CHAPTER-3
NATURE, CLASSIFICATION AND DIMENSION

This chapter outlines the nature, classification and dimension of economic crimes, cyber crimes, the type of attacks, the modus operandi of the cyber crime, and current status of cyber security, and how do we approach the problem. A brief review of some of the cases of cyber crime has also been analyzed in this chapter.

Introduction:

In today's age of electronic connectivity, there are about 2 billion computers in the world and this number is expected to double in the next three years. More than 300 billion e-mail messages are being exchanged every day which means that more than 3 million e-mails are sent every second. The explosive growth in computer systems and their interconnections via networks and the dependency on computers by organizations and individuals have heightened awareness of the need to protect data. The greatest threat of cyber attacks is being experienced by national critical infrastructures and defense systems, but the commercial domain is also equally impacted by viruses, worms, hackers, electronic eavesdropping, electronic fraud, and so on.

Characteristics of economic crime:

The government is powerless to stop organized 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 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 objectives 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 native and often unaware of the fact that they have been cheated.

Another characteristics 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. Exposures 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 crimes are relatively invisible, compared with violent crime, for example. The effects on society of economic crimes are hidden as public fear and concern are heightened in cases that affect personnel security more directly.

A significant proportion of transnational organized crimes assumed 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 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 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 system.

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. Economic crimes can be classified as follows:

(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;
Money laundering and Hawala through which proceeds of transnational organized crimes are transmitted abroad.

**Corruption:**

Amongst the many critical predicaments that the Indian economy suffers from, corruption has been one of the biggest monsters, and thankfully the most talked about in recent days. Needless to say, corruption has corroded every delivery system and has made it completely dysfunctional. The entire Indian public life is riddled with overriding rates of corruption – from the Adarsh land scam to Commonwealth Games misappropriations to the 2G Spectrum scam – the list here has been endless, and the magnitude, obscene. In fact, India’s public life was never clean – the infamous Bofors scandal, Harshad Mehta’s nexus with senior politicians and Ketan Parekh’s stock market manipulation – all had their own perilous impact on the economy! It requires no empirical study or statistical survey to exhibit that we comfortably are the top performers in all corruption related global indices. Take for instance, Transparency International’s Corruption Perception Index (CPI) where India’s rank has been slipping consistently – languishing at the 95th position now with a score of 3.1 (on a scale of 10), a sizeable 23 rank down from 2007. India is far behind China that stands at 75th position with a score of 3.6. CPI score is not only about corruption but is more about the way corruption has got institutionalized in our system. Also, it is a fact that India’s score could have been better had it not been battered with the monstrous 2G Spectrum scam. Interestingly, all the least corrupt countries like New Zealand, Denmark and Finland with 9.5, 9.4 and 9.4 scores, respectively, are not just socially developed but also economically progressive. And that’s why these are those nations that experience very few cases of crime, corruption and other forms of social malaise—unlike India (Arindam Chaudhuri, 2012).
The thumb-rule that set the pattern is that the developed countries mostly have high CPI scores, whereas at the bottom of the table are the countries mired by civil strife and oppressive regimes; and in-between are the emerging economies as well as former communist blocks. There is also a direct correlation between CPI rankings and Human Development Index (barring some aberration like Greece, which, in spite of being a developed country is ranked below China at number 80; and South Korea, which is ranked 12th in HDI and is 43 in CPI). Most of the African as well as Asian nations have a combination of low CPI and low HDI scores and most of the European and North American countries have the opposite; thus reflecting a direct bearing between the two indices. On hindsight, it may appear that there is no impact of corruption on GDP growth and investments. China and India, both scored quite low on CPI, yet have been riding on decent economic growth and FDI inflow. Vietnam and Indonesia are even lower in ranks in CPI with 2.9 and 3.0, respectively, are recipient of quantum investments with their economy kicking (Arindam Chaudhuri, opp. cit).

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 of the value of 84000 million rupees.

There are two kinds of corruption: Corruption can be defined as
corruption where money has to be paid to acquire services that are legitimately due and honestly entitled. Collusive Corruption implies bribe given or bribe taken to give something that is not legitimately due and here the bribe taker and bribes give, collude to transact a resource, which honest means would not have entitled. Corruption can also be categorized as: Political Corruption and Retail Corruption. Political corruption is corruption by elected representatives. Retail Corruption is corruption by government officials. Often corruption in India is accepted. However there is a cost to corruption. India’s growth rate could be higher by 2 per cent if India’s corruption level is contained.

So, if corruption is not contained India’s GDP could be half in three decades. It is difficult to estimate the quantum of corruption in India. But in a GDP of national economy of Rs. 60 lakh crores, almost 3–5 lakh crores is routed through corruption. Thus, almost 5 per cent of GDP is routed through corruption.

The World Bank estimates that almost 5 per cent of global GDP is lost due to corruption around the world and this may be as high as 25 per cent in some African countries. If these estimates seem a little high, consider this there are 4 million trucks. Each truck has to pay Rs. 200 a day. Thus, almost Rs. 100 crores a day or Rs. 35000 crores a year is routed through corruption only in truck sector. Consider registration of housing, one has to pay amount equal to registration fees for corruption and this may amount to as much as 1 per cent of cost of housing. Thus real estate sector could significantly add to corruption.

Enterprises have to pay some amount, even when paying appropriate legitimate taxes. Thus, even to do legitimate dealing, one has to pay an illegal component. These are examples of retail corruption. But there is considerable, political corruption too. Expenditure on elections is huge. While there is expenditure limit of Rs. 25 lakh on Parliamentary elections and Rs. 10 lakh on Assembly
elections, it is reasonable to estimate that these expenditure limits are exceeded by 10-100 times, depending upon the state and nature of constituency. It is not unreasonable to estimate that almost Rs. 2.5 lakh crores is earned by politicians over 5 year period. That would mean almost Rs. 50,000 crores per annum.

Thus, out of total corruption of Rs. 3 lakh crores, anywhere between Rs. 50,000 crores to Rs. 75,000 crores (including local government corruption) is political corruption and almost 80 per cent of corruption is retail corruption. Thus though political corruption attracts most attention, retail corruption cannot be neglected as it almost forms 70-80 per cent of all corruption. Indeed, while there are mere 5000 politicians there are almost 20 million government employees. Election expenditure, that are in excess of ceiling limit are usually indulged in to buy votes, through enticement. Some people estimate that almost 20-60 per cent of votes are bought by politicians by providing liquor or giving cash of some goods. Most poor class votes or even lower middle class votes are purchased. Voters may even take money from multiple candidates. Since Indian elections operate on principle of first past the post system, every single vote is invaluable. And hence politicians are willing to spend huge amount of money to acquire the marginal vote because it is so valuable.

