بسم الله الرحمن الرحيم

IN THE NAME OF ALLAH THE MOST BENEFICENT AND MERCIFUL

An Analysis of Digital / Electronic Fraud & Computer Forensic Issues Concerning Corporate Crime Investigation in Pakistan.

Supervisor : Muhammad Usman Mirza Ex-Judge Adv.
High Court

Submitted by : **Khalid Mehmood Qureshi**
House # 54, Lane # 11,
Askari-VII, Adyala Road,

1-Computer crimes - Investigation - Pakistan
2- Internet fraud

International Islamic University Islamabad
Faculty of Shariah & Law

*****

Approval Sheet

This is to certify that we evaluated the thesis entitled "An Analysis of Digital / Electronic Fraud and Computer Forensic Issues Concerning Corporate Crime Investigation in Pakistan" submitted by Mr. Khalid Mahmood Qureshi, Reg. no. 30-FSL/LLMCL/F04 in partial fulfillment of the award of the degree of LLM Corporate Law. The thesis fulfills the requirements in its core and quality for the award of the degree.

Muhammad Usman Mirza, Supervisor
Ex-Judge / Advocate High Court

Mr. Ataullah Khan Mehmood, Internal Examiner
Assistant Professor, Department of Law

Sahibzada Uzair Hashim, External Examiner
Advocate High Court

DEDICATION

۞ وَمَا مِن دَآبَّةٍ فِى ٱلْأَرْضِ إِلَّا عَلَى ٱللَّهِ
رِزْقُهَا وَيَعْلَمُ مُسْتَقَرَّهَا وَمُسْتَوْدَعَهَا ۚ كُلٌّ فِى كِتَـٰبٍ مُّبِينٍ ﴿٦﴾

"And there is none moving on this earth, the provision of that is not upon the generous responsibility and He knows its place of stay and the place of return. All is recorded in a clear explanatory Book."

This research effort is a compliment to the super most computer in the master plan (Loh-e-Mahfooz) of this entire universe recorded.

An effort to understand the delicacies and intricacies of intellectual system in which man's sixth sense has always been hacking.

ACKNOWLEDGEMENT

All goes to ALLAH – the most Beneficent & Merciful who gave the courage to lay hand in this research work.

The task of accomplishment of this thesis could not have been materialized without the help of a number of individuals and organizations and it would be ingratitude not acknowledge their services.

First of all I am highly indebted to my supervisor Muhammad Usman Mirza, Former Judge, Special Prosecutor NAB Rawalpindi, who put his recommending note on the proposal of this research thesis, resulting which the University approved the same and I embarked upon this task. His encouragement and guidance remained with me throughout the process.

Then thank goes to the concerned law enforcing agency i.e FIA (NR3C, especially to Mr. Irfan Qureshi, Forensic Expert FIA) which gave me know how about the task undertaken by them in that regard. I am also grateful to the authors of the books Mr. Albert J. Marcella, Jr. Doug Menendez and John R.Vacca and authors of different articles namely Mervat Tallawy Executive Secretary of ESCWA, Dr. Mohammed Zaheeruddin, Associate Professor, College of Law, UAE University, Justine Heazlewood Acting Director and Keeper of Public Records, Public Record Office Victoria. Their works have helped me a great deal to understand and analyze the cyber crime problem in its true prospective and to assess its dimensions which lead me to finally draw logical conclusions.

I am especially thankful to my venerable teacher Professor Ahmed Rafique Akhtar, Director CPTU/DIG Mahmoud Alam Mahsud and friends DSP Ilyas Khan, Sh. Azfar Ameen Advocate & his associates, Inam-ur-Rahman Khan Bangash, Shabbir Hussain Advocate, Qasim Mughal who extended their cooperation in collecting relevant material from different books, articles and web sites. I must also acknowledge the help of my ex-students ASI Nasir Abbasi, ASI Muhammad Zubair and Hafiz Sajid Mahmood who did typing work for this thesis.

I also wish to express my thanks to my friend Haji Muhammad Amir and associates namely Imran Usman, Daud Rajput, Nasir Mushtaq who not only provided space in their office but also served with splendid hospitality during the completion period of research work.

