ECONOMIC CRIME IN A GLOBALIZING SOCIETY: ITS IMPACT ON THE SOUND DEVELOPMENT OF THE STATE - AN INDIAN PERSPECTIVE

*Deepa Mehta**

I. INDIA: THE LAND AND THE PEOPLE

India is a vast sub-continent covering an area of 3, 287,590 sq. km. It extends from the snow covered Himalayas in the north to the tropical rain forests in the south. It is the seventh largest country in the world. It is surrounded by water on three sides: the Arabian Sea on the west, the Bay of Bengal on its east and the Indian Ocean on the south. Neighbouring countries are Pakistan on the northwest, China, Nepal and Bhutan on the north and Bangladesh and Myanmar on the east. India is a federal republic with its national capital in New Delhi. Administratively, it is divided into 28 states and 7 union territories. It is very densely populated with over 1050 million or 1.05 billion people. The national language is Hindi but there are 14 other official languages. Likewise, about 80% of the population is composed of Hindus and others are Muslims, Christians, Sikhs, Buddhists, Jains, Parsis, etc.

On the economic front, India has traditional village farming as well as modern agriculture, handicrafts as well as a wide range of modern industries and a multitude of support services.

In recent years, government controls have been reduced on imports and foreign investment and the growth rate since 1990 has been 6%. Although, poverty has been reduced considerably, overpopulation is still a major handicap and about a quarter of the population is still too poor to be able to afford an adequate diet. Despite that, India has a large number of well-educated people skilled in the English language and is a major exporter of software services and software workers. In fact, the information technology sector leads the strong growth pattern.

India is a Union of States and is governed by a written Constitution, which came into force on 26th November 1949. As I mentioned earlier, India consists of 28 states and 7 union territories. According to the Constitution Parliament can make laws on certain subjects for the whole or any part of India and this is known as the Union List. Similarly, the Legislature of a State can make laws for the State and this is known as the State list. There is also a third list known as the Concurrent list where both the Parliament and the states can legislate. The 'Police' and 'Public Order' are both in the State List but 'Criminal laws' and 'Criminal procedure' are in the Concurrent List. As a result, the Indian Parliament has enacted the basic criminal statutes, namely, the Indian Penal Code, Criminal Procedure Code and Indian Evidence Act but 'Police', being a State subject, is raised and maintained by the State government. Each State or Union Territory has a separate police force. In addition to the state police, the Central government has set up certain central investigating agencies, including the Central Bureau of Investigation. Established on 1 April 1963, and evolved from the Special Police Establishment established in 1941, it is a premier investigative agency of the state government and can take up cases falling within the jurisdiction of the States with their consent. Other investigative agencies are the Narcotics Control Bureau, the Enforcement Directorate, the Central Board of Direct Taxes and the Central Board of Customs and Excise, etc. These agencies investigate criminal cases falling in the ambit of special statutes being administered by them and are empowered to launch prosecutions.

Against such a background, the New Year has heralded an even greater increase in the GDP of the country. The headlines in the Hindustan Times on 1st January, 2004 were 'All sectors on fire, GDP grows 8.4%'. The Times of India stated 'Economy breaks 8% barrier'. Agriculture has grown at 4.1%, manufacturing has clocked 7.3% and services have grown at 9.6% according to data released by the Central

* Inspector General of Police, Chief Vigilance Officer, Delhi Metro Rail Corporation, India.

Statistical Organization. Economic liberalization in India, which commenced in 1991 "has come to stay" as benefits of an open economy have started percolating. Economic liberalization and globalization have opened up the prospects of regional economic integration with the extended neighbourhood and the opening up of markets. However, it has also brought in its fold opportunities for white-collar criminals to manipulate and benefit from business expansion, particularly in the field of financial and capital markets. Lack of understanding and expertise in these new spheres of crime has made it more difficult for government and criminal justice agencies to control and suppress such economic crime.

II. CHARACTERISTICS OF ECONOMIC CRIME

It is important in the first instance to understand the nature of economic crime. Economic or white-collar crime, as it is generally referred to, is a crime committed by a person of a certain social status in the course of his occupation. The economic crime occurs as a deviation from the violator's occupational role. Also, most of the laws involved or violated are not part of the traditional criminal code. Such crimes are corruption, corporate fraud, public fraud, tax evasion, goods smuggling, stock manipulation, currencies forgery, credit card fraud, environmental crime, intellectual property infringement and the more recent phenomenon of cyber crime.

These crimes are different from traditional crimes in the characteristics of their objective and modus operandi. The traditional criminal steals small sums of money and often uses brute force and conventional tools to achieve his aim. On the contrary, a criminal committing an economic crime steals large sums of money and employs technology and communications to carry out unlawful commercial transactions, disturb databases or orchestrate massive frauds. His victims are ignorant and naïve and often remain unaware of the fact that they have been cheated.

Another characteristic of economic, commercial, corporate or white-collar crimes is that they are often perceived as 'good business': and good business often requires 'cutting corners'. Legal violations by corporations are often viewed as part of the business system, much like industrial spying or psychologically suggestive marketing techniques. These activities are considered as an extension of the capitalist system based on profit and a technical adherence to the letter rather than the spirit of the law.

Such crimes are, however, very costly for our society. In contrast to conventional crimes, which affect specific individuals, economic crimes affect society as a whole. For instance, false advertising induces the public to invest in products that do not have the desired effect. Unsafe drugs, pesticides and food additives affect the health of thousands. Exposure to industrial hazards such as unsafe equipment and poisonous materials and emissions have an adverse effect on workers' longevity. That is because many forms of economic crime are relatively invisible, compared with violent crime, for example. The effects on society of economic crime are hidden as public fear and concern are heightened in cases that affect personal security more directly.

