an organized criminal group need to ‘reinvest’ the organization’s profits in future activity. The reinvestment of proceeds from criminal activities is necessary to sustain the future activities of the organized criminal group.

This is similar to a legitimate business concern that needs to plough back a certain portion of its turnover in order to sustain the business. The proceeds from criminal activities become the lifeblood of the organized criminal group.

For the criminal engaged in organized crime, however, any profit close to the source of the crime represents a particular vulnerability. Unless the organized criminal group can effectively distance itself from the crime that generates the profit, it remains susceptible to detection and prosecution. Consequently, the very proceeds of an organized criminal group can pose a significant threat to its members.

In the majority of cases, organized criminal groups obtain cash, or assets that are converted into cash from their criminal activities. When an organized criminal group makes use of these proceeds without altering the appearance of their illegal source, it exposes itself to detection. In order to reduce this risk, organized criminal groups need to launder their illegitimate proceeds before reinvesting them. Hence, one reason why organized criminal groups launder their proceeds from criminal activities is to enable them to sustain and continue their criminal activities.

A second reason for organized criminal groups to engage in money-laundering is to ensure that crime pays. Apart from reinvesting the profits of an organized criminal group, those in control of the organisation would want to use its profits to improve their lifestyles. The risk of detection also exists and, in fact, increases when members of the groups use the unexplained wealth generated by their criminal activities to acquire luxury items.

Cleaning money or property acquired from illegal activities provides the avenue to enjoy it without revealing its illegal origin. As a result, members of
an organized criminal group are able to use these proceeds without fear that the underlying criminal activity will be detected.

There is also a third important reason why organized criminal groups launder the proceeds from their criminal activities. Many countries have introduced, or are in the process of introducing procedures for the confiscation of the proceeds of criminal activities. A confiscation procedure adds to the risks faced by an organized criminal group. Apart from being prosecuted and punished for their criminal activities, groups also face the prospect of losing the profits they had hoped to gain from those activities. Organized criminal groups are no longer just facing a prosecution risk, but also a confiscation risk. The possession and enjoyment of criminal profits can pose the danger not just of detection and prosecution, but also of confiscation. The added risk of losing the profits from their criminal activities serves as a further incentive to criminals to launder their ill-gotten gains. The third reason why organized criminal groups become involved in money-laundering is therefore to circumvent confiscation procedures and to retain the proceeds of their criminal activities.

4.3 SOURCES OF DIRTY MONEY:

Organized crime in all its forms primarily uses the illicit narcotics industry, to finance its affairs. Secondly one should know that `the proceeds of criminal act' which means any offence tribal on accusation, assists and maintains support for the criminal drugs industry, by providing other sources of money which can be used most effectively to disguise the identification of the profits earned from narcotics. It has been stated that the muscle power of crime-mafia is sustained by its enormous financial power, which is acquired by `committing economic offences with impunity'.

The primary sources of criminal proceeds in the Asia/Pacific Group (APG) region were identified as trafficking in human beings and illicit drugs, gambling and the

5 GOI-MHA, 1993:5
activities of organized crime group. Some other identified sources include kidnapping, arms smuggling, hijacking, extortion, public corruption, terrorism and tax evasion. It was also noted that the perpetrators of the predicate offences commonly launder their own proceeds\(^6\).

It is pointed out that it is not the organized crime alone that uses the money laundering techniques; non-organized and opportunistic crimes too use the money laundering tools and can be charged for offence of money laundering (as per the list of predicate offences covered by respective national laws). However, a major percentage of the proceeds subjects to laundering are generated by organized crimes.

**4.4 ORGANIZED CRIME AND MONEY LAUNDERING:**

The basic aim of various criminal activities is exclusively the achievement of a large illegal material profit. Organized crime attempts to legalize such profit, acquired through illegal activities, by introducing it into the normal economic flows. The effects of this are twofold: it conceals the true nature or the origin of that money, and concurrently conceals the existence of criminal acts from which the money resulted. That is, the use of banking, economic and other transactions based on well-established schemes, hinders detection of “black” money so it can be safely used as a legal trade tool, casually utilized by the organized crime to increase such profits.

Overall, money laundering is an important activity of organized crime, as proposed, its typical and common behavior. Corruption, as criminal behaviour of certain individuals in banks or other institutions who ‘launder’ money for a share of profit, is closely related to this phenomenon.

Transnational organized crime simulates the behavior of large transnational companies and increasingly develops so-called strategic cooperation, which strengthens its ability to bypass legislation and criminal responsibility. This also decreases mutual antagonism and minimizes the risk of being

caught in illegal actions, which finally influences the achievement of different profits on the markets in which the “operations” took place. Based on the same rationale used in legal economy, organized crime also promotes entrepreneurship, while both sectors’ final aim involves the achievement of the greatest possible profit. Supporting that the constant flow of new resources from criminal activities and dispersal into new areas of action should not be neglected, the UN officials for combating drug trafficking and organized crime, emphasize that a large portion of global economy, even the 1/5 as some propose, belongs to organized crime activities, mainly weapons, drugs and human trafficking.

In this context, the British Guardian columnist reported that “all the leading world banks who have desperately needed cash reached out towards the mafia money, including a significant portion of the incredible 352 billion dollars of drug trafficking profit placed into the global economy. In this way, the black money has been laundered and the global financial system survived the recent crisis due to the organized crime money”. The author of this column quotes Balzac’s idea that “behind each great fortune, there is a great crime” and concludes that governments worldwide “must find political will to deal with grand crime and not only the minor ones”  

The strategy to fight organized crime is not expected to succeed unless the input of dirty money into legal economy is prevented. Particularly, since organized crime bases its power on money resulting from criminal acts, this money subsequently reinforces corruption and enters legal economy, and laundering such ‘black’ money covers the nature, origins and existence of illegally acquired funds, concealing the criminal act it has resulted from. Moreover, it provides smooth utilization of the acquired funds and allows expansion of criminal activities with numerous implications for a society as a whole.