Indeed the political class presumes, that while spending on elections does not ensure victory, not spending on election almost certainly guarantees loss. Considering the enormous importance of money in elections, political parties are compelled to field candidate with money spending power and hence by definition, politicians, who are more likely than not likely to be corrupt. However, very few, if any people, much less politicians are punished for corruption. Indeed, not a single politician has been jailed for prolonged period of corruption, though it is realistic to presume that a very large percentage of
politicians are corrupt. There is also very scant and not strong enough action against retail corruption. Hence, both retail corruption and political corruption continue to thrive unchecked by law.

Another research and advocacy organization, the Global Financial Integrity (GFI), released a report called ‘The Drivers and Dynamics of Illicit Financial Flows from India: 1948-2008. The report alluded to some jaw dropping facts. As a direct result of black money stashed abroad, India has lost a humungous sum. Tax evasion, bribery and kickbacks, cases of crime and other forms of corruption – all are listed between 1948 and 2008. The 2G Spectrum is a classic case of a royal kickback scam by the politician (A Raja) and it is intriguing how the system managed it to keep it off-the-hook, more so as this was done during the Bofors era. Notwithstanding, in this gigantic corruption saga, the present valuation of this illegal capital flight is more than double the US external debt. Even at the corporate level, the private sector always preferred overseas financial centers – the share of which (in terms of deposits), went up from 36.4 per cent in 1995 to 54.2 per cent in 2009.

Since India was positioned as a nation-state post Independence, corruption developed a strong foothold in Indian politics. Moreover, given the series of scams that have come to limelight in the last one year, it is tempting to assert that Indians are by nature immoral and are liable to be corrupted easily. However, researches have shown that Indians are as prone to become corrupt as their peers in other developing nations of Asia. But one thing that sets Indians apart is their willingness to tolerate such corrupt measures. This is evident from the amount of bribes the common man in India pays for availing of even the basic services in his day to day life. From getting a service in the hospital to lodging an FIR or getting a driving license, every service requires a common man to pay bribe for getting the work done without
much bureaucracy. Almost all the public services like the Public Distribution System (PDS), hospitals, schools, water supply, are corrupt from head to toe. As per the India Corruption Study 2010 by CMS, rural households of 12 surveyed states have paid an amount close to Rs 4700 million as bribes during the last one year (Arindam Chaudhuri, opp.cit).

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.

**Smuggling:**

Smuggling, which consists of clandestine operations leading to unrecorded trade, is one of the major economic offences affecting India. According to property recovery based model developed on the data by National Crime Records Bureau (NCRB) Ministry of Home Affairs, New Delhi, the total amount of recovery from the crime proceeds is Rs 190 crores. In total 70,773 cases were investigated during 2000-2009. Whereas, the total loss to the Indian economy due to the various crimes including commercial fraud, smuggling, drug trafficking, bank frauds, tax evasion and corruption was pegged at Rs 22,528 crores, the study said, citing its second model to ascertain the size of corruption.

The study, based on GDP model, estimated at Rs 1886 thousand crores the quantum of money laundering using corrupt ways, citing international standards. "According to studies conducted by International Monetary Fund, it was estimated that the quantum of
money laundered is approximately 2 to 5 per cent of GDP of the world," the report said. Considering that 5 per cent of the amount equivalent to the size of GDP is laundered, "it is possible to conclude that the size of money laundered is Rs 1886 thousand crores and the corruption in India could be more than Rs 1555 thousand crores."

The assumptions were made taking into account the GDP receipts between 2000 and 2009, the study said. "Other than cooperation from different investigating and enforcement agencies, the Securities and Exchange Board of India, which is the stock market regulator, can play a significant role in preventing the corruption in India".

**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 ramifications 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", 

38
"Invoices', "Letters of Credit", departure schedules of sailing vessels, etc. despite their being public documents. International cooperation is therefore needed to curb this menace.

**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 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 rupee 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.

**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.

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.
Money laundering and Hawala transactions threaten developing economies and contribute to illicit drug trafficking and terrorist and subversive activities. As mentioned earlier, 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 amount 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 remittance 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 199, FERA has been replaced by the Foreign Exchange Maintenance Act. A bill named as 'The Prevention of Money Laundering Bill' has been introduced in the 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.

**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.

Some examples of Cyber Crimes are:

E-mail Spoofing:

A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source e.g., Pooja has an e-mail address pooja@asianlaws.org. Her enemy, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Pooja, her friends could take offence and relationships could be spoiled for life. E-mail spoofing can also cause monetary damage. Misinformation about companies are sent through e-mails and thus large lose will occur to companies in form of money and customers.

Forgery:

Counterfeit currency notes, postage and revenue stamps, mark sheets, etc can be forged using sophisticated computers, printers and scanners.

Unauthorized access to computer systems or networks:

This activity is commonly referred to as hacking. The user hack data and images without proper authorization.

E-mail Bombing:

E-mail bombing refers to sending large number of e-mails to the victim resulting in the victim’s e-mail account (in case of an individual) or mail servers (in case of a company or an e-mail service provider) crashing. Cyber cafes have emerged as hot spots for cyber crimes. Even terrorists prefer the anonymity of a cyber cafe to communicate with each other. The mushrooming of cyber cafe in the city, which provide the secrecy through cabins constructed for users, has also made the porn literature easily accessible to the people visiting them. (Chandigarh Tribune, 28 May, 2001).
Data Diddling:

This kind of attack involves altering raw data just before it is processed by a computer and the changing it back after the processing is completed.

How Cyber Criminals Works:

Cyber crime has become a profession and the demographic of your typical cyber criminal is changing rapidly, from bedroom-bound geek to the type of organized gangster more traditionally associated with drug-trafficking, extortion and money laundering.

It has become possible for people with comparatively low technical skills to steal thousands of pounds a day without leaving their homes. In fact, to make more money than can be made selling heroin (and with far less risk), the only time the criminal need leave his PC is to collect his cash. Sometimes they don't even need to do that.

In all industries, efficient business models depend upon horizontal separation of production processes, professional services, sales channels etc. (each requiring specialized skills and resources), as well as a good deal of trade at prices set by the market forces of supply and demand. Cyber crime is no different: it boasts a buoyant international market for skills, tools and finished product. It even has its own currency.