A significant proportion of transnational organized crimes assume the nature of global economic crime. Proceeds of transnational crimes such as drug trafficking, extortion, corruption, tax evasion, arms smuggling, terrorism, and fraud have to be laundered. The international economic threat, posed by Global Organized Crime, in an increasingly global economy is among the major "new" threats to national security. Global Economic Crime does not just affect a select group of financial institutions or regional areas; it affects international financial networks and economies at a national level. Laundering billions of dollars in organized crime money worsens national debt problems because the large sums of money are then lost as tax revenue to that country's government. Global Organized Crime can have a damaging effect on political structures, especially fragile democracies and developing economies. As people feel that the government is powerless to stop organized crime, they turn to crime leaders for protection and political institutions begin to deteriorate.

Economic crimes have mushroomed in many countries, especially those that are in the process of economic, social or political development. A number of difficulties arise in the investigation of such offences. The first is that of definition: for instance the characteristics or constituents of 'illegal monopolies' or 'manufacture of unsafe products'. The second is the determination of responsibility: whether it is that of the corporation or the individuals within it. Thirdly, it is often very difficult to prove the intent to commit a crime. Lastly, and perhaps, most importantly, the public, although it is becoming increasingly aware of the

nature of such crimes, is largely apathetic, and even if in some cases it is concerned, is unable to put pressure on the government leaving the issue to a few consumer protection groups.

Cooperation among Global Organized Crime groups has increased as restrictions have lessened between international borders. These foreign havens for criminals and their assets have made it increasingly difficult for Law Enforcement to trace illegal profits; gather evidence on the criminal leaders; and identify and contain criminal groups. These global networks allow organized crime groups to greatly increase the profits of their operations and their methods of evading local governments as they share information, skills, costs, market access and relative strengths.

Financial transactions, while being perfectly legitimate, are extremely complex and involve the financial systems of many countries. Financial markets operate with speed due to modern communications and electronic data processing and create an impression of impropriety. Caution has to be exercised in regulating financial and economic activities in such a way that they foster free competition and do not stifle it through over regulation. In other words, a balance has to be struck between the regulatory and legislative systems.

III. STATE OF ECONOMIC CRIME IN INDIA

Against this backdrop, let us now focus on the state of economic crime in India and its effect on the sound development of the State. I have classified economic crime in India into three groups viz.:

(i) Traditional economic crime such as corruption, smuggling, invoice manipulation, bogus imports;
(ii) Emerging technological economic crime such as credit card frauds, counterfeiting, cyber crime;
(iii) Money laundering and hawala through which proceeds of transnational organized crime are transmitted abroad.

A. Group - I

1. Corruption

Corruption is an economic crime that is a primary reason for low achievement in the poverty alleviation efforts of the nation. Greed and poverty are the two basic reasons for corruption. It occurs in many countries but it has increased substantially in India in recent years. Corruption has a very upsetting impact as it increases injustice and violates human rights. Corruption arises due to monopoly, power and discretion without accountability. Too many laws, rules and formalities perpetuate corruption and provide opportunities for corrupt practices among government officials. The demoralizing fact is that many in high places remain untouched. In 2001, 2990 cases were registered by anti-corruption departments in India and property recovered or seized was of the value of 84000 million rupees.

Mr. N. Vittal, former Central Vigilance Commissioner of India has stated that corruption in India is anti-national involving the transfer of money through 'Hawala' or underground banking and money laundering; corruption is anti-poor; and corruption is anti-economic development. Measures for combating corruption are simplification of rules and procedures, transparency and creation of public awareness, and an effective prosecution and punishment system.

2. Smuggling

Smuggling, which consists of clandestine operations leading to unrecorded trade, is one of the major economic offences affecting India. Though it is not possible to quantify the value of the contraband goods smuggled into this country, it is possible to have some idea of the extent of smuggling from the value of contraband seized which is indicated in the table given below:

Year	Value of the Goods Seized
1988	443 Crores
1989	555 Crores
1990	760 Crores
1991	775 Crores
1992	535 Crores
1993	388 Crores
1994	535 Crores
1995	631 Crores

The high point of smuggling was in 1991 when contrabands worth Rs. 775 crores were seized. Introduction of various liberalization measures such as the gold and silver import policies in 1992-93 have had their impact on customs seizures in that the total value of seizures came down by 30% in 1992.

A look at the seizures of important commodities seized from 1991 to 1996 indicates that gold and silver which accounted for 44% of the total seizures prior to liberalized import policies came down to 21% after liberalization and have been falling further. On the other hand, the seizure of commodities like electronic goods, narcotics, synthetic fabrics, and foreign currency has been rising. In 1990, gold occupied the top position amongst smuggled items followed by silver, electronic items and narcotics. In 1995, however, narcotics occupied the number one position followed by gold, foreign currency, electronics and synthetic fabrics.

Year	1990-91	1991-92	1994-95	1995-96
Gold	198.8	188.5	55.4	50.8
Silver	146.6	147.7	3.6	0.54
Narcotics	25.1	21.8	54.3	77.94
Electronic items	55.5	23.1	51.2	38.0
Foreign currency	7.7	10.8	27.4	40.2
Indian currency	6.5	5.6	6.6	5.6
Synthetic fabrics	4.8	2.0	2.4	12.9
Watches	3.2	6.2	3.3	3.9

Smuggling, in its broader connotation also includes drug trafficking, smuggling of migrants and trafficking in persons.

3. Invoice Manipulation

This is another variety of economic crime affecting India. In fact all developing countries are victims of invoice manipulations. The term means invoicing of goods at a price less or more than the price for which they were actually sold or purchased. Such transactions are collusive between the trade partners. Both are guilty of fabrication of false documents and records and violate national laws with a view to cheating customs and tax authorities.

By under-invoicing, the value of the goods is lowered which would mean lesser payment of import duties. By over-invoicing the value of goods is shown higher which would mean higher out-flow of foreign exchange from the country. By these methods, the country is depleted of its revenues and foreign exchange earnings.