---

4.5 KEY FEATURES OF ORGANIZED CRIME AND MONEY LAUNDERING:

The various features of organized criminal groups which help them carry out their criminal activities without any difficulties.

4.5.1 POLITICAL DIMENSION:

One identifying phenomenon of organized crime is the easiness with which it is able to creep into and corrupt the political, executive and judicial systems of the host nations, while at the same time, their activities can go beyond `national boundaries' reaching the highest positions in public life. Once they are able to infiltrate the public and power systems, they get the protection for their criminal and financial enterprises.

4.5.2 COMMERCIAL DIMENSION:

Second important element of the organized crime is- it is run like a private commercial enterprise. The Mafia’s, run their operations under the mask of respectable commercial fronts. They use the services of reputed firms of lawyers and accountants for their legal and commercial requirements. Many a time, they even pay their taxes, realizing that the most efficient way to launder illegal money is to declare it to the Revenue.

4.5.3 HIERARCHICAL STRUCTURE:

The third element of an organized criminal enterprise is its distinct hierarchical structure with additional feature of `familial' ties within the criminal group thus implying an even greater degree of loyalty and `constituting a form of disciplined, self-perpetuating criminal structure’.

---

8 Bosworth-Davies & Salt marsh, 1994:31
### 4.5.4 USE OF VIOLENCE:

The fourth aspect differentiating criminal enterprise from a legitimate activity is its willingness to resort to violence (even acts of murder and other crimes against the person) to enforce internal discipline and to achieve passive acceptance of its activities by sections of general population\(^{10}\). Violence is also used to achieve payment of its debts; to protect its investments; or maintain the independence of its operations.

Royal Canadian Mounted Police (RCMP Canada)\(^ {11}\) mentions fourteen characteristics of organized crime groups, which have been listed below:

1. **Corruption:**
   - The use of illicit influence, exploitation of weaknesses, and the blackmail of public and prominent figures.

2. **Discipline:**
   - The enforcement of obedience to the organization through fear and violence.

3. **Infiltration:**
   - Continued effort to gain a foothold in legitimate institutions to further profit or gain a level of protection from detection.

4. **Insulation:**
   - Protection of the organization's leaders by separating them from the soldiers, cell from cell, and function from function.

5. **Monopoly:**
   - Control over certain criminal activities within a geographic area with no tolerance for competition.

6. **Motivation:**
   - Sole motivation is power and influence resulting from the accumulation of wealth (whereas terrorists are motivated by political or social gains).

---

\(^{10}\) NCIS Briefing Paper, 1993 as cited in Bosworth-Davies & Saltmarsh, 1994:32-33

7. **Subversion:**
   Of society's institutions and legal and moral value systems.

8. **History:**
   Long continued period of activity allows entrenchment and refinement of criminal practices.

9. **Violence:**
   Used without hesitation to achieve criminal aims of the organization.

10. **Sophistication:**
    In the use of advanced communication systems, financial controls, and operations.

11. **Continuity:**
    Like a corporation, the organizations survive the individuals who created and run it.

12. **Diversity:**
    In illicit activities, to further insulate the organizations from dependence on one criminal activity.

13. **Bonding:**
    Individual to individual, and individual to organization, for solidarity and protection, often through complex initiation rites.

14. **Mobility:**
    A disregard for national and jurisdictional boundaries.

### 4.5.5 EXAMPLE OF NEXUS BETWEEN CRIME AND MONEY LAUNDERING:

Following example and diagram shows the nexus between the money laundering and organised crime.

1. **Money laundering case related to drug trafficking network**

   The chart\(^{12}\) explains the transactions and methods involved in a particular money laundering scheme.

---

A number of individuals in Canada used a variety of money services businesses to send number of wire transfers overseas that were under the reporting entrance which is also known as ‘structuring’. The transfers were sent to numerous money services businesses in Central America and the Caribbean and were received by three individuals. One of them used the money to buy and consign a large quantity of cocaine to Canada, while the other two were supposed of having relations to organized crime. All three were supposed to have used the funds to buy the cocaine that was being consigned. The drug consignment was seized by police at a Canadian port.

II. Money Laundering and Terrorist Financing

The chart explains a particularly alleged terrorist financing scheme. Different individuals and entities in Canada and the United States make electronic funds transfers particularly to two money services businesses and company, which is located in Canada. Multiple money services business agent locations in Canada and the United States were used to send electronic funds transfers and
cheques to the two money services businesses and the company; in return, the money services businesses performed currency exchanges for the money services business agent locations and sent back electronic funds transfers and bank drafts, while the company sent back bank drafts and cheques. The company also purchased gold bullion. Three individuals – one involved with one of the Canadian money services businesses, the other two involved with the Canadian company – exported currency and sent electronic funds transfers to seven individuals in a foreign country, all of whom were linked to a terrorist organization. For this reason, law enforcement suspected the three individuals in Canada of terrorist financing.
4.5.6 LIST 1: TOP DESTINATION OR ORIGINATING JURISDICTIONS OF ELECTRONIC FUNDS TRANSFERS RELATED TO SUSPECTED MONEY LAUNDERING CASES INVOLVING DRUG OFFENCES:¹³

1) United States of America
2) India
3) Vietnam
4) Hong Kong
5) China
6) Taiwan
7) Iran
8) United Kingdom
9) Belarus
10) Latvia
11) Switzerland
12) Mexico
13) Peru
14) Israel
15) Thailand