The rise of cyber crime is inextricably linked to the ubiquity of credit card transactions and online bank accounts. Get hold of this financial data and not only can you steal silently, but also – through a process of virus-driven automation – with ruthlessly efficient and hypothetically infinite frequency. The question of how to obtain credit card/bank account data can be answered by a selection of methods each involving their own relative combinations of risk, expense and skill.

The most straightforward is to buy the ‘finished product’. In this
case we'll use the example of an online bank account. The product takes the form of information necessary to gain authorized control over a bank account with a six-figure balance. The cost to obtain this information is $400 (cyber criminals always deal in dollars). It seems like a small figure, but for the work involved and the risk incurred it's very easy money for the criminal who can provide it. Also remember that this is an international trade; many cyber-criminals of this ilk are from poor countries in Eastern Europe, South America or South-East Asia. The probable marketplace for this transaction will be a hidden IRC (Internet Relay Chat) chat room. The $400 fee will most likely be exchanged in some form of virtual currency such as e-gold.

Not all cyber-criminals operate at the coalface, and certainly don't work exclusively of one another; different protagonists in the crime community perform a range of important, specialized functions. These broadly encompass: Coders – comparative veterans of the hacking community. With a few years' experience at the art and a list of established contacts, ‘coders’ produce ready-to-use tools (i.e. Trojans, mailers, custom bots) or services (such as making a binary code undetectable to AV engines) to the cyber crime labour force – the ‘kids’. Coders can make a few hundred dollars for every criminal activity they engage in.

Kids – so-called because of their tender age: most are under 18. They buy, trade and resell the elementary building blocks of effective cyber-scams such as spam lists, mailers, proxies, credit card numbers, hacked hosts, scam pages etc. ‘Kids’ will make less than $100 a month, largely because of the frequency of being ‘ripped off’ by one another. Drops – the individuals who convert the ‘virtual money’ obtained in cyber crime into real cash. Usually located in countries with lax e-crime laws (Bolivia, Indonesia and Malaysia are currently very popular), they represent ‘safe’ addresses for goods purchased with stolen financial details to be sent, or else ‘safe’ legitimate bank accounts for money to be transferred into
illegally, and paid out of legitimately.

Mobs – professionally operating criminal organizations combining or utilizing all of the functions covered by the above. Organized crime makes particularly good use of safe ‘drops’, as well as recruiting accomplished ‘coders’ onto their payrolls. Gaining control of a bank account is increasingly accomplished through phishing. There are other cyber crime techniques, but space does not allow their full explanation.

All of the following phishing tools can be acquired very cheaply: a scam letter and scam page in your chosen language, a fresh spam list, a selection of php mailers to spam-out 100,000 mails for six hours, a hacked website for hosting the scam page for a few days, and finally a stolen but valid credit card with which to register a domain name. With all this taken care of, the total costs for sending out 100,000 phishing e-mails can be as little as $60. This kind of ‘phishing trip’ will uncover at least 20 bank accounts of varying cash balances, giving a ‘market value’ of $200 – $2,000 in e-gold if the details were simply sold to another cyber criminal. The worst-case scenario is a 300 per cent return on the investment, but it could be ten times that.

Better returns can be accomplished by using ‘drops’ to cash the money. The risks are high, though: drops may take as much as 50 per cent of the value of the account as commission, and instances of ‘ripping off’ or ‘grassing up’ to the police are not uncommon. Cautious phishers often separate themselves from the physical cashing of their spoils via a series of ‘drops’ that do not know one another. However, even taking into account the 50 per cent commission, and a 50 per cent ‘rip-off’ rate, if we assume a single stolen balance of $10,000 – $100,000, then the phisher is still looking at a return of between 40 and 400 times the meager outlay of his/her phishing trip.

In large operations, offshore accounts are invariably used to
accumulate the criminal spoils. This is more complicated and far more expensive, but ultimately safer. The alarming efficiency of cyber crime can be illustrated starkly by comparing it to the illegal narcotics business. One is faster, less detectable, more profitable (generating a return around 400 times higher than the outlay) and primarily non-violent. The other takes months or years to set-up or realizes an investment, is cracked down upon by all almost all governments internationally, fraught with expensive overheads, and extremely dangerous.

Add phishing to the other cyber-criminal activities driven by hacking and virus technologies – such as carding, spy ware planting, online extortion, industrial spying and mobile phone dialers – and you’ll find a healthy community of cottage industries and international organizations working together productively and trading for impressive profits. Of course these people are threatening businesses and individuals with devastating loss, financial hardship and troubling uncertainty – and must be stopped.

On top of viruses, worms, bots and Trojan attacks, organizations in particular are contending with social engineering deception and traffic masquerading as legitimate applications on the network. In a reactive approach to this onslaught, companies have been layering their networks with stand alone firewalls, intrusion prevention devices, anti-virus and anti-spy ware solutions in a desperate attempt to plug holes in the armory. They're beginning to recognize it's a failed strategy. After all, billions of pounds are being spent on security technology, and yet security breaches continue to rise. To fight cyber crime there needs to be a tightening of international digital legislation and of cross-border law enforcement coordination. There is an urgent need for a more creative and inventive responses from such organizations which are under cyber threats. Piecemeal, reactive security solutions are giving way to strategically deployed multi-threat security systems. Instead of having to install, manage and maintain disparate devices, organizations can consolidate their security.
capabilities into a commonly managed appliance. These measures combined, in addition to greater user education are the best safeguard against the deviousness and pure innovation of cyber-criminal activities.

**An Overview of Internet Fraud:**

Internet fraud is committed in several ways. The FBI and police agencies worldwide have people assigned to combat this type of fraud; according to figures from the FBI, U.S. companies' losses due to Internet fraud in 2003 surpassed US$500 million. In some cases, fictitious merchants advertise goods for very low prices and never deliver. However, that type of fraud is minuscule compared to criminals using stolen credit card information to buy goods and services.

The Internet serves as an excellent tool for investors, allowing them to easily and inexpensively research investment opportunities. But the Internet is also an excellent tool for fraudsters.

**Geographic origin and targets:**

In some cases Internet Fraud schemes originate in the US and European countries, but a significant proportion seems to come from Africa, particularly Nigeria and Ghana, and sometimes from Egypt. Some originate in Eastern Europe, Southwest Asia and China. For some reason, many fraudulent orders seem to originate from Belgium, from Amsterdam in the Netherlands, from Norway, and from Malmo in Sweden. Europe, US, and some Asia Pacific countries like Singapore and Australia are the leading targets of this type of fraud.