The practice of invoice manipulation has international ramification and adversely affects the economy of the victim country. A number of difficulties are experienced in the investigations of invoice manipulations particularly in retrieving information such as documents like “Bills of Entry, “Shipping Bills,” “Bills of Lading,” “Invoices,” “Letters of Credit,” departure schedules of sailing vessels, etc. despite their being public documents. International cooperation is therefore needed to curb this menace.

4. Bogus Imports

Several cases have come to notice in the recent past, which indicate that there is leakage of foreign exchange through the device of bogus imports. The modus operandi is quite simple. The operator opens a current account in India in a bank authorized to deal in foreign exchange. He usually poses as a small-scale industrialist and produces forged certificates/ documents to establish his credentials. His partners abroad prepare a set of export documents such as an invoice, bill of lading, and bill of exchange and send them through their foreign bank branches to Indian banks for collection. On receipt of these documents, generally on collection basis, the importer’s agent deposits the amount in Indian rupees in his bank’s current account and the bank remits the foreign exchange. No goods, of course, are ever imported and the country loses valuable foreign exchange.

B. Group – II

1. Cyber Crime

The use of computers has grown exponentially during the last few years. Financial networks, communication systems, power stations, modern automobiles and appliances all depend on computers, and these computers can record withdrawals, deposits, purchases, telephone calls, usage of electricity, medical treatments, driving patterns and a lot more. It is therefore not surprising that computer technology is involved in a growing number of crimes. These are generally taken to include theft of computer services, unauthorized access to protected computers, software piracy and the alteration and theft of electronically stored information, extortion committed with the assistance of computers, obtaining unauthorized access to records from banks, credit card issuers or customer reporting agencies, traffic in stolen passwords and transmission of destructive viruses or commands. With the physical growth of the Internet over the past few years, a number of new generation crimes affecting the LAN, WAN and Internet such as theft of communication services, information piracy, forgery and counterfeiting, dissemination of offensive materials, stalking, extortion, electronic vandalism and terrorism, sales and investment fraud, etc. Hacking, computer network breaches, copyright piracy, software piracy, child pornography, password sniffers, credit card frauds, cyber squatting are some of the new terms in the average criminal investigator's dictionary. Highly intelligent persons commit these new generation crimes leaving hardly any trace and making investigation highly difficult and complicated.

Computer crimes are now a matter of growing concern. Traditional barriers to crime faced by criminals are being obliterated by digital technologies. In a digital world, there are no state or international borders; customs agents do not exist. Bits of information flow effortlessly around the globe, rendering the traditional concept of distance meaningless. In the past, the culprit had to be physically present to commit a crime. Now cyber crimes can be committed from anywhere in the world as bits are transmitted over wires, by radio waves or over satellite. Similarly, in the past, companies protected their secrets and bank funds in locked file cabinets and vaults in buildings surrounded by electronic fences and armed guards. Now this information is located in one computer service that is connected to thousands of other computers round the world. Anyone of these networks or even a phone line into a company's main computer is a transnational invitation to crime. Crime in the digital world has another advantage for crooks over "atom-based" crime: electrons and bits have no effective mass or weight. Robbing a bank or an armoured vehicle of cash would pose problems of transportation and storage whereas transfer of money poses no such problems in the digital world.

Information technology is redefining the ways of conducting business and communication, and is shaping the interaction between business and consumers for sale and purchase of goods and services. Traditional commerce has become electronic commerce. It involves selling and purchasing of information, products and services over communication networks. It encompasses a wide array of commercial activities carried out through the use of computers, including online trading of goods and services, electronic fund transfers, online trading of financial instruments and electronic data transfers within and among companies. For purchasing goods or services, a customer is required to pay. While in a traditional business it is done through cash or cheque, in E-business, it is done through digital cash. However, the growth of the electronic mode of conducting business hinges on assuring the consumers and the business that their use of communication network services is secure and reliable, that their transactions are safe, and that they will be able to verify important information about the transacting parties. Security is indispensable to E-commerce. Authentication, integrity and confidentiality are the three issues associated with electronic communications.

Cyber crimes have become a reality in India too. Cyber hackers have broken into and maliciously altered the content of several computer websites, including that of the Ministry of Information Technology and of Parliament. Indian Airlines was subjected to fraud of several millions of rupees by tampering with the computerized booking records. Computer hackers also got into the Bhaba Atomic Research Centre Computer and extracted some data. Some computer professionals, who prepared the software for the M.B.B.S. examination, altered the data and gave an upward revision to some students in return for a hefty fee. A big loss was caused to a bank where the computer records were manipulated to create false debts and credits and in another bank false bank accounts were created. A telephones official manipulated computer terminals by reversing the electronic telephone meter systems, thereby allowing some companies to make overseas calls without charges. In a case of software piracy some of the employees stole a copy of the source code and in another educational software was stolen.

Law enforcement agencies today face a number of challenges in the investigation of such cases. These can be categorized as technical, legal and operational challenges.

Technical challenges:

When a hacker disrupts air traffic control at a local airport or a child pornographer sends computer files over the Internet, or when credit card numbers are stolen from a company engaged in e-commerce, investigators must locate the source of the communication. They have to trace the 'electronic trail' leading from the victim to the perpetrator in almost every case. To succeed in identifying and tracing global communications investigators have to work across borders, not only with one's counterparts but also with industry to preserve critical evidence such as log files, e-mails, etc. before it is altered or deleted. Besides, while less sophisticated cyber criminals may leave electronic 'fingerprints' more experienced criminals know how to conceal their tracks in cyber space. Internet telephony, strong encryption, and wireless and satellite communication and other technological advances have made it possible for international criminals and terrorists to target victims in unprecedented ways.

(i) *Legal challenges:*

Deterring and punishing computer criminals requires a legal structure that will support detection and prosecution of offenders yet the laws defining computer offences, and the legal tools needed to investigate criminals using the Internet, often lag behind social and technological changes, creating legal challenges to law enforcement agencies. In India, however, the Information Technology Act, 2000 has been enacted in pursuance to the General Assembly of United Nations resolution A/RES/51/162, dated the 30th January 1997.