4.5.7 LIST 2: TOP DESTINATION OR ORIGINATING JURISDICTIONS OF ELECTRONIC FUNDS TRANSFERS RELATED TO SUSPECTED MONEY LAUNDERING CASES INVOLVING FRAUD OFFENCES (EXCEPT SECURITIES/INVESTMENT FRAUD):¹⁴

1) United States of America
2) United Kingdom
3) Iran
4) Japan

¹³ FINTRAC Typologies and Trends Reports – April 2012
¹⁴ FINTRAC Typologies and Trends Reports – April 2012
5) Hong Kong
6) Israel
7) Switzerland
8) China
9) Germany
10) Italy
11) Austria
12) France
13) Cyprus
14) Guernsey
15) India

4.5.8 LIST 3: TOP DESTINATION OR ORIGINATING JURISDICTIONS OF ELECTRONIC FUNDS TRANSFERS RELATED TO SUSPECTED MONEY LAUNDERING CASES INVOLVING SECURITIES/INVESTMENT FRAUD OFFENCES:¹⁵

1) United States of America
2) Netherlands Antilles
3) United Kingdom
4) China
5) Mexico
6) Bahamas
7) Antigua and Barbuda
8) Netherlands
9) Bermuda
10) Hong Kong
11) Panama
12) Dominican Republic
13) Turks and Caicos

¹⁵ FINTRAC Typologies and Trends Reports – April 2012
14) Barbados
15) Luxembourg

4.5.9 LIST 4: TOP DESTINATION OR ORIGINATING JURISDICTIONS OF ELECTRONIC FUNDS TRANSFERS RELATED TO SUSPECTED TERRORIST FINANCING CASES:

1) United States of America
2) United Arab Emirates
3) Lebanon
4) Pakistan
5) United Kingdom
6) India
7) Austria
8) Netherlands
9) Iran
10) Hong Kong
11) Sri Lanka
12) Saudi Arabia
13) Switzerland
14) Hungary
15) Turkey

The countries mentioned above are big financial hubs. Out of these some of jurisdictions are entry points for drug traffickers, some are known for being tax havens and offshore financial centres, or locations of terrorist groups. The most commonly represented jurisdictions across the recognized predicate offences were the USA, the UK and Hong Kong. Hong Kong is known as an offshore financial centre and for having strong bank secrecy laws.

16 FINTRAC Typologies and Trends Reports – April 2012
Jurisdictions such as Vietnam, Taiwan, Belarus, Latvia, Peru and Thailand only appeared in the top 15 of drug-related cases (List 1). Both Vietnam and Thailand have been previously identified by the Financial Action Task Force (FATF) as having deficient AML/ATF regimes, which have since improved. The Asia-Pacific region is known for its supply and smuggling routes. Latvia is a regional financial centre and is vulnerable to organized crime activity, which may explain its ranking in this category. Drug trafficking is a primary source of illicit proceeds in Belarus, which is also a drug transhipment point. Peru is known as a top producer of cocaine.

In terms of general fraud-related cases (List 2), Japan, Germany, Italy, France, Cyprus and Guernsey were the jurisdictions identified uniquely. Europe had the greatest representation in this category, which included the UK, Switzerland, Germany, Italy, Austria, France, and Guernsey.

The securities/investment fraud category in List 3 had the highest number of unique jurisdictions not found in other categories. These jurisdictions were the Netherlands Antilles, Bahamas, Antigua and Barbuda, Bermuda, Panama, Dominican Republic, Turks and Caicos Islands, Barbados and Luxembourg. With the exception of the Dominican Republic, all of these jurisdictions have strong bank secrecy laws. Antigua and Barbuda and the northern part of Cyprus were previously identified by the FATF as having deficiencies in their AML/ATF regime; these have since improved.

United Arab Emirates (UAE), Lebanon, Pakistan, Sri Lanka, Saudi Arabia, Hungary and Turkey. Some of the jurisdictions identified in List 4 have direct and indirect associations to terrorism, where they have been either a target of terrorism or a training/organizational base for terrorist activity. These jurisdictions include Lebanon, Pakistan, India, Iran, Sri Lanka, Saudi Arabia, and Turkey. The FATF has singled out Sri Lanka, Pakistan and Turkey as having deficient AML/ATF regimes. India’s geographic location makes it susceptible to drug trafficking via neighbouring countries and it is a significant target for terrorism. The UAE is a major financial centre in the Middle East.
region, as well as a leading trade and transportation hub. Due to its geographic location, the UAE is vulnerable to money laundering and terrorist financing.

4.6 PRINCIPAL TRANS-NATIONAL CRIMINAL ORGANIZATIONS (TCOs) INVOLVED IN MONEY LAUNDERING:

This section briefly discusses principal traditional groups of TCOs operating in different regions of the globe for which 'purifying' the profits using money laundering tools are most essential for their survival and sustenance.

4.6.1 ITALIAN CRIMINAL ENTERPRISES:

Italian organized crime is commonly thought of as the Mafia. But the *Mafia is only one of four distinct criminal groups* operating from Italy. The other three are the Camorra, the 'Ndrangheta, and the Sacra Corona Unita (Sacred Crown). These groups are organized on family/clan relationship, and have existed for centuries through a system of power known as *sistema delpotere*.

- **The Mafia** –

  The Sicilian Mafia or *Coosa Nostra* (literally, "our affairs") is the most known organized crime group. Worldwide it is controlled from its historic home of Palermo. It operates in more than 40 countries including the heroin producing nations of Far East. The Mafia consists of approximately 180 families with 5000 members. From Palermo, the Sicilian Mafia controls crime and criminal groups the world over. France's Foreign Intelligence Service estimates that as much as $20 billion in laundering criminal profits returns each year to Palermo, a city that ranks 80th among Italian cities in reported per capita income but fifth in consumer spending.17

  The Mafia and the Russian Mafia have operated jointly too in drug and human trafficking, using Russian transportation and the Italian know-how.