**Popular products:**

Fraudsters seem to prefer small and valuable products, such as: watches, jewelry, laptops, ink cartridges, digital cameras, and camcorders. These items are usually commodities that are easily sellable and have a broad range of appeal. However, fraud in hosted marketplaces such as E-
bay covers a broad range of products from cellular phones to desktop computers. The craft has continually evolved in sophistication. In some instances, a picture of the product is sent in place of the actual product. Other times, products are outright never sent after the bill is charged to credit card accounts. Victims are left to deal with credit card companies for charge backs. Some fraudsters market intangibles such as software downloads or documentation. Pricing on such items is low in order to encourage a purchase perceived by the consumer as low risk (in accordance with low cost.) Software download scams are frequently targeted at high-population buying communities such as online gaming worlds. Wow stat hack is an example of one such scam.

Identity theft schemes: Stolen credit cards:

Most Internet fraud is done through the use of stolen credit card information which is obtained in many ways, the simplest being copying information from retailers, either online or offline. There have been many cases of crackers obtaining huge quantities of credit card information from companies' databases. There have been cases of employees of companies that deal with millions of customers in which they were selling the credit card information to criminals.

Despite the claims of the credit card industry and various merchants, using credit cards for online purchases can be insecure and carry a certain risk. Even so called "secure transactions" are not fully secure, since the information needs to be decrypted to plain text in order to process it. This is one of the points where credit card information is typically stolen.

Get wire transfer info:

Some fraudsters approach merchants asking them for large quotes. After they quickly accept the merchant's quote, they ask for wire transfer information to send payment. Immediately, they use online check issuing systems as Qchex that require nothing but a working e-mail, to produce
checks that they use to pay other merchants or simply send associates to cash them.

**Purchase scams:**

The most straightforward type of purchase scam is a buyer in another country approaching many merchants through spamming them and directly asking them if they can ship to them using credit cards to pay. An example of such e-mail is as follows:

From: XXX XXX [xxxxx@hotmail.com] Sent: Saturday, October 01, 2005 11:35 AM Subject: International order enquiry

Good day Sales. This is XXX XXX and I will like to place an order for some products in your store, but before I proceed with listing my requirements, I will like to know if you accept credit card and can ship internationally to Lagos, Nigeria. Could you get back to me with your website so as to forward you the list of my requirements as soon as possible. Regards, XXX XXX, XXXX Inc. 9999 XXX Street, Mushin, Lagos 23401, Nigeria Telephone: 234-1-99999999, Fax: 234-1-99999999, E-mail: xxxxx@hotmail.com

Most likely, a few weeks or months after the merchant ships and charges the Nigerian credit card, he/she will be hit with a chargeback from the credit card processor and lose all the money.

**Counterfeit Postal Money Orders:**

According to the FBI and postal inspectors, there has been a significant surge in the use of Counterfeit Postal Money Orders since October 2004. More than 3,700 counterfeit postal money orders (CPMOs) were intercepted by authorities from October to December of 2004, and according to the USPS, the "quality" of the counterfeits is so good that ordinary consumers can easily be fooled.

On March 9, 2005, the FDIC issued an alert [1] stating that it had
learned that counterfeit U.S. Postal Money Orders had been presented for payment at financial institutions. On April 26, 2005, Tom Zeller Jr. wrote an article in The New York Times [2] regarding a surge in the quantity and quality of the forging of U.S. Postal Money Orders, and its use to commit online fraud. The article shows a picture of a man that had been corresponding with a woman in Nigeria through a dating site, and received several fake postal money orders after the woman asked him to buy a computer and mail it to her.

Counterfeit Postal Money Orders (CPMOs) are usually received by Small Internet retailers, classified advertisers, individuals who have been contacted through e-mail or chat rooms by fraudsters posing as prospective social interests or business partners, and convinced to help the fraudsters unknowingly. Geographical origin of such frauds are mostly from Nigeria, Ghana and Eastern Europe. The penalty for making or using counterfeit postal money orders is up to ten years in jail and a US$25,000 fine.

**Online automotive fraud:**

There are two basic schemes in online automotive fraud:

A fraudster posts a vehicle for sale on an online site, generally for luxury or sports cars advertised for thousands less than market value. The details of the vehicle, including photos and description, are typically lifted from sites such as eBay Motors and re-posted elsewhere. An interested buyer, hopeful for a bargain, e-mails the seller, who responds saying the car is still available but is located overseas. He then instructs the buyer to send a deposit via wire transfer to initiate the "shipping" process. The unwitting buyer wires the funds, and doesn't discover until days or weeks later that they were scammed. A fraudster feigns interest in an actual vehicle for sale on the Internet. The "buyer" explains that a client of his is interested in the car, but due to an earlier sale that fell through has a certified check for thousands more than the asking price and requests the seller to send the
balance via wire transfer. If the seller agrees to the transaction, the buyer sends the certified check via express courier (typically from Nigeria). The seller takes the check to their bank, which makes the funds available immediately. Thinking the bank has cleared the check, the seller follows through on the transaction by wiring the balance to the buyer. Days later, the check bounces and the seller realizes they have been scammed. But the money has long since been picked up and is not recoverable.

In another type of fraud, a fraudster contacts the seller of an automobile, asking for the vehicle identification number, putatively to check the accident record of the vehicle. However, the supposed buyer actually uses the VIN to make fake papers for a stolen car that is then sold.

**Cash the check system:**

In some cases, fraudsters approach merchants and ask for large orders: $50,000 to $200,000, and agree to pay via wire transfer in advance. After brief negotiation, the buyers give an excuse about the impossibility of sending a bank wire transfer. The buyer then offers to send a check, stating that the merchant can wait for the check to clear before shipping any goods. The check received, however, is a counterfeit of a check from a medium to large U.S company. If asked, the buyer will claim that the check is money owed from the large company. The merchant deposits the check and it clears, so the goods are sent. Only later, when the larger company notices the check, will the merchant's account be debited.

In some cases, the fraudsters agree to the wire but ask the merchant for their bank's address. The fraudsters send the counterfeited check directly to the merchant's bank with a note asking to deposit it to the merchant's account. Unsuspecting bank officers deposit the check, and then the fraudster contacts the merchant stating that they made a direct deposit into the merchant's account.
Re-shippers:

Re-shipping scam trick individuals or small businesses into shipping goods to countries with weak legal systems. The goods are generally paid for with stolen or fake credit cards.