The Information Technology Act elaborates upon digital signature; electronic governance; attribution, acknowledgement and dispatch of electronic records; secure electronic records and secure digital signatures; regulation of certifying authorities; digital signature certificates; duties of subscribers, penalties and adjudication; the cyber regulations appellate tribunal; offences; and non-liability of network service providers in certain cases, etc. It specifies that Electronic Signatures will be valid and legally enforceable only if the e-transaction is done through "public key cryptography". The Act delineates two separate types of penal provisions: contraventions and information technology offences. While contravention results in monetary penalty, the IT offences may result in the offender being imprisoned or paying a fine or both. Tampering with computer source codes, obscenity, hacking, unauthorized access to a protected system, misrepresentation before authorities, breach of confidentiality and privacy, publication of false particulars in digital signature certificates, etc. have been listed as criminal offences under this Act. Amendments have also been made to the Indian Penal code, Indian Evidence Act, the Bankers' Book Evidence Act and Reserve Bank of India Act to facilitate investigation and prosecution of cyber crime.

(ii) *Operational challenges:*

There is a need to have high tech crime units that respond to quick investigation and assist law enforcement agencies faced with computer crimes. The police have to be made cyber sensitive through adequate training and supported by an expert group with specialized knowledge of computer forensics.

Just as investigators followed the trails and physical signs of robbers, modern investigators have to understand and follow a criminal's paper trail, or cyber trail, in the form of invoices, communications, and other records that leave behind evidence of the criminal's passing. A cyber trail is both an extension of crime scenes in the real world, and a digital crime scene in itself. If a crime occurs in the physical world and there is a computer with network access at the crime scene, investigators have to search the computer and network for related digital evidence. Similarly, if a crime is first witnessed or recorded on a network, investigators have to collect all relevant digital evidence on the network and, if possible, determine the physical locations of the primary computers involved and treat those locations as crime scenes.

The investigation of computer crime requires a team effort of police, forensic scientists, lawyers and programmers or system administrators. Police are generally expected to know how to oversee an investigation, but may not know much about computers and computing and thus not know what evidence to look for. Programmers and system administrators may know a great deal about computers, networks, and how they work, but nothing about legal procedural requirements regarding the preservation of evidence. Forensic scientists may know how to deal with evidence but, like the police, may not know what to look for

when dealing with digital evidence or how to apply real-world forensic science methods to it. Lawyers may know about the law of evidence but not much else. But today, when cyber crimes are fast increasing, the police have to learn how to handle digital evidence, use it to generate investigative leads, and to know when to call in an expert for assistance. Programmers and system administrators, who handle digital evidence, need to use it to generate investigative leads, and to know when to call in police for assistance. Forensic scientists have to become intimately familiar with every aspect of digital evidence so that they can process it to support an investigation. Finally, lawyers of both prosecution and defence, have to learn to dig up digital evidence, defend it against common arguments, and determine whether it is admissible. Together, this team will then be able to conduct an investigation of a computer crime, look for evidence, find it, and treat it so as to preserve its admissibility once it is found.

The Central Bureau of Investigation has recently created a Cyber Crime Research & Development Unit which maintains close liaison with international agencies like the FBI, Interpol and other foreign police agencies to share skills and techniques in investigating cyber crimes. The officers of the CBI associated in this exercise share their expertise with the State police forces through regional training programmes held periodically.

2. Counterfeiting

Currency counterfeiting is an organized white-collar crime, which has assumed serious proportions globally. It not only causes serious setbacks to the world's economy but also jeopardizes genuine business transactions. These days, counterfeiting of currency notes is done with the help of modern equipment such as colour scanners, colour laser photocopiers and printers, as well as by computer graphics software. Most of the security features such as the use of complex designs, special paper, watermarks, optical fibre, security thread, micro-printing, currency-printing, colour shift, and holography in genuine notes are copied with the help of advanced computer technology, which provides them with sophistication and perfection.

There has been an upsurge in the incidence of supply of counterfeit Indian currency notes from across India's borders. During the year 1999, counterfeit Indian currency notes valued at Rs. 18.4 million were seized as compared to Rs. 6.5 million during 1998 indicating a threefold increase. Almost half of the total seizures are made from the three states of Uttar Pradesh, Bihar and West Bengal. Counterfeiting of currency is resorted to to gain quick profit, acquire funds for drug trafficking or subversive activities, or mobilize funds for smuggling. Sometimes, external agents in the form of travellers and cross border smugglers are involved. Counterfeit currency can be used for destabilizing economies, provide financial assistance to terrorists and militants for buying arms and ammunition and sponsor religious fundamentalism, etc.

India, as a signatory to the Geneva Convention, 1929, is committed to extend full cooperation to all other countries for eliminating or containing to the furthest extent possible, the counterfeiting of domestic as well as foreign currencies. Indian laws and enforcement measures are in full conformity with the principles laid down in the Convention. The Indian Penal code provides for punishment of varying degrees and up to life imprisonment for counterfeiting any currency or making or possessing instruments or materials for forging or counterfeiting currency notes or for possession of forged or counterfeit currency notes or bank notes.

Counterfeiting, however, goes beyond the production of bogus currency to the counterfeiting of all kinds of manufactured products such as clothing, audio and video equipment, compact discs, watches, liquor, perfumes, etc. In such cases, losses are suffered by the manufacturers of the products, their employees, the economies of the concerned states and the concerned governments that would have received tax revenues.