---

• **The Camorra –**

The Camorra, based in Naples, Italy is made up of 30 family and approximately 6000 members. It is known as 'up and coming' criminal enterprise, often trumping the Sicilian Mafia in its ability to adapt to new trends and forming new alliances. The Camorra is known to have strong ties with Russian Mafia. In 1995, the Camorra and the Mafia had an arrangement whereby the Camorra would bleach out US $1 bills and reprint them as US $100, then ship them to the Mafia for distribution in 29 eastern block and FSU (former Soviet Union) countries. In exchange the Russians paid the Camorra with property (including a Russian Bank) and FSU arms, smuggled into Eastern Europe and Italy. In August 1997, Italian 'anti Mafia police' seized approximately US $285 million in assets (200 buildings, 49 land holdings, 26 companies, race horses, cars, stocks and bonds) of the powerful Caserta clan of the Camorra.

• **`Ndrangheta –**

The' Ndrangheta is based in Calabria’s and is especially active in heroin trafficking. In 1989' Ndrangheta group was found to use Pizza shops in major east coast cities in US as fronts for heroin trafficking and used a New York travel agency to launder their money.

• **Sacra Corona Unita (Sacred Crown) –**

It is relatively new group founded in 1970 comprising of 20 families with 1400 members. It is concentrated in Puglia, Italy.

**4.6.2 THE RUSSIAN MAFIA:**

In size, resources, brutality and growth, the Russian Mafia is becoming the world's dominant criminal organization. In Russia it is known as racketeers

---

and in the US as ROC (Russian Organized Crime) or Red fell as. The Russian Mafia consists of 100,000 members organized in about 300 structured groups. Of these following three are well-known:

- The Brigade of the Sun,
- The Odessa Mafia, and
- The American Organized Crime Groups.

Although Russian criminal class existed for centuries, the Russian Mafia as known today took birth with the collapse of former USSR (Dec 25, 1991). A wave of criminality supreme in modern days was unleashed with the end of the old Soviet regime. The Russian Mafia includes much of the ruling class from the old KGB. Russian Mafia has their operational base in the pockets of refugee Russians. Worldwide, it is involved in narcotics trafficking, slavery and human smuggling, car theft, extortion, currency and arms smuggling (including submarines, nuclear arms), murder for hire, credit theft, forgery and fuel/gas frauds, insurance /business frauds, design and production of designer drugs, illegal exports of raw materials (as much as $40 billion per year excluding the business of Russia's most lucrative export, diamonds) and of course money laundering.

It is estimated that its control over 400 Russian banks allows it to launder an estimated $250 billion per year of its own and others' (mainly Italian Mafia's) international drug profits. Mafia controls 8596 of the voting stock of Russian corporations and 5096 to 8096 of all Russian banks.21

The Mafia strictly follows an 18-part "thieve' Code" or Italian vorovsky zakan. A typical Mafia group's chief controls its various criminal cells through a Brigadier. Each cell has got specialty like drugs, prostitution, political contacts, enforcement, smuggling, rackets, and protection. To contain the activities of Russian Mafia FBI (US) entered into an understanding with their Russian counterpart, Russian Interior Ministry's FSB (Federal Security Service).

4.6.3 JAPANESE YAKUZA:

The *Boryokudon*, known as the Yakuza, has origin traced back to early 1600s, when wandering gangs of strange *samurai*, known as *Kaubukimono* (literally crazy ones) terrorized villages, defended by the *machi yokko* (servants of the term). Yakuza has about 60,000 members making it the second largest criminal group after the Chinese Triads. Yakuza groups are loosely organized into families, which are led by the *Oyabum* or the father. The under-boss, officers, enlisted men, and apprentices all serve *Oyabum*.

In March 1992 the Japanese Government passed the *Act for Prevention of Unlawful Activities* by Yakuza or criminal gang members. But their criminal activities continue. The Yakuza remain involved in every aspect of Japan's economy, both legitimate and illegitimate with emphasis on drug distribution, casinos, brothels, hard-core pornography, loan sharking, and extortion focusing on large corporations and banks. They have floated state gangs too around the world with major bases in South Korea, Australia, Brazil and all major cities on the west coast of the US.

Today $300 billion to $600 billion in bad debts are owed to Yakuza-affiliated real estate speculators and the banks are afraid to collect it.\(^2\)

4.6.4 THE CHINESE TRIADS (TONGS):

The six great triads along with smaller satellite groups form the world's largest criminal association. They have over 100,000 members scattered all over the world.

Five of these Triads are in Hong Kong and Taiwan and have formed an alliance with the Great Circle Triad of Shanghai. Of these the largest and most powerful is Hong Kong based *Sun Yee On* ("new righteousness and peace") Triad, which is a 56,000 strong, tightly structured organization involved in all

---

aspects of criminal activity including extortion, heroin trafficking, and alien smuggling in Canada, Australia, Thailand and Central America. Two Triads, which are prominent in America, are *Sum Yee On* and WO Hop To.