Nigerian version:

In the Nigerian version, the fraudsters have armies of people actively recruiting single women from western countries through chat & matchmaking sites. At some point, the criminal promises to marry the lady and come to their home country in the near future. Using some excuse the criminal asks permission of his "future wife" to ship some goods he is going to buy before he comes. As soon as the woman accepts the fraudster uses several credit cards to buy at different Internet sites simultaneously. In many cases the correct billing address of the cardholder is used, but the shipping address is the home of the unsuspecting "future wife". Around the time when the packages arrive, the criminal invents an excuse for not coming and tells his "bride" that he urgently needs to pick up most or all the packages. Since the woman has not spent any money, she sees nothing wrong and agrees. Soon after, she receives a package delivery company package with pre-printed labels that she has agreed to apply to the boxes that she already has at home. The next day, all boxes are picked up by the package delivery company and shipped to the criminal's real address (in Nigeria or elsewhere). After that day the unsuspecting victim stops receiving communications from the "future husband" because her usefulness is over. To make matters worse, in most cases the criminals were able to create accounts with the package deliverer, based on the woman's name and address. So, a week or two later, the woman receives a huge freight bill from the shipping company which she is supposed to pay because the goods were shipped from her home. Unwittingly, the woman became the criminal re-shipper and helped him with his criminal actions.
East European version:

This is a variant of the Nigerian Version, in which criminals recruit people through classified advertising. The criminals present themselves as a growing European company trying to establish a presence in the U.S. and agree to pay whatever the job applicant is looking to make, and more. The fraudsters explain to the unsuspecting victim that they will buy certain goods in the U.S. which need to be re-shipped to a final destination in Europe. When everything is agreed they start shipping goods to the re-shipper's house. The rest is similar to the Nigerian Version. Sometimes, when the criminals send the labels to be applied to the boxes, they also include a fake cheque, as payment for the re-shipper's services. By the time the cheque bounces unpaid, the boxes have been picked up already and all communication between fraudster and re-shipper has stopped.

Chinese version:

This is a variant of the East European Version, in which criminals recruit people through spam. The criminals present themselves as a growing Chinese company trying to establish a presence in the U.S. or Europe and agree to pay an agent whatever the unsuspecting victim is looking to make, and more. Here is an example of a recruiting e-mail:

Dear Sir/Madam, I am Mr. XXX XXX, managing XXXXXX Corp. We are a company who deal on mechanical equipment, hardware and minerals, electrical products, Medical & Chemicals, light industrial products and office equipment, and export into the Canada/America and Europe. We are searching for representatives who can help us establish a medium of getting to our customers in the Canada/ America and Europe as well as making payments through you to us. Please if you are interested in transacting business with us we will be glad. Please contact us for more information. Subject to your satisfaction you will be given the opportunity to negotiate your mode of which we will pay for your services as our
representative in Canada/America and Europe. Please if you are interested forward to us your phone number/fax and your full contact addresses. Thanks in advance. Mr. XXX XXX. Managing Director"

Call tag scam:

The Merchant Risk Council reported that the "call tag" scam re-emerged over the 2005 holidays and several large merchants suffered losses. Under the scheme, criminals use stolen credit card information to purchase goods online for shipment to the legitimate cardholder. When the item is shipped and the criminal receives tracking information via e-mail, he/she calls the cardholder and falsely identifies himself as the merchant that shipped the goods, saying that the product was mistakenly shipped and asking permission to pick it up upon receipt. The criminal then arranges the pickup issuing a "call tag" with a shipping company different from the one the original merchant used. The cardholder normally doesn't notice that there is a second shipping company picking up the product, which in turn has no knowledge it is participating in a fraud scheme. The cardholder then notices a charge in his card and generates a chargeback to the unsuspecting merchant.

Business opportunity/"Work-at-Home" schemes:

Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in "work-at-home" ventures. These schemes typically require the individuals to pay anywhere from $35 to several hundred dollars or more, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.

Often, after paying a registration fee, the applicant will be sent advice on how to place ads similar to the one that recruited him in order to recruit others, which is effectively a pyramid scheme.

Other types of work at home scams include home assembly kits. The
applicant pays a fee for the kit, but after assembling and returning the item, it’s rejected as sub-standard, meaning the applicant is out of pocket for the materials. Similar scams include home-working directories, medical billing, data entry (data entry scam) at home or reading books for money.

**Website scams Click fraud:**

The latest scam to hit the headlines is the multi-million dollar Click fraud which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via spyware, the affiliate is then paid a commission on the cost-per-click that was artificially generated. Affiliate programs such as Google's Ad sense capability pay high commissions that drive the generation of bogus clicks. With paid clicks costing as much as US$100 [verification needed] and an online advertising industry worth more than US$10 billion, this form of Internet fraud is on the increase.

**International modem dialing:**

Many consumers connect to the Internet using a modem calling a local telephone number. Some web sites, normally containing adult content, use international dialing to trick consumers into paying to view content on their web site. Often these sites purport to be free and advertise that no credit card is needed. They then prompt the user to download a "viewer" or "dialer" to allow them to view the content. Once the program is downloaded it disconnects the computer from the Internet and proceeds to dial an international long distance or premium rate number, charging anything up to US$7-8 per minute. An international block is recommended to prevent this, but in the U.S. and Canada, calls to the Caribbean (except Haiti) can be dialed with a "1" and a three-digit area code, so such numbers, as well as "10-10 dial-round" phone company prefixes, can circumvent an international block.

**Another type of Click Fraud:**

This type of fraud involves a supposed internet marketing specialist
presenting a prospective client with detailed graphs and charts that indicate that his web site receives (x) thousands of hits per month, emphasizing that if you pay for his services you will succeed in getting a number clicks converted to customers or clients.

When you receive no request for more information and no clients, the fraudster responds that it must be something you web site is not doing right.