3. Credit Card Frauds

A major form of economic crime is credit card fraud. Here also, the fraudster is one step ahead of law enforcement agencies as technology has facilitated the manufacture of false cards. As financial institutions introduce innovations against counterfeiting and fraud, increasingly sophisticated ways of profiting from or beating those systems are devised. Most of the credit card fraud is committed by using counterfeited cards, which are re-embossed or re-encoded. Nowadays, counterfeiters have reproduced holograms and encoded magnetic stripes on credit cards. New security measures can only be introduced gradually and if measures are taken against fraudulent card users in one part of the world, they quickly move to another part where detection measures are less sophisticated. Thus, problems associated with these kinds of frauds take a long time to overcome and cause losses around the world. In India, credit card frauds also occur by stealing the

cards and the accompanying information at the time of application or delivery and forging signatures. Sometimes merchants or employees of hotels, restaurants or shops take genuine numbers of cards from sales slips and pass them on to syndicates.

C. Group – III

Before we discuss the strategies that have been adopted by money launderers, let us pause to consider the specific kinds of transnational crimes where proceeds are transmitted out of a country's national borders.

1. Transnational Organized Gangs

In the sixties and seventies India had Haji Mastaan (gold smuggling), Yusuf Patel (gold smuggling) and Karim Lala (drug smuggling). In the eighties and nineties other gangs emerged. Dawood Ibrahim, Tiger Memon and Mohammad Dosa are reportedly operating from abroad (Dubai) and are involved in extortion of money from builders and film producers, mediating in monetary disputes, and undertaking contract killings. The other major gangs of Mumbai indulging in organized crime are those of Chota Rajan (Drug Trafficking and Contract Killings), Arun Gawli (Contract Killings and Protection Money), Late Amar Naik (Protection Money), Chota Shakeel and Om Prakash (Babloo) Shrivastava (Kidnappings for ransom and Killings). In the field of terrorism certain transnational organizations such as Lashkar-e-Toiba, Jaish-e-Mohammad, Hizbul Mujahiddin, etc. have been operating. The most essential characteristic of organized crime is making money or "maximisation of profits".

2. Drug Trafficking

Flanked by the Golden Crescent, (South-west Asia) and the Golden Triangle (South-east Asia), India has, due to its geographic location, become the corridor for movement of heroin and hashish to various destinations in Europe, America and Africa. Substances of abuse include alcohol, tobacco and natural and manufactured drugs. A kilogram of heroin, which costs approximately a thousand dollars on the Indo-Pak border, is reportedly sold for 250,000 dollars in Europe or USA.

The global drug trade has grown phenomenally. It is said to fund terrorism and other forms of transnational crime. Legislative measures against drug trafficking include The Narcotic Drug and Psychotropic Substances Act and Rules, 1985 and The Prevention of Illicit Traffic in Narcotic Drugs and Psychotropic Substances Act, 1988. The Narcotics Control Bureau functions as a coordinator between various departments and arranges interagency coordination meetings

International drug trafficking poses a threat to the social fabric of all countries. The increase in the scale of these operations has led to an increase in drug use, addiction, and the general crime level. Drug profits are transferred electronically to dozens of banks around the world in less than 24 hours by using falsified export documents and invoices for goods in order to disguise drug trafficking transactions.

3. Smuggling of Migrants

There have recently been many reports of smuggling migrants from India and an industry has emerged which involves Indian agents recruiting migrants, transporting them to Europe or North America, collecting fees from them and sometimes providing them with jobs in the destination areas. India is both a source and a destination country for migrant workers. Skilled workers from India migrate to the U.S.A., Europe, the Middle East and East Asian countries. Similarly, migration into India takes place from neighbouring countries. Sometimes smuggling and trafficking activities are carried out by criminal networks, which are also involved in trafficking of narcotics, document fraud, money laundering, arms smuggling and other transnational crimes

4. Trafficking in Persons

Trafficking in human beings is a transnational organized crime that involves the illegal trade of human beings, through abduction, threat of force, deception, fraud or "sale" for the purposes of sexual exploitation or forced labour. A major reason is the search for work abroad due to economic disparity, high unemployment and disruption of traditional livelihoods. Traffickers face few risks and earn huge profits by taking advantage of large numbers of potential immigrants. In many cases, drug traffickers have switched to trafficking human beings because it is more lucrative and relatively risk free.

In cross border trafficking, India is a sending, receiving and transit nation. Receiving women and children from neighbouring countries and sending women and children to Middle Eastern nations is a common

occurrence. The long and porous border between India and its neighbouring countries facilitates trafficking in women and girls.

5. Terrorism

Terrorism has been there for quite a while in India. It is characterized by hijacking and killing of well-known individuals, shoot-outs or bomb attacks in public and religious places and more recently, an attempted attack on the Indian Parliament. There are a number of terrorist outfits operating in India such as Lashkar-e-Toiba, Hizbul Mujahidin, Jaish-e-Mohammad and so on.

There are many causes of terrorism ranging from ideology, religion, fundamentalism, fanaticism, politics to corruption and money-laundering and mercenary ones. Different and varied methods have been adopted to create panic – from the hijack of the Indian Airlines aircraft in Afghanistan in December 1999 to suicide strikes evident in the assassinations of former Prime Minister Rajiv Gandhi in 1991 and Chief Minister Beant Singh in 1995 to 'Fidayeen' strikes in Jammu and Kashmir to terrorist attacks such as the attack on the Indian Parliament in 2001, an attack on the American Centre, Kolkata in 2002 and attacks on Akshardham temple and Raghunath temple, also in 2002. . Firm links have also been established between militant outfits in India and the underworld – drug traffickers, border crossers, currency counterfeiters, travel racketeers, mafia syndicates, etc. – which are used not merely as a support mechanism but also to execute actual actions.

6. Trafficking in Arms

The Purulia Arms Drop case is the most glaring example of transnational arms smuggling. In December 1996, an Anotov 26 aircraft dropped over 300 AK 47/56 rifles, ammunition, sniper weapons, rocket launchers and night vision devices in Purulia in West Bengal. The aircraft was bought from Latvia, chartered by a company, Carol Airlines, registered in Hong Kong, moved to Bulgaria to pick up the consignment of arms and finally apprehended in Bombay after it had dropped its consignment. There is evidence of smuggling of arms in Jammu and Kashmir, Punjab and the North East where caches of arms have been seized.