Moreover, I am thankful to Prof. Majid Rasheed and Muhammad Abdul Jabbar Khan Niazi who did proof reading of the manuscript and gave final touches to the work.

In the end, I am highly thankful to my family that allowed my time of their share to complete this job especially the weekends on which I had to go to my village.

INDEX

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER – 1

1.1 INTRODUCTION

Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In this age, when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, Cyber crime has assumed rather sinister implications.

During the last decade the Internet has achieved considerable expansion. Today it is estimated that here are over 9.4 million computers and as many as 40 million people world – wide linked with the Internet. It is very much predictable that by the end of this century there could be over 200 million Internet users.

In October 1992, the Association International de Drop it Penal (AIDP) held the colloquium on computer crimes and other crimes against information technology in Wartburg, Germany. The AIDP released its report on computer crime at the conference which was based on other reports received from its member countries. The report stated that less than five percent of computer crime was being reported to law enforcement authorities.

There are several reasons that computer crime statistics do not reflect the true scope of computer crime. Criminologists use the term "dark Figure:" to refer to undiscovered computer crimes. Several factors contribute to this dark figure. First, the operational speed and storage capacity of computer hardware makes criminal activity very difficult to detect. Second, law enforcement officials often lack the necessary technical expertise to deal with criminal activity in the data processing environment. Third, many victims of computer crime have failed to create contingency plans to deal with computer criminals. Fourth, once criminal activity had been detected many business entities have been reluctant to report it because of fear of adverse publicity, loss of good will, embarrassment, loss of public confidence, investment loss and economic repercussions.

Due to heavy use of digital environment by the masses and organizations in their routine business and commitments and continuing interruption by the unauthorized buzzers in the smooth working of the internet or intranet communications emerges out with the necessity of legislation for the users of networks and thus the concept of cyber law was introduced.

1.2. CYBER CRIME DEFINITION:

Cyber-crime, computer crime, e-crime, hi-tech crime or electronic crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime.

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access (unauthorized access), illegal interception (by technical means of non-public transmissions of computer data to, from or within a computer system), data interference (unauthorized damaging, deletion, deterioration, alteration or suppression of computer data), systems interference (interfering with the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data), misuse of devices, forgery (ID theft), and electronic fraud.[1]

[1] ^ Paul Taylor (1999)

With the potential growth of internet connections the opportunities for the exploitation of any weakness in information security and multiplying has increased. Cyber crime may be internal or external with the former easier to perpetrate.

Cyber crimes have no virtual boundaries and may affect every country in the world. It may be defined as any crime with the help of computer and telecommunication technology, with the purpose of influencing the functioning of computer or the computer system.

Cyber crimes are a very serious threat for the times to come and pose one of the most difficult challenges to the law encroachment machinery. Mostly cyber crimes do not involve violence but rather greed, pride or play on some character weakness of the victims. It is difficult to identify the culprit, as the net can be a vicious web of deceit and can be accessed from any part of the globe. For these reasons, cyber crimes are considered as white collar crimes.

A general definition of cyber crime may be the unlawful acts wherein the computer is either a tool or target or both. . The computers may be used as a tool in the kinds of activities that include financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crimes, e-mail spoofing, forgery, cyber defamation and cyber stalking.

The sine qua non for cyber crime is that there should be an illegal unauthorized involvement at any stage of the virtual cyber medium.

1.3. REASON OF CYBER CRIME:

Human beings are vulnerable, so rule of law is required to protect them. Applying this statement to the cyber space we may say that computers are also vulnerable, so force of law is required to protect and safeguard them against cyber crime. The reason for the vulnerability of computers may be said to be:

1.3.1. Capacity to store in comparatively small space:

The computer has unique characteristic of storing data in a very small space. This affords the opportunity to remove or derive information either through physical or virtual medium which makes it much easier.

1.3.2. Easy to access:

The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorder; retina imagers etc. that can befool biometric system and bypass firewall can be utilized to get past many a security system.

1.3.3. Complex:

The computer work and the operating system in turn are composed of millions of codes. Human mind is fragile and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

1.3.4. Negligence:

Negligence is very closely connected with human conduct. It is therefore very probable while protecting the computer system there might be any negligence which in turn provides opportunity to a cyber criminal to gain an access and control over the computer system.