Phishing:

"Phishing" is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an e-mail, or an instant message). It is a form of social engineering attack. The term was coined in the mid 1990s by crackers attempting to steal AOL accounts. An attacker would pose as an AOL staff member and send an instant message to a potential victim. The message would ask the victim to reveal his or her password, for instance to "verify your account" or to "confirm billing information". Once the victim gave over the password, the attacker could access the victim's account and use it for criminal purposes, such as spamming. Phishing attacks were more popular among Indian users due to rising Internet penetration and growing online transactions. India has now joined the dubious list of the world's top 15 countries hosting "phishing" sites which aims at stealing confidential information such as passwords and credit card details [The Hindu, Sunday Nov 26, 2006]. Phishing has been widely used by fraudsters using spam messages masquerading as large banks (Citibank, Bank of America) or Pay Pal. These fraudsters can copy the code and graphics from legitimate websites and use them on their own sites to create legitimate-looking scam web pages. They can also link to the graphics on the legitimate sites to use on their own scam site. These pages are so well done that most people cannot tell that they have navigated to a
scam site. Fraudsters will also put the text of a link to a legitimate site in an e-mail but use the source code to links to own fake site. This can be revealed by using the "view source" feature in the e-mail application to look at the destination of the link or putting the cursor over the link and looking at the code in the status bar of the browser. Although many people don't fall for it, the small percentage of people that do fall for it, multiplied by the sheer numbers of spam messages sent, presents the fraudster with a substantial incentive to keep doing it.

Anti-phishing technologies are now available.

**Pharming:**

Pharming is the exploitation of vulnerability in the DNS server software that allows a hacker to acquire the domain name for a site, and to redirect that website's traffic to another web site. DNS servers are the machines responsible for resolving internet names into their real addresses - the "signposts" of the internet.

If the web site receiving the traffic is a fake web site, such as a copy of a bank's website, it can be used to "phish" or steal a computer user's passwords, PIN or account number. Note that this is only possible when the original site was not SSL protected, or when the user is ignoring warnings about invalid server certificates.

For example, in January 2005, the domain name for a large New York ISP, Panix, was hijacked to a site in Australia. In 2004 a German teenager hijacked the eBay de domain name.

Secure e-mail provider Hush mail was also caught by this attack on 24th of April 2005 when the attacker rang up the domain registrar and gained enough information to redirect users to a defaced webpage. Anti-pharming technologies are now available.
Auction and retail schemes online:

Fraudsters launch auctions on eBay or Trade Me with very low prices and no reservations especially for high priced items like watches, computers or high value collectibles. They received payment but never deliver, or deliver an item that is less valuable than the one offered, such as counterfeit, refurbished or used. Some fraudsters also create complete web stores that appear to be legitimate, but they never deliver the goods. An example of such a fraudulent site is marselect.com. They take payment but never shipped the order. In some cases, some stores or auctioneers are legitimate but eventually they stopped shipping after cashing the customers' payments.

Sometimes fraudsters will combine phishing to hijacking legitimate member accounts on eBay, typically with very high numbers of positive feedback, and then set up a phony online store. They received payment usually via check, money-order, cash or wire transfer but never deliver the goods; and then they leave the poor, unknowing eBay member to sort out the mess. In this case the fraudster collects the money while ruining the reputation of the conned eBay member and leaving a large number of people without the goods they thought they purchased.

Stock market manipulation schemes:

These are also called investment schemes online. Criminals use these to try to manipulate securities prices on the market, for their personal profit. According to enforcement officials of the Securities and Exchange Commission, the 2 main methods used by these criminals are:

Pump-and-dump schemes:

False and/or fraudulent information is disseminated in chat rooms, forums, internet boards and via e-mail (spamming), with the purpose of causing a dramatic price increase in thinly traded stocks or stocks of shell
companies (the "pump"). As soon as the price reaches a certain level, criminals immediately sell off their holdings of those stocks (the "dump"), realizing substantial profits before the stock price falls back to its usual low level. Any buyers of the stock who are unaware of the fraud become victims once the price falls. When they realize the fraud, it is too late to sell. They lost a high percentage of their money. Even if the stock value does increase, the stocks may be hard to sell because of lack of interested buyers, leaving the shareholder with the shares for a far longer term than desired.

**Short-selling or "scalping" schemes:**

This scheme takes a similar approach to the "pump-and-dump" scheme, by disseminating false or fraudulent information through chat rooms, forums, internet boards and via e-mail (spamming), but this time with the purpose of causing dramatic price decreases in a specific company's stock. Once the stock reaches a certain low level, criminals buy the stock or options on the stock, and then reverse the false information or just wait for it to wear off with time or to be disproved by the company or the media. Once the stock goes back to its normal level, the criminal sells the stock or option and reaps the huge gain.

**Avoiding Internet investment scams:**

The US Security Exchange Commission has enumerated guideline on how to avoid internet investment scams. The summary is as follows:

The Internet allows individuals or companies to communicate with a large audience without spending a lot of time, effort, or money. Anyone can reach tens of thousands of people by building an Internet web site, posting a message on an online bulletin board, entering a discussion in a live "chat" room, or sending mass e-mails. If you want to invest wisely and steer clear of frauds, you must get the facts. The types of investment fraud are usually found online mirror the frauds perpetrated over the phone or through the
mail. Consider all offers with skepticism.

**E-mail Account Hacking**

E-mails are increasingly being used for social interaction, business communication and online transactions. Most e-mail account holders do not take basic precautions to protect their e-mail account passwords. Cases of theft of e-mail passwords and subsequent misuse of e-mail accounts are becoming very common.

**The scenarios**

1. The victim's e-mail account password is stolen and the account is then misused for sending out malicious code (virus, worm, Trojan etc) to people in the victim's address book. The recipients of these viruses believe that the e-mail is coming from a known person and run the attachments. This infects their computers with the malicious code.

2. The victim's e-mail account password is stolen and the hacker tries to extort money from the victim. The victim is threatened that if he does not pay the money, the information contained in the e-mails will be misused.

3. The victim's e-mail account password is stolen and obscene e-mails are sent to people in the victim's address book.

**The law: Who is liable?**

**Scenario 1:** Persons who have stolen the e-mail account password and who are misusing the e-mail account.

**Scenario 2:** Persons who have stolen the e-mail account password and who are threatening to misuse it.

**Scenario 3:** Persons who have stolen the e-mail account password and who are misusing the e-mail account.
Modus Operandi:

- The suspect would install key loggers in public computers (such as cyber cafes, airport lounges etc) or the computers of the victim.
- Unsuspecting victims would login to their e-mail accounts using these infected computers.
- The passwords of the victim’s e-mail accounts would be e-mailed to the suspect.

Credit Card Fraud:

Credit cards are commonly being used for online booking of airline and railway tickets and for other ecommerce transactions. Although most of ecommerce websites have implemented strong security measures (such as SSL, secure web servers etc), instances of credit card frauds are increasing.