The Triads are structured like a modern business enterprise. They control the eastern Asian heroin trade, with annual profits in excess of $200 billion. Smuggling weapons accounts for about $3 billion per year; and the "importation" of illegal aliens into North America and Europe brings in about $3.5 billion per year. The smuggling in of illicit aliens give them double benefit: not only do the triads charge as much as $30,000 to smuggle into the US; that person is sold as slave to brokers, who assimilate his/her into the various China-towns where he/she works for years to pay off fee by manning the Triads' brothels, sweat shops, and drug businesses. Triads are also known as 'tongs' in North America. Almost all the heroin flowing through China and Hong Kong is the 'businesses' of the Triads and originates in the jungles of the "Golden Triangle" of Thailand, Myanmar, and Laos. Martin Booth in his book *The Triads* points out:

"(Triads) no longer confine themselves to sucking the life blood from Chinese community... they are now major players in international syndicated crimes.... The key to this power is not street.... The real money comes from heroin in particular"  

23

4.6.5 **COLOMBIAN DRUG CARTELS:**

Most important among the drug barons are the Colombian drug cartels, who are powerful players in the drug trade not only in the North and South America but also in Europe24. A few of these are:

- **The Medellin Cartel –**

Prior to its collapse in the late 1980s, drug kingpins operating from Medellin, Colombia, controlled the world's cocaine trade. The main kingpin controlling

---

the operations till his death was Pablo Escobar Gaviria. The Medellin Cartel was at its peak during 1984 to 1987. It was responsible for the assassination of at least 15 Colombia judges and a number of US DEA informants.

The documents seized in 1989 from Medellin drug kingpin Jose Gacha showed that he had about $300 million stashed away: about $140 million in various banks and about $150 million actually buried in various locations in Colombia.

- **The Cali Cartel –**

Gacha's death, combined with other incidents made way for the Cali Cartel to take place of the Medellin Cartel. The Cali Cartel is now responsible for 8096 of the world's cocaine supply—over 600 metric tons per year. They have effective control of the Peru-Bolivia-Colombia cocaine production and distribution trade. The Cali Cartel uses deception and guile whereas the Medellin Cartel relied primarily on violence and corruption. Cali Cartel kingpins' profits were more than US $8 billion for 1995 alone. To put it in perspective- in 1997, Coca Cola's total sales were approximately 8 billion (with profits of $120 million); General motors and Wal-Mart's combined profits were just less than 8 billion. If the Cali Cartel were a corporate, it would rank number one in gross profits, beating out Exxon ($7 billion), General Electric ($6.3 billion), and IBM ($5.4 billion)\(^2\).

- **Cartel de le Corta –**

Following the arrests of main bosses of the Medellin and Cali Cartel, the Cartel de le Corta emerged as the new and prominent Colombia based drug trafficking organization. It distributes cocaine in Europe as well as in the U.S.

---

4.6.6 MEXICO'S MEXICAN FEDERATION:

There are following four major groups from Mexico under the umbrella of the Mexican Federation:

- Gulf Cartel
- Juarez Cartel
- Sonarh Cartel
- Tijuana Cartel

They control the majority of the heroin, cocaine, and marijuana production, smuggling and distribution in Mexico and Western US controlling different geographical areas along the Mexico-US border. The Mexican Federation launders over $ 7 billion annually, equivalent to about 2.596 of the Mexican economy's value.

- Amezque Organization-

Amezque Organization is the fifth group mainly controlling the Mexican methamphetamine trade.

4.6.7 PANAMA'S MANUAL NORIEGA:

Noriega, Panama's dictator until 1998 "earned" millions between 1982 to 1988 through his drug smuggling and money laundering activities.

There are other criminal organizations, which are working in different regions of the world. They are smaller yet more organized and have specific criminal specialties. They work with and for principal TCOs mentioned above like a franchisee entity. Important among them are Nigerian criminal organizations that are drug smuggling specialists.²⁶

4.6.8 INDIA'S UNDERWORLD:

Indian Mafioso principally operates in India's metro-cities and also in its various States capital cities. The two important notorious gangs comprising Indian Mafioso are the Dawood gang and the Rajan gang also known as 'D' gang and 'R' gang respectively.27

The chief of these gangs is always the unchallengeable leader and commander with all control power and command functions vested in him. The second rung leaders operate with a sub-group of four to five operatives in their assigned geographical areas. These operatives are assisted by foot soldiers including persons with specialized knowledge and skills.28

- The 'D' Gang- Dawood Ibrahim Kaskar known to common man as Dawood or Bhaii heads the 'D' gang. He jumped bail in a murder case and left India in 1984 shifting his headquarters to Dubai in Middle East. Presently he is headquartered in Karachi (Pakistan).

'D' gang runs its commerce of `contract killing' (\textit{supari commerce}) and its other immoral activities like drug trafficking, extortion and protection racket mainly in the States of Maharashtra and Gujarat but has its operational presence in other parts of India as well. It has got its bases outside India in Katmandu (Nepal), Karachi (Pakistan), Dubai, London.29

It is said that Dawood gang has got operational networking not only with smugglers, drug traffickers but also with the rogue elements in politics, business and bureaucracy. Ajit Ninan's cartoon "Don Bad man's XI" vividly illustrates this (see Fig. II.ii).30

---

27 Nair, 2002:58.
29 Nair, 2002:65.
30 Source: India Today, 2001 "Don Bad man's XI by Ajit Ninan" \textit{India Today} 3rd September, XXVI (36) 10
• The ‘R’ Gang - The ‘R’ gang’s chief is Rajan. He initially was a close associate of Dawood. He split up after 1993 Mumbai riots and floated his own gang. Other than Mumbai in India, ‘R’ gang has bases in Malaysia, Hong Kong, Nepal and Singapore. About the operations of these gangs, it has been commented that their activities seriously jeopardize the smooth functioning of the administration, and the safety of life and property of the common man causing a sense of despair and alienation among the people. At times underworld mafia push the State apparatus into irrelevance.

Some of the major terrorist groups have been listed in Appendix B.