1.3.5. Loss of evidence.

Loss of evidence is a very common and obvious problem as all the routing data can be destroyed. Further, collection of data outside the territorial extent also paralyses the system of crime investigation.

1.4. TYPES OF CYBER CRIMES:

Now after defining "cyber crime" and differentiating it from "conventional crime", let us examine the acts wherein the computer is a tool for an unlawful act. This kind of activity usually involves a modification of a conventional crime by using computers. Some examples are:

1.4.1. Hacking:

Hacking in simple terms means an illegal intrusion into a computer system or network. There is an equivalent term to hacking i.e. cracking but from Indian laws perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They posses the desire to destruct and they get the kick back of such destruction. Some hackers hack for personal monetary gains such as to stealing the credit card information transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening him to publish the stolen information which is critical in nature.

Government websites are the hot targets of the hackers due to the press coverage it receives. Hackers enjoy the media coverage.

- *Motives behind the Crime*

1. Greed
2. Power
3. Publicity
4. Revenge
5. Adventure
6. Desire to access forbidden information
7. Destructive mindset
8. Wants to sell n/w security services

1.4.2. Cyber Pornography:

Pornography or porn is the depiction of explicit sexual subject matter for the purpose of sexually exciting the viewer. Pornography makes no claim to artistic merit, unlike erotica which does.

1.4.3. Cyber stalking:

Although there is no universally accepted definition of cyber stalking, however the term is used to refer to the use of the Internet e-mail or other electronic communication devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly such as following a person at a person's home or place of business, making harassing phone calls, leaving written messages or objects or vandalizing a person's property. While some conduct involving annoying or menacing behavior might fall short of illegal stalking. Such behavior may be a prelude to stalking, violence should be treated seriously.

Both kind of Stalkers online and offline have desire to control the victim's life. Majority of the stalkers are the dejected lovers or ex-lovers who then want to harass the victim because they failed to satisfy their secret desires. Most of the stalkers are men and victim female.

1.4.4. E-Mail Spoofing:

A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source. For instance, david who has an e-mail address david@asianlaws.org, his enemy peter spoofs his email and sends obscene messages to all his acquaintances. Since the e-mail appears to have originated from david his friends could take it amiss and relationships could be spoiled for life.

E-mail spoofing can also cause monetary damage. In an American case a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed e-mails purportedly from news agencies like Reuters to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

Recently a branch of the Global Trust Bank experienced a run on the bank. Numerous customers decided to withdraw all their money and close their accounts. It was revealed that someone had sent out spoofed emails to many of the bank's customers stating that the bank was in very bad shape financially and could close operations at any time. The spoofed e-mail appeared to have originated from the bank itself.

1.4.5. Sale of Illegal articles:

Sites based companies which sell illegal drugs on the internet pose a significant public health risk and a real problem. This also include sale of narcotics, weapons and wildlife etc. by posing information on websites, auction websites and bulletin boards or simply by using e-mail communication.

1.4.6. Online gambling:

There are millions of websites; all hosted on servers abroad that offer online gambling. In fact it is believed that many of these websites are actually fronts for money laundering. Gambling is a multi-billion dollar industry. One can gamble from the convenience of his own home with his web browser. Whether this is or should be legal is fact in issue. Since most gambling sites exist offshore in countries where gambling is legal. Gambling site owners feel that what they are doing is legal.

1.4.7. Intellectual Property crimes:

These include software piracy, copyright infringement, trademarks, brand name violations and theft of computer source code etc.

The unauthorized copying and distribution of computer programs can cause considerable economic loss to the legitimate owners. Several jurisdictions have dictated that this activity should be subject to criminal sanctions but others declined to hold the defendant liable under the wire fraud statute because his infringement activities of distributing computer software did not result in a profit. The court went on to rule that criminal and civil penalties should attach to defendants involved in willful multiple infringements of copyrighted software even if the infringer lacked commercial motive. The court left it to the legislature to define the crime and to establish the penalty.

Ironically many who pirate software are fully aware of the illegalities though they are able to rationalize continuing the practice. Some have difficulty in understanding the distinction between freeware shareware and commercial software. Others believe students won't be able to take advantage of the many technology-based educational opportunities without access to unaffordable software. Since software budgeting is often inadequate and occasional upgrade of hardware makes older versions of software obsolete after few years. Some think the only solution to the problem is to pirate newer versions of past purchased software. Finally some people don't believe that software piracy is truly a stealing because there is no loss of a tangible product involved in the act of piracy.