Modus Operandi

Scenario 1: The suspect would install key loggers in public computers (such as cyber cafes, airport lounges etc or the computers of the victim. Unsuspecting victims would use these infected computers to make online transactions. The credit card information of the victim would be e-mailed to the suspect.

Scenario 2: Petrol pump attendants, workers at retail outlets, hotel waiters etc note down information of the credit cards used for making payment at these establishments. This information is sold to criminal gangs that misuse it for online frauds.

Cyber Squatting:

Cyber squatting is the act of registering a famous domain name and then selling it for a fortune. This is an issue that has not been tackled in IT act 2000.
Bot Networks:

A cyber crime called 'Bot Networks', wherein spamsters and other perpetrators of cyber crimes remotely take control of computers without the users realizing it, is increasing at an alarming rate. Computers get linked to Bot Networks when users unknowingly download malicious codes such as Trojan horse sent as e-mail attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them get activated, and those who are behind the Bot Networks attacks get the computing powers of thousands of systems at their disposal. Attackers often coordinate large groups of Bot-controlled systems, or Bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks. Trojan horse provides a backdoor to the computers acquired. A 'backdoor' is a method of bypassing normal authentication, or of securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed program, or could be a modification to a legitimate program. Bot networks create unique problems for organizations because they can be remotely upgraded with new exploits very quickly and this could help attackers pre-empt security efforts.

Vulnerability

The Open-Source Vulnerability Database (OSVDB) project maintains a master list of computer - security vulnerabilities, freely available for use by security professionals and projects around the world. Vulnerability information is critical for the protection of information systems everywhere: in enterprises and other organizations, on private networks and intranets, and on the public Internet. Given the fact that nearly $120 million worth of mobiles are being lost or stolen in the country every year, the users have to protect information, contact details and telephone numbers as these could be misused. Nearly 69 per cent of
information theft is carried out by current and ex-employees and 31 per cent by hackers. India has to go a long way in protecting the vital information [The Hindu, Saturday, Oct 27, 2007].

Symantec shares the numbers from its first systematic survey carried out on the Indian Net Security scene: The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate e-mail traffic. India's home PC owners are the most targeted sector of its 37.7 million Internet users: Over 86 per cent of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability.

Some incidents of cyber terrorism

The following are notable examples of cyber terrorism:

In 1998, ethnic Tamil guerrillas swamped Sri Lankan embassies with 800 e-mails a day over a two-week period. The messages read "We are the Internet Black Tigers and we're doing this to disrupt your communications." Intelligence authorities characterized it as the first known attack by terrorists against a country's computer systems.

During the Kosovo conflict in 1999, NATO computers were blasted with e-mail bombs and hit with denial-of-service attacks by hacktivists protesting the NATO bombings. In addition, businesses, public organizations, and academic institutes received highly politicized virus-laden e-mails from a range of Eastern European countries, according to reports. Web defacements were also common.

Since December 1997, the Electronic Disturbance Theater (EDT) has been conducting Web sit-ins against various sites in support of the Mexican Zapatistas. At a designated time, thousands of protestors point their browsers to a target site using software that floods the target with rapid and repeated download requests. EDT's software has also been used by animal rights groups against organizations said to abuse animals.
Electrohippies, another group of hacktivists, conducted Web sit-ins against the WTO when they met in Seattle in late 1999.

Does cyber terrorism extend to the use of computers and the Internet by “conventional” terrorists?

This is a complex question and must be answered with care. The uses of encryption, secure e-mail services etc by “conventional” terrorists does not fit into the definition of cyber terrorism offered above.

An illustration: A terrorist organization, spanning 6 countries assassinates the leader of a religious group. During the planning and execution of this assassination, 512 bit encryption and steganography was used to convey essential information to the members of the organization. This should not be referred to as an incident simply because computers and the Internet were used as tools incidental to the commission of the terrorist act. Let us extend this illustration a little further. Suppose that the assassination caused widespread rioting in some country. As a result of the rioting the premises of some Internet Service Providers were damaged and Internet access to millions of people was cut off. This would still not make the act an act of cyber terrorism. Here although cyber space activities have been disrupted, this disruption is merely a consequence of a conventional terrorist activity. Including the use of computers and the Internet by terrorists within the ambit of cyber terrorism is highly undesirable. Then the use of telephones by terrorists would give rise to “telephone terrorism”, and the list would be endless.

Denial of service attacks, hate websites and hate e-mails, attacks on sensitive computer networks are all rapidly gaining momentum. To tackle this global phenomenon of the abuse and misuse of computers and the Internet, an international convention, backed by national legislations, is needed. The UK Terrorism Act 2000 is a step in the right direction although the Act includes cyber terrorism within the ambit of conventional terrorism.
This is not the desired approach as it is essential that cyber terrorism be addressed as a separate issue and not as a part of conventional terrorism. In addition, it is prudent to distinguish between cyber crime, a domestic issue that may have international ramifications and cyber terrorism, an international issue that may have domestic ramifications.

Deepa Mehta, Inspector General of Police, Chief Vigilance Officer, Delhi Metro Rail Corporation, India, Resource material series no 66. 126th International senior seminar visiting expert’s paper, “Economic crime in a globalizing society: its impact on the sound development of the state - an Indian perspective”

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.

Hacking:

Extensive computerization has resulted in business organizations storing all their information in electronic form. Rival organizations employ hackers to steal industrial secrets and other information that could be beneficial to them. The temptation to use professional hackers for industrial espionage also stems from the fact that physical presence required to gain access to important documents is rendered needless if hacking can retrieve those.

A case of suspected hacking of certain web portals and obtaining the residential addresses from the e-mail accounts of city residents had recently come to light. After getting the addresses, letters were sent through post mail and the recipients were lured in to participating in an international lottery that had Australian $ 23 lakhs at stake.

Computer hackers have also got into the Bhaba Atomic Research Centre (BARC) computer and pulled out important data. Some computer professionals who prepared the software for MBBS examination altered the data and gave an upward revision to some students in return for a hefty payment. A key finding of the Economic Crime Survey 2006 of Price water house Coopers (PwC) was that a typical perpetrator of economic crime in India was male (almost 100 per cent), a graduate or undergraduate and 31-50 years of age.