7. Money Laundering

Crime pays and criminals naturally want to be able to enjoy their profits without worrying about the police or the courts. This is not something new. However, globalization has brought about an increase in the international movement of money. The rapid expansion of international financial activity has gone hand in hand with the development of transnational crime, which takes advantage of political borders and exploits the differences between legal systems in order to maximize profits.

Money laundering cannot be disassociated from other forms of crime. It is a fact that it thrives on corruption. Corrupt people use financial techniques to hide their fraudulently obtained assets and the continued successful application of these techniques depends on the involvement of influential accomplices. Money laundering is therefore at the centre of all criminal activity, because it is the common denominator of all other criminal acts, whether the aim is to make profits or hide them.

Laundering operations are, in fact, intended more to conceal the origin of the money than its criminal nature, in other words to hide the traffic from which it is derived rather than the general criminal activity which actually generated it. It is therefore essential to move the money in order to scramble the route it takes. The operation is wholly successful when the nature of the money is also concealed and it is impossible to establish a link with any criminal activity because the different circuits taken give it the appearance of legitimate income.

8. Hawala

The Indian Hawala or Hundi system is the transfer of money through unofficial channels, normally outside the banking channels used by businessmen. The money so transferred often includes the money derived from criminal activities or in violation of the country's legislation. Underground banking, which conveys a sense of a system, may not strictly cover the misuse of a banking channel. It may refer to, in a restricted manner, a system of rendering services, the most important in this context being the transmission of money. Hawala represents such services. It operates in the following manner.

Someone in the U.S.A., for example, deposits $1,000 to an underground banker for payment to be made to an Indian in India. The U.S.A. underground banker contacts his counterpart in India immediately on the

phone or by wire and sends some coded message for payment of money to the Indian recipient. As in a bank, there is no physical transfer of money from one country to another; the accounts are settled by a reverse process when an Indian sends $1000 to someone in the U.S.A. The Indian operator contacts his counterpart in U.S.A. and money is paid in U.S.A. without any physical transfer of money. These operators work in a very organized manner and have a well-knit network. They undertake their business under cover of absolute secrecy and no paper trail for audit is kept. The system operates on an ethnic network. The network may include more than three or four countries. The principal operators engage agents and sub-agents in various countries for collection and disbursement of money. Hawala is widespread in India from metropolitan cities to smaller towns. Members of Indian families earning a living abroad are the clients of the system.

Money laundering and Hawala transactions, threaten developing economies and contribute to illicit drug trafficking and terrorist and subversive activities. As mentioned earier, India, for instance, is a transit point for drug traffickers and other criminals from the Golden Crescent and the Golden Triangle. It has become a conduit for the South East, Middle East, and Far East and Latin American countries. Both non-resident Indians and resident Indians use the Indian Hawala system or underground banking extensively for drug trafficking and remittances of money. In the mid-nineties Bombay was attracting huge amounts of Narcotics money from drug cartels in Columbia (London Times, May, 1993). The private sector is also involved in quick transfer of cash across continents. Travel agents and courier companies target Indians living abroad who want to repatriate money. The time taken to transfer money is much less. Money launderers also use such private companies for money transfers.

There are many reasons for the use of underground banking channels instead of the normal banking system. The high tax rate and the Exchange Control Regulations (though now considerably liberalized) have been the major reasons for Hawala and other economic crimes in India. Underground banking is extensively used for drug trafficking and remittances of money. It is here that the economic offenders and the launderers meet. Economic offenders want to remit money and money launderers help in doing so. Another reason for money laundering is due to evasion of taxes by some corporate houses.

Money laundering techniques include smurfing (a large number of small transactions, each transaction being less than the mandatory transaction reporting threshold), establishment of front companies, remittances through Hawala (non-banking channels), over-invoicing and double invoicing legitimate business (ordering goods at inflated prices and depositing the difference between the real and inflated values in an offshore account) and foreign remittances. Non-resident Indians have been given some special banking facilities. These facilities are misused to bring back the money as white money. For example, a portfolio account is opened in a foreign country and the money is laundered back to be invested in the stock markets. Another modus operandi is to launder the money through bogus exports. The conversion of black money is done by over-invoicing the products. Some shell companies are set up to issue bills or invoices accompanied by bogus transport receipts in order to obtain funds against these documents from bank/financial institutions and then divert major parts of such proceeds by issuing cheques in the names of non-existent front companies of cheque discounters. The cheque discounters then hand over cash immediately to the party after deduction of their commission. They file income tax returns in which the commission is shown as taxable income and also issue fake Letters of Credit and false bills. The cheque discounters are generally associated with commodities markets where fake transactions in commodities can largely go unnoticed.

Money laundering has so far been dealt with mainly under the Foreign Exchange Regulation Act, 1973, but with effect from 1999, FERA has been replaced by the Foreign Exchange Maintenance Act. A bill named as 'The Prevention of Money Laundering Bill' has been introduced in Parliament by the Government of India and is to be enacted as law. Money laundering has been proposed as a cognizable crime punishable with rigorous imprisonment of 3-7 years which could be extended to 10 years and a fine of up to Rs. 0.5 million. The acquisition, possession or owning of money, movable and immovable assets from crime, especially from drug and narcotic crimes, would be tantamount to money laundering. Concealment of information on proceeds or gains from crime committed within India or abroad is proposed to be an offence. An adjudicating authority is proposed which would have powers to confiscate properties of money launderers. An administrator may be appointed to manage the confiscated assets. An appellate tribunal is proposed to be set up to hear appeals. Financial institutions are expected to maintain transaction records and furnish these to the adjudicating authority. Failure to do so would be punishable too.