The possible social and political costs of money laundering, if left unchecked or dealt with ineffectively, are serious. Organized crime can infiltrate financial institutions, acquire control of large sectors of the economy through investment, or offer bribes to public officials and, indeed, governments.

The economic and political influence of criminal organizations can weaken the social fabric, collective ethical standards, and, ultimately, the democratic institutions of society. This criminal influence can undermine countries undergoing the transition to democratic systems.

Most fundamentally, money laundering is inextricably linked to the underlying criminal activity that generated it. Laundering enables criminal activity to continue.

4.7 E-COMMERCE, THE INTERNET AND THE MONEY LAUNDERING:

4.7.1 SPREAD OF INFORMATION TECHNOLOGY:

The world has experienced an information explosion in the past two decades. The Internet has been mainly responsible for this information blast. Through this medium, which has been networked to various servers, it has become possible for people in the comfort of their own homes to access information about practically anything in the world, from the various websites, through their personal computers- of which there were estimated to be one billion in 2002. To give some idea of the spread and reach of this information boom, the population of Internet users worldwide has been estimated at half a billion in 2002.

Starting out with the information boom, e-commerce has also opened up several opportunities for trade and commerce. It is now possible to draw up contacts, letters of credits and other instruments of trade and to communicate the same on the internet; prior to communication, all of these documents can also be certified by digital signatures. Even hard copies can be scanned and contracts and other papers sent to trading partners via the internet. To make these commercial transactions secure and also to ensure the privacy of individuals, cryptography is being utilized.
4.7.2 E-COMMERCE: GAINING IN STRENGTH:

Today the whole of commercial transactions could be paperless; relevant data is stored in the computers at either end after it has been communicated through electronic impulses. Of course, it is always possible to reduce the whole transaction to hard copy by taking a printout of the data. In fact, e-commerce transactions are estimated to be worth hundreds of billions of dollars. By all accounts, e-commerce will witness an exponential increase in the future.

4.7.3 E-COMMERCE, E-MONEY, SECURITIES TRADING ONLINE AND INTERNET GAMBLING:

The spread of this new electronic medium has also extended to other areas which have facilitated the process of e-commerce. E-banking on the Internet, is increasingly used by individuals all over the world; it would be no exaggeration to say that most banking transactions in times to come will probably be through this medium. Electronic money, in other words digital cash, also known as smart/cash cards, is very much in vogue; like e-banking, the use of e-money is also bound to increase over the next few years. Both e-banking and e-money aid e-commerce by ensuring that the speed of payments keeps pace with the speed of commercial transactions.

Another area in which the internet has become increasingly popular and where is being used extensively is that relating to trading in securities on the capital markets; the computerization of stock exchanges and their link through the Internet was one of the early developments which led to this new medium being heavily used for securities trading. Internet gambling is another activity that has caught on like wildfire. Both trading in securities on the internet and online gambling offer huge scope to criminals to launder their proceeds.
4.7.4 REASONS FOR PREFERING THIS NEW ELECTRONIC MEDIUM:

At this stage it would be worth examining the reasons for the increasing use of e-commerce, e-banking, e-money, securities trading on the internet and online gambling. With this new electronic medium of the internet, the world seems to have become a much smaller place where one can reach out to areas which were once considered inaccessible; this in turn has led to the greater use of this medium in the field of e-commerce and related activities. E-commerce and other related activities have received a further boost through this new medium because there are no national frontiers to contend with. The speed of transactions is perhaps one of the key factors which has influenced the increasing use of e-commerce. The security of the medium has also been a big contributory factor in the growth of e-commerce and other related activities. Amongst the other features that have led to its growth are that one-to-one contact or detailed time-consuming correspondences are no longer necessary for conducting business.

4.7.5 VULNERABILITIES OF THE INTERNET:

Like anything in this world, the new electronic medium of the internet is also vulnerable both as a medium and in terms of the uses to which it is put. Jurisdiction and the borderless environment are the most problematic areas of this new medium. Anonymity, by which one does not know with whom one is dealing, is another great weakness of the internet. The security offered by this system is also not foolproof; scope for breaches of security is inherent in the interconnectivity through which the system operates: there have been numerous instances of hackers breaching security viruses corrupting and destroying data on a very large scale. In this medium of electronic impulses, one is dealing with virtual data which has been digitalized on the computers; virtual data in itself is a concept that most people have yet to come to grips with in terms of its admissibility as evidence in the context of laws currently in force. Other problems relating to data relate to corruption and loss of it due to
the impermanent nature of data, i.e., it need not to be kept beyond a certain period of time. This medium is also totally unsupervised one; thus lack of supervision is another vulnerable area; even if one has a modicum of built-in software for supervision, this has its limitations. In any given situation human intervention is always a useful input; in this medium there is no human intervention and hence no alarms and no suspects. It is also vulnerable because of the opportunities it offers to create virtual jurisdiction in cyberspace; to establish contact and to exercise control over these virtual jurisdictions would be one of the great challenges with which this medium would have to contend.

4.7.6 THE EMERGENCE OF CYBERCRIME:

Apart from the vulnerabilities of the internet that have been described, it is also a new medium that is prone to crime. Since it is new, what types of crime might be occurring in this medium is still a grey area, as many of the crimes have not yet been identified or detected. It must also be recognized that as the medium evolves and grows, the potential for the occurrence of computer crimes will also increase.

Cybercrime is another name given to computer related crime. Computer crimes can be categorized under three headings. The first type of computer crimes are those where the internet and the computer are the target: hacking, stealing of data, destruction and corruption of data are some of the crimes which fall into this category. The second type of computer crimes are those where the computer becomes a tool for committing crimes; computer related frauds, computer related forgeries, pornography and cyber squatting, amongst many others, are crimes that would fall into this second category. The third type of computer related crime is that in which the computer is incidental to the crime; instances of such crime occur where data/evidence related to the crime is stored in the computer—for instance, in cases of frauds/white-collar crimes.