The Central Bureau of Investigation (CBI) and the Mumbai police have recommended issuance of licenses to cyber cafe owners. Many countries, including India, have established Computer Emergency Response Teams (CERTs) with an objective to coordinate and respond during major security incidents/events. These organizations identify and address existing and potential threats and vulnerabilities in the system and coordinate with stakeholders to address these threats. Policy initiatives on
cyber crime are as yet lethargic because of a general sense that it is nothing more than juvenile hackers out to have fun or impress someone. Prateek Bhargava, cyber law expert says. "There is huge potential for damage to national security through cyber attacks. The internet is a means for money laundering and funding terrorist attacks in an organized manner. In the words of Pawan Duggal, Supreme Court Lawyer, "Cyber crime is omnipresent and although cyber crime cells have been set up in major cities, most cases remain unreported due to lack of awareness."

Cyber Space Security Management has already become an important component of National Security Management, Military-related Scientific Security Management and Intelligence Management all over the world. Future intrusions threatening our national security may not necessarily come from across the land frontier, or in air space or across maritime waters, but happen in cyber space. Intelligence operations and covert actions will increasingly become cyber-based. It is important that our intelligence agencies gear themselves up to this new threat. It is, therefore, necessary to put in place a 'National Cyber Space Security Management Policy' to define the tasks, specify responsibilities of individual agencies with an integrated architecture. The degree of our preparedness in the face of all these potential threats, does leaves much to be desired. The Government should also take note of this slow but worrying development and put in place a proper mechanism to curb the misuse. It is a well-known fact that terrorists have been using the Internet to communicate, extort, intimidate, raise funds and coordinate operations. Hostile states have highly developed capabilities to wage cyber wars. They have the capability to paralyze large parts of communication networks, cause financial meltdown and unrest.

Today's Hackers – Tomorrows Security Analysts

Frank William Abagnale, Jr. is a former check con artist, forger and
Imposter who, for five years in the 1960s, passed bad checks worth more than $2.5 million in 26 countries. During this time, he used eight aliases—even more to cash bad checks. Currently he runs Abagnale and Associates, a financial fraud consultancy company. His life story provided the inspiration for the feature film Catch Me If You Can.

An Indian teenage hacking expert who has helped global think-tanks and police officials combat computer attackers and digital swindlers is spurning job offers to pursue a degree at the prestigious Stanford University. Ankit Fadia, 18 has crisscrossed India, giving lectures to police departments, software companies, educational institutions and government agencies on how to fight "cyber criminals" and deal with computer viruses.

Fadia, developed his computer skills after spending long hours on the Internet, breaking into Web sites as an "ethical hacker" and then informing companies about their sites' vulnerability. Also, he wants to start his own computer security firm.

There are certain hackers whose job is to intrude into a software system by evading or disabling security measures and checks how vulnerable the system is to the bad hackers. Ethical computer hacking has come of age in order to stop or pre-empt intruders from messing around with a computer programme. “Financial transactions are the mainstay of banking operations. Banks and other such institutions need to be extra careful of the bad hackers. Ethical hackers do what a hacker does but only to identify the loopholes in software programmes.

**Cyber Ethics:**

Ethics and morality in different circumstances connotes varied and complex meanings. Each and everything which is opposed to public policy, against public welfare and which may disturb public tranquility may be termed to be immoral and unethical.

In the past terms such as imperialism, colonialism, apartheid, which
were burning issues have given way to cyber crime, hacking, 'cyber-ethics' etc. Today in the present era there is a need to evolve a 'cyber-jurisprudence' based on which 'cyber-ethics' can be evaluated and criticized. Further there is a dire need for evolving a code of Ethics on the Cyber-Space and discipline.

**Cyber Crimes and General Principles:**

As the new millennium dawned, the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with the criminal element. According to Donn Parker, “For the first time in human history, computers and automated processes make it possible to possess, not just commit, a crime. Today, criminals can pass a complete crime in software from one to another, each improving or adapting it to his or her own needs.” The majority of what are termed “cyber-crimes” is really violations of longstanding criminal law, perpetrated through the use of computers or information networks. The problems of crime using computers will rarely require the creation of new substantive criminal law; rather, they suggest need for better and more effective means of international cooperation to enforce existing laws. On the other hand, there are new and serious problems posed by attacks against computers and information systems, such as malicious hacking, dissemination of viruses, and denial-of-service attacks. Such attacks should be effectively prohibited, wherever they may originate. At the same time, it is to be remembered that often the most effective way to counter such attacks is to quickly deploy technical countermeasures; therefore, to the extent that well-meaning but overbroad criminal regulations diminish the technical edge of legitimate information security research and engineering, they could have the
unintended consequence of actually undermining information security.

Criminal Law – General Principles:

According to criminal law, certain persons are excluded from criminal liability for their actions, if at the relevant time; they had not reached an age of criminal responsibility. After reaching the initial age, there may be levels of responsibility dictated by age and the type of offense allegedly committed.

Governments enact laws to label certain types of activity as wrongful or illegal. Behavior of a more antisocial nature can be stigmatized in a more positive way to show society's disapproval through the use of the word criminal. In this context, laws tend to use the phrase, "age of criminal responsibility" in two different ways:

1. As a definition of the process for dealing with alleged offenders, the range of ages specifies the exemption of a child from the adult system of prosecution and punishment. Most states develop special juvenile justice systems in parallel to the adult criminal justice system. Children are diverted into this system when they have committed what would have been an offense in an adult.

2. As the physical capacity of a child to commit a crime. Hence, children are deemed incapable of committing some sexual or other acts requiring abilities of a more mature quality. The age of majority is the threshold of adulthood as it is conceptualized in law. It is the chronological moment when children legally assume majority control over their persons and their actions and decisions, thereby terminating the legal control and legal responsibilities of their parents over and for them. But in the cyber world it is not possible to follow these traditional principles of criminal law to fix liability. Statistics reveal that in the cyber world, most of the offenders are those who are under the age of majority. Therefore, some other mechanism has to be evolved to deal with cyber criminals.
Conclusion

It is apparent from the above analysis that 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 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 states 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 can manipulate computer terminal 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 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.

The Information Technology Act 2000 was passed when the country experienced problems of growing cyber crimes. Since the Internet is the medium for huge information and a large base of communications around the world, it is necessary to take certain precautions while operating it. Therefore, in order to prevent cyber crime it is important to educate everyone and practice safe computing.

In the cyberspace, following traditional principles of criminal law to fix liability is not possible. Since most of the cyber criminals are those who are under the age of majority, some other legal framework has to be evolved to deal with them. Since cyber world has no boundaries, it is a Herculean task to frame laws to cover each and every aspect. But, however a balance has to be maintained and laws be evolved so as to keep a check on cyber crimes.