D. Indian Legislation to deal with Money Launderers

Presently, legislation to deal with such offenders is specifically intended to deprive offenders of the proceeds and benefits derived from the commission of offences against the laws of the country. It provides for the confiscation or forfeiture of the proceeds or assets used in connection with the commission of certain crimes. The concerned Acts in Indian legislation are:

(i) Criminal Law (Amendment) Ordinance, 1944;
(ii) Customs Act, 1962 (Secs. 119 to 122);
(iii) Code of Criminal Procedure, 1973 (Sec. 452);
(iv) Smugglers & Foreign Exchange Manipulators (Forfeiture of Property) Act, 1976;
(v) Narcotic Drugs & Psychotropic Substances Act, 1985 (Sections 68-A to 68-Y);
(vi) In addition, Indian statutes also contain provisions for preventive detention of foreign exchange racketeers under the Conservation of foreign Exchange and Prevention of Smuggling Activities (COFEPOSA) Act, 1974, and of the drug traffickers under the Prevention of Illicit Traffic in Narcotic Drugs and Psychotropic substances (PITNDPS) Act, 1988.

For this purpose, the Government of India has set up the following Investigating Agencies that function under the Department of Revenue in union with the Ministry of Finance.

E. The Central Economic Intelligence Bureau

An apex intelligence and coordinating body, the Central Economic Intelligence Bureau was set up with the intention of coordinating and strengthening intelligence gathering and investigative efforts of all agencies enforcing economic laws. Accordingly, the Bureau collects intelligence regarding aspects of the black economy that require close watch and investigation as well as the emergence of new types of such offences and evolves counter-measures required for effectively dealing with existing and new types of economic offences. It acts as the nodal agency for cooperation and coordination at the international level with other customs, drugs, law enforcement and other agencies in the area of economic offences. It implements the Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1971.

F. The Directorate of Revenue Intelligence

The Directorate of Revenue intelligence is concerned with Customs related offences and collects intelligence about smuggling of contraband goods, narcotics, under-invoicing, over-invoicing, etc. through sources. It analyses and disseminates such intelligence to its field formations for action and keeps a watch over important seizures and investigations. It also functions as the liaison authority for exchange of information among ESCAP countries for combating international smuggling and customs frauds and liaisons with foreign countries, Indian Missions and enforcement agencies abroad as well as with the CBI and INTERPOL on anti-smuggling matters. Cases are referred for action to the Income Tax Department.

G. Enforcement Directorate

The Directorate of Enforcement is mainly concerned with the enforcement of the provisions of the Foreign Exchange Management Act 1999 to prevent leakage of foreign exchange which generally occurs through remittances of Indians abroad otherwise than through normal banking channels; illegal acquisition of foreign currency; non-repatriation of the proceeds of exported goods; unauthorized maintenance of accounts in foreign countries; under-invoicing and over-invoicing of exports and imports and other types of invoice manipulation; siphoning off of foreign exchange against fictitious and bogus imports; illegal acquisition of foreign exchange through Hawala and obtaining secret commissions abroad.

The main functions of the Directorate are to collect intelligence relating to violation of the provisions of the Foreign Exchange Regulation Act; conduct searches of suspected persons, conveyances and premises and investigate such cases. The Directorate also adjudicates cases of violations for levying penalties and confiscates amounts involved in contraventions.

H. The Directorate General of Anti-Evasion (Central Excise)

Due to the growth of the Central Excise revenue and its coverage to almost all manufactured products a specialized intelligence agency, the Directorate of Anti Evasion, was created to target prevention of Central Excise duty evasion. The Directorate collects intelligence relating to evasion of central excise duties, studies their modus operandi and alerts Collectorates. It also studies the price structures, marketing patterns and classification of commodities in respect of which possibilities of evasion are likely in order to

advise Collectorates for plugging loopholes and co-ordinates with Enforcement agencies like Income tax, Sales tax, etc.

I. The Directorate General(s) of Income Tax (Investigation)

The Directorate Generals of Income Tax Investigation deal with all matters connected with investigations under the Income Tax Act of the Central Government. They collect intelligence pertaining to evasion of Direct Taxes and organize searches to unearth black money. They take steps to ensure that persons having information about tax evaders come forward with the same to the Department and disburse rewards.

J. The Narcotics Control Bureau

The national policy on Narcotic Drugs and Psychotropic Substances is based on the Directive Principles contained in the Indian Constitution (Article 47), which directs that the State shall endeavour to bring about prohibition of the consumption, except for medicinal purposes, of intoxicating drugs injurious to health. Besides, India is also a signatory to:

- Single Convention on Narcotic Drugs 1961 as amended by the 1972 Protocol.
- Conventions on Psychotropic Substances 1971.
- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988.

The broad legislative policy in the matter is contained in the three Central Acts, viz. Drugs and Cosmetics Act, 1940, The Narcotic Drugs and Psychotropic Substances Act, 1985, and The Prevention of Illicit Traffic in Narcotic Drugs and Psychotropic Substances Act, 1988. The Department of Revenue has the nodal co-ordination role as administrator of the Narcotic Drugs and Psychotropic Substances Act, 1985 and the Prevention of Illicit Traffic in Narcotic Drugs and Psychotropic Substances Act, 1988.

The Narcotics Control Bureau was constituted in 1986 to exercise the powers and functions of the Central Government for coordination of action by various authorities under the N.D.P.S. Act, Customs Act, Drugs and Cosmetics Act, etc. and for countermeasures against illicit traffic under various international conventions and protocols presently in force. It is the apex-coordinating agency and collects and analyses data related to seizures of narcotic drugs and psychotropic substances, studies trends, modus operandi, collects and disseminates intelligence and works in close cooperation with the Customs, State Police and other law enforcement agencies.

K. Special Investigative Tools

In addition to traditional investigative methods to combat global economic crime, law enforcement agencies utilize special investigative tools such as controlled delivery, undercover operations and electronic surveillance (wiretapping, communications interception, etc.) to effectively fight global economic crime. However, their use is controversial because they may infringe on human rights to privacy or may be misused.