1.4.8. Forgery:

The world of business or commerce today operates on the basis of documents (paper or electronic). It's been this way ever since the merchant class became literate and documents took on the quality of expressing legal rights and obligations. In today's world we prove important things by producing documents (e.g. birth certificates driving licenses, titles invoices and bills of sale). False documents represent a threat to social stability and order. They undermine confidence in the authenticity of documents.

1.4.9. Cyber Defamation:

Defamation is defined as an intentional false communication either published or publicly spoken that injures another's reputation or good name; a statement which exposes a person to contempt, hatred or ridicule. Defamation when in a written and permanent form is known as libel and oral defamation is known as slander. While web pages can include sound files which with the use of a sound card and speakers can reproduce sounds words etc. the overwhelming majority of content on the internet is graphical in nature. As the internet at least for the time being is primarily a visual medium and considering that the view from a screen is readily printable into a more permanent form. Defamatory speech over the internet most probably falls under the definition of libel.

1.4.10. FINANCIAL CRIMES:

This would include cheating, credit card, ATM card, on line banking frauds, frauds by Mobile phone and money laundering etc.

1.4.10.i. Money Laundering:

Definition

Generally, money laundering is defined as under:

> *"A process by which illegal cash assets or black money generated by whatsoever criminal activities are manipulated in such a way as to make them look as if they were derived from very clean, immaculate, licit and legitimate sources."*

Under United States Law:

> *"Money Laundering means moving illigimately obtained funds through people or accounts to hide the source of those funds.*

FATF has defined Money Laundering as under:

> *"The conversion or transfer of property, the concealment or disguise of its true nature or source or the acquisition, possession or use of property knowing it to be criminally derived."*

Another way to express way to express money laundering is:

> *"The process by which one conceals the existence of illegal source, or illegal acquisition of income and then disguises that income to make it appear legitimate". In other words, the processes used by criminals through which they make "dirty" money appear "clean".*

Though initially considered as an aspect integral to only drug trafficking, laundering represents a necessary step in almost every criminal activity that yields profits. Now it is recognized a criminal offence all over the world.

Criminals engage in money laundering for the following three reasons.

First, money represents the lifeblood of the organization that engages in criminal activities for financial gain because it covers operating expenses, replenishes inventories, purchases the services of corrupt officials to escape detection and further the interests of the illegal enterprise, and pays for an extravagant lifestyle. To spend money in these ways, criminals must make the money, they derived illegally, appear legitimate.

Second, a trail of money from an offence to the criminals can become incriminating evidence. Criminals must obscure or hide the source of their wealth or alternately disguise ownership or control to ensure that illicit proceeds are not used to prosecute them.

Third, the proceeds from crime often become the target of investigation and seizure. To shield ill-gotten gains from suspicion and protect them from seizure, the criminals must conceal their existence or, alternately, make them look legitimate.