A draft European Convention on Cyber Crimes has been the first international initiative by the Council of Europe to categorize types of cybercrime. This
convention has categorized cybercrimes under four headings. The first pertains to offences against the confidentiality. Integrity and availability of computer data and systems; types of crime under this heading are illegal access, illegal interception, data interference, system interference and misuse of devices; these types of crimes are those in which the computer/internet are the target. The second heading pertains to computer related offences: computer related forgery and computer related frauds fall into this category; these types of crimes are those in which the computer is the tool with which to commit the crime. Heading three of this Convention relates to contract related offences; child pornography is covered under this heading. Under heading four of the Convention, offences related to infringement of copyright and related rights are dealt with.

There is also an interesting study by the Australian Institute of Criminology which has categorized computer crimes as theft of telecommunications services, communications in furtherance of criminal conspiracies, telecommunications piracy, dissemination of offensive materials, electronic money laundering and tax evasion, electronic vandalism, terrorism and extortion, sales and investment frauds, illegal interception of telecommunications and electronic funds transfer frauds.

4.7.7 MONEY LAUNDERING AND E-COMMERCE: SOME DISTINCT ADVANTAGES:

Another outcome of the increasing of e-commerce will be that the money laundering process will become much easier. Anonymity, security, speed, ease of communication, borderless trading and lack of supervision are all facets of the internet that would facilitate the process of money laundering. This new medium would also make the placement of money much easier through internet banking and through digital cash (smart cards/cash cards) where no banks are involved. The process of layering the money and integrating the same as laundered money would also become easier through the medium of internet, because money can pass through a greater number of jurisdictions
with relative ease and speed, with all the other attendant advantages that this medium offers.

Intermediaries located in financial heavens, also known as facilitators, generally play a very important role in money laundering. These intermediaries are generally chartered accountants, lawyers, company formation agents and other professionals in the field of finance. This medium would do away with the need for these intermediaries and therefore make not only e-commerce but also money laundering more cost effective and cheaper.

The newness of the medium is another feature that will aid the process of money laundering. In this new electronic medium, since the rules of the game have yet to be fully laid out, especially with regard to regulations and enforcement, the process of money laundering could be greatly facilitated.

Internet trading in securities is now known to be a *modus operandi* widely used by money launderers to explain their proceeds of crime. In the layering and integration process, the securities markets, especially those where international trading of securities takes place, are very useful for passing off criminal proceeds as legitimate earnings from stock exchanges.

Likewise, internet gambling is increasingly being used to launder money. A number of financial havens have private internet casinos in place. These casinos are a very convenient tool for laundering money. The potential for internet gambling being used to launder money can be gauged from the fact that in-house gambling was estimated at a staggering US$ 49 billion worldwide in 1998. the way in which internet gambling is spreading, coupled with the intense competition amongst financial havens to extend this facility further, will result in more money being laundered using this method. Most of the servers of these internet casinos, including the casinos themselves, are located in the financial havens; sometimes the server is in one financial haven and the casino in another. The customers of these internet casinos can be from principal onshore centres, other financial havens, or anywhere in the world. Some of the ‘captive internet casinos’ are sometimes simply fronts for passing off illegal proceeds as earnings from gambling and thereby launder the same.
Sometimes these casinos may be in collusion with the criminals and book their bets in a doctored manner to pass them off as casino winnings, once again with the intention of laundering the money.

Reporting of suspicious transactions in which a large turnover of money takes place, such as in banks, brokerage houses, money changers, money transmission agents and the securities markets, is nowadays considered to be one of the principal tools for countering money laundering; in such a fast-moving medium as the internet, suspicious transactions tend to go unreported, especially when norms for reporting such transactions are not clearly laid out. Moreover, intelligent reporting of suspicious transactions would always remain a remote possibility on the internet because of lack of the physical presence of human intelligence; perhaps refining of software might help to some extent in expeditious analysis. Even due diligence processes such as ‘know your customer’, which again are an integral part of the fight against money laundering, tend to be ignored in this new medium.

4.7.8 PROBLEMS WITH REGARD TO ENFORCEMENT:

Several problematic areas peculiar to law enforcement also have to be tackled in the context of this new medium of the internet. The first problem is that of jurisdiction; in the event of an offence being committed on the internet, which country has the jurisdiction to take cognizance? Since the internet is a borderless world, the consensus is now veering toward the view that the country where the server is located is the one which should exercise jurisdiction to investigate and take further follow-up action in relation to a crime. Law enforcement is also greatly hampered due to the fact that in the most countries there are no laws to deal with computer crimes, or even to regulate this new and fast-moving medium. Moreover, as has already been discussed, cybercrimes have not yet been comprehensively identified; to codify criminal code for effective policing of the internet is therefore still a long way off. ‘Criminal intention’ or ‘mens rea’, which is one of the essential requirements to treat an act as a crime, is very difficult to prove in this
electronic medium. Since one is dealing with virtual data, the question of its admissibility as evidence is yet to be resolved; the virtual nature of data also poses other problems with regard to effective law enforcement. Even the assets in this new medium, which are of intangible nature, tend to confound law enforcement when it comes to search and seizure of such assets. Since the computerized networked environment is a totally new and unfamiliar medium, ways for conducting searches and seizures within it have yet to be fully devised by law enforcement.

Admissibility of new forms of evidence that could emerge in this new medium must also be evaluated; the question of new forms of evidence becomes all the more important because they will tend to conflict with the existing laws to a large extent. Several other problem areas relating to law enforcement in this new medium could be listed. Many other new areas that law enforcement has never dealt with before are also likely to emerge in the future.