L. Controlled Delivery

Controlled delivery techniques have proven an important enforcement tool in identifying the principles involved in drug trafficking and other major smuggling offences especially those who, by the use of couriers, creation of false documents and other deceptive practices, carefully disassociate themselves and try to be remote from the drug trafficking operations. It is the technique of allowing illicit or suspect consignments… to pass out of, through or into the territory of one or more countries, with the knowledge and under the supervision of their competent authorities, with a view to identifying persons involved in the commission of offences (The United Nations Conference for the Adoption of a Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances). Further, according to Article 11 of the Convention, controlled delivery is to be allowed on the basis of mutual agreements or arrangements between nations.

Section 4 of the Indian Narcotic Drugs and Psychotropic Substances Act, 1985 endorses these international obligations. However, before adopting this technique, the originating country and the recipient country should discuss in detail the entire operation, maintain surveillance simultaneously in both the countries, keep close surveillance on the movement of drugs either through cargo or through couriers, and time the final strike operation simultaneously in both the countries to achieve maximum results. In India,

the Narcotics control Bureau, the nodal agency for enforcement of laws concerning narcotic drugs and psychotropic substances, has undertaken controlled delivery operations with a number of countries from time to time.

M. Electronic Surveillance

Electronic surveillance covers wiretapping, communications interception, etc. Telephone interception and the monitoring of all electronic communications are controversial aspects of electronic surveillance, yet are useful in assisting law agencies to combat global economic crime. In India, interception of messages is covered under subsection 2 of section 5 of the Indian Telegraphic Act, 1885, when it is necessary or expedient to do so in the public interest. Also, a legal provision has been made in the licensing conditions of cellular companies to provide parallel monitoring facilities for all communications being received and emanating from mobile sets.

N. Survey on Economic Crime in India

PriceWaterhouseCoopers Corporation carried out a survey across a sample drawn from the top 1000 Indian companies in the manufacturing, services and financial services sector in 2003. According to the survey, there has been a significant increase in economic crime over the past two years but there has been a reluctance to report it. Corruption and bribery are perceived as the most prevalent economic crimes in India. Reluctance to admit them may be due to fear of adverse implications or acceptance of corruption as an everyday cost of doing business. Other economic crimes having high prevalence include financial misrepresentation, product piracy and counterfeiting. The incidence of low reporting of financial misrepresentation may be attributed to low transparency and poor accountability. Companies appear to be unaware of the extent to which product piracy and counterfeiting are rampant and tend to avoid publicity for fear of adverse implications, particularly their effect on brand image. Perceived prevalence of asset misappropriation and cyber crime in India is also relatively low and suggests the need for tighter internal controls and other deterrents. The reported absence of money laundering is somewhat surprising and seems indicative of poor detection.

Most Indian respondents were unable to quantify their loss arising from economic crime as the financial impact of less tangible economic crimes such as corruption and bribery or product piracy and counterfeiting is difficult to quantify. They are, however, conscious of the collateral cost of economic crime on their business which, apart from financial loss results in undermining of staff morale and impacting business relationships, reputation and brand image.

Audits (external and internal), tip-offs and accident or chance are reported to be the main factors in the detection of economic crime in India. Most organizations are aware that they are required to report frauds but the reporting is low because of a reluctance to initiate recovery proceedings, scepticism about recovery, desire to avoid publicity, concerns regarding implications of disclosure, drawn out litigation process and a propensity to accept certain crimes as a customary business risk. Development of controls in their organization such as organization ethics or a code of conduct will form an effective deterrent in combination with pre-employment screening and fraud detection training. Looking ahead, respondents believe that despite improved controls, vulnerability to corruption and bribery, asset misappropriation and financial misrepresentation continue to be high, despite an expected decline in corruption. However, an increased threat is expected from economic crimes like product piracy and counterfeiting, cyber crime and industrial espionage.

IV. CONCLUSION

National strategies are inherently inadequate for responding to challenges that cross multiple borders and involve multiple jurisdictions and a multiplicity of laws. The rapid growth in global economic crime and the complexity of its investigation requires a global response. At present, the measures adopted to counter these crimes are not only predominantly national, but these measures differ from one country to another. It is absolutely imperative to increase cooperation between the world's law enforcement agencies and to continue to develop the tools, which will help them effectively counter global economic crime.

Tracing the money trail, including the origin of funds, combating money laundering through reduction of bank secrecy and seizure of assets are issues of paramount importance. Putting in place legislation on forfeiture and confiscation of properties acquired through criminal activities and sharing of available

technology on the subject would be a step in the right direction. Extradition is one of the most important tools used for bringing transnational fugitives to justice and extraditable crimes include unlawful seizure of aircraft; unlawful acts against the safety of civil aviation; crimes against internationally protected persons; common law offences like murder, kidnapping, hostage taking; and offences relating to firearms, weapons, explosives and dangerous substances, etc. when used as a means to perpetrate indiscriminate violence involving death or serious injury, or serious damage to property. However, it is also an area that poses the greatest problems. A large number of countries have not entered into extradition treaties and even where such treaties exist, they are mostly embroiled in complicated procedures leading to undue delay in extradition. There is a need for simplifying procedures and expediting the process.

In India, the Extradition Act, 1962 deals with extradition of fugitive criminals. India has extradition treaties with a number of countries. It has also entered into Mutual Legal Assistance Agreements/Treaties in criminal matters such as the investigation and prosecution of crime and the tracing, restraint and confiscation of the proceeds and instruments of crime, including currency transfer and terrorist funds with a number of countries. India is a signatory to the United Nations Convention against Transnational Organized Crime and to the South Asia Association for Regional Cooperation (SAARC) Convention for Suppression of Terrorism. Pursuant to the SAARC Convention, India enacted the SAARC Convention (Suppression of Terrorism) Act.