4.7.9 SOME OTHER IMPORTANT DIMENSIONS:

1. Right to privacy and use of cryptography

The right to privacy in this electronic medium is another issue around which a great debate is raging. Some argue that the right of privacy is absolute, which of course is a totally untenable position. If there is wrongdoing or some crime that has been committed in this new medium, it must be investigated and to that extent the right of privacy needs to be curtailed. The rules of the game with regard to privacy and access to regulatory authorities have to be defined and put into place. Cryptography, which is integral to privacy in this new medium, would have to be considerably regulated; several countries are even talking about keeping cryptographic keys with third-party mediators to resolve all issues relating to rights of privacy as opposed to access to information.
2. Need for an effective audit trail

In order to monitor this electronic medium effectively and ensure that it is not abused, an effective audit trail would need to be built up with respect to all communications and data that passes through it. Digital signatures would of course be a very important element in this audit trail. Adequate software could also be devised indicating the source, the destination and the intermediate points for communication of data. Digital cash, which may result in the elimination of banks, would also need to be closely monitored because it could be misused for laundering money and committing a host of other crimes and irregular acts. The monitoring of digital cash at the time of loading could, of course, be ensured, but once this cash enters the electronic medium and moves around the world, monitoring it could be highly problematic; effective ways and means would have to be devised to do the same.

3. The concept of cyberspace

Under this new electronic medium one can not only operate through regular jurisdictions, but also create virtual jurisdiction in cyberspace and operate out of the same. These virtual jurisdictions would offer limitless opportunities for all kinds of clandestine operations, as they might be very difficult to detect. How to detect and police these virtual jurisdictions in cyberspace will be great challenge for enforcement.

4. Enactment of suitable laws to counter cybercrime

Substantive laws, procedural laws and evidentiary laws to deal with cybercrime would also have to be framed by all countries to police this new medium effectively; these laws must take into account all the peculiar problems of the medium that have been referred to earlier with regard to law enforcement.

5. Technology and the changing role of the judiciary

The judiciary would also have to lend itself to change in this fast–moving new electronic medium of the internet. Once new crimes are detected, new laws come into force to deal with them and a regulatory framework is put into
place to deal with several issues, that courts would have to move into a
different gear altogether. The concept of ‘E-courts’ would have to be put into
place to deal with problems thrown up by this new medium. Such E-courts are
already functioning in Singapore, and in them virtual data stored on computers
is admissible evidence; so also are the depositions of witness through video
conferencing, under certain circumstances. It has been the Singapore
experience that these E-courts are able to administer justice in a very speedy
manner. Deposition of evidence through video conferencing in this fast-
moving borderless world, where witnesses could be located at long distances,
would be practical and cost-effective and new methods for administering
justice through E-courts will emerge in the future.

6. Further need to discipline offshore jurisdictions

Amongst some of the other issues pertaining to this new medium are the
recalcitrant offshore jurisdictions which are providing opportunities for its
abuse; these would have to be effectively disciplined and brought into line
with accepted norms of good conduct. The potential for increasing the
mischief, once would also have to be taken into account and countered
effectively. The need for bilateral, regional and international co-operation
cannot be over-emphasized, and suitable treaties and conventions would have
to be drawn up to ensure this.

4.7.10 CONVERGENCE OF TECHNOLOGIES TO BE
RECOGNIZED:

Another factor that needs to be recognized in the context of information
technology/the internet is the convergence of other fast-evolving technologies
such as telecommunications and broadcasting with the internet. Considering
the level of convergence that is likely to emerge, it would be appropriate to
introduce the convergence law to regulate these interrelated technologies and
deal with the problems that they might pose collectively or individually in
terms of crime or otherwise. India is planning to introduce such a convergence
law, and a convergence bill in this respect is pending with the Indian legislature for enactment into law.

4.7.11 SOME ESTIMATES OF THE EXTENT OF COMPUTER-RELATED CRIME:

According to a study carried out in 2000 by Price Waterhouse Coopers, computer fraud is costing Australian organizations almost $4 billion per annum; the worldwide extent of these computer frauds is estimated to be around $250 billion. The ‘I love you’ computer virus originating from the Philippines (in 2000) affected almost 10 million people worldwide, causing an estimated loss of US$ 10 billion. It is conjectured that the ‘I love you’ computer virus could have been a failed attempt at bank robbery or identity theft; this virus, while infecting computers, was also reading and copying passwords from files in every computer it infiltrated, to a website in the Philippines. The dilemma facing law enforcement agencies as to how to deal with computer crime is clearly brought out by the response of the Philippines enforcement authorities to the ‘I love you’ virus; for several days they could not take action because they were searching for an appropriate law to apply in this case.

According to the US Federal Bureau of Investigation (FBI), recent statistics indicate that computer fraud rose by 600% in 1998; of course, today the rate of growth, as also extent of crime, must be much larger. The FBI is one federal agency that is targeting computer crimes at a national level in the US through a network of agents. Up to 1999 it had dealt with almost 18,000 complaints from within the US and outside; the average loss per victim was estimated at US$ 800.

While the Price Waterhouse Coopers study appears to have overstated the extent of computer frauds, the law enforcement response as evidenced by the FBI indicates that it is still trying to come to grips with a crime in a totally new medium.
Perhaps the weakest links in the chain in the fight against computer crimes are the law enforcement agencies. Law enforcement officers worldwide are known to be averse to the use of computers and do not like to work in unfamiliar mediums. In this world of fast-moving convergent technologies, law enforcement officers would have to become computer-literate in order to deal with this type of crime, for which they would also need relevant training.