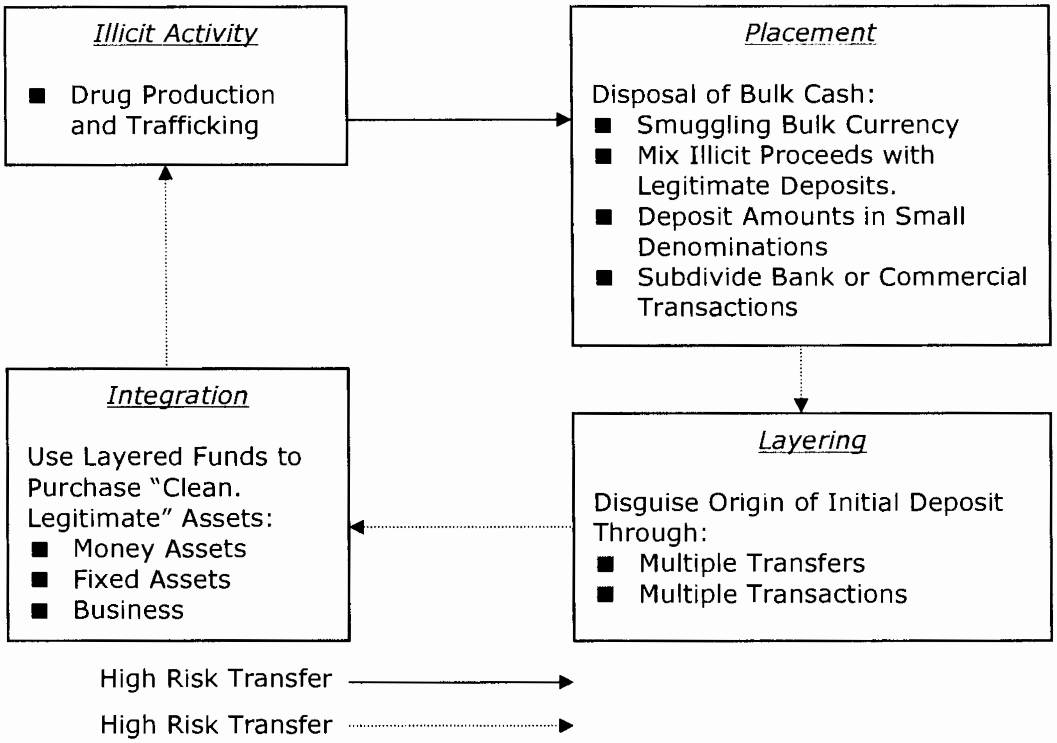
When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved. Criminals do this by disguising the sources, changing the form, or moving the funds to a place where they are less likely to attract attention. Hence,

"Money laundering is the concealment, conversion, transfer or disguise of any property that represents proceeds from criminal activity."

The people launder money in an attempt to explain that they acquired their wealth legitimately. In some countries it is now considered a criminal activity in an attempt to evade the legal systems.

"In the first Interim Report of the US President's commission on Organized Crimes defined Money Laundering as the process by which one conceals the existence, illegal source, or illegal application of income, and then disguises that income to make it appear legitimate. The term refers to several different but interrelated processes, all of which meet the basic definition of transforming criminally tainted cash illegally earned into a form that disguises its origins so that it can be used in legitimate commerce as a legally appearing instrument or asset and thus become "clean". Recently the term's meaning has broaden to refer not only to the individual act of laundering but to numerous complex steps used in the illegal asset conversion process, beyond the basic exchange of cash, for less conspicuous and more socially acceptable methods of payment."

PROCESS OF MONEY LAUNDERING



Illicit Activity
■ Drug Production and Trafficking
Placement
Disposal of Bulk Cash:
■ Smuggling Bulk Currency
■ Mix Illicit Proceeds with Legitimate Deposits.
■ Deposit Amounts in Small Denominations
■ Subdivide Bank or Commercial Transactions
Integration
Use Layered Funds to Purchase "Clean. Legitimate" Assets:
■ Money Assets
■ Fixed Assets
■ Business
Layering
Disguise Origin of Initial Deposit Through:
■ Multiple Transfers
■ Multiple Transactions
High Risk Transfer
High Risk Transfer

1.4.10.ii. Online investment newsletters:

Many newsletters on the interments provide the investors with free advice recommending stocks where they should invest. Sometimes these recommendations are totally bogus and cause loss to the investors.

1.4.10.iii. Credit card fraud:

"With the electronic commerce rapidly becoming a major force in national economies it offers rich pickings for criminals prepared to undertake fraudulent activities. In U.S.A the ten most frequent fraud reports involve undelivered and online services, damaged, defective, misrepresented or undelivered merchandise auction sale pyramid schemes and multilevel marketing and of the most predominant among them is credit card fraud. Something like half a billion dollars is lost to consumers in card fraud alone. There is also publishing of false digital signatures."

1.4.10.11. Theft of information contained in electronic form:

This includes information stored in computer hard disks and removable storage media etc.

1.4.10.12. Email bombing:

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.

"Email bombing is characterized by abuses repeatedly sending an email message to a particular address at a specific victim site. In many instances the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused increasing the denial of service impact."

1.4.10.13. Data diddling:

"Data diddling involves changing data prior or during input into a computer. In other words information is changed from the way it should be entered by a person typing in the data a virus that changes data, the programmer of the database or application or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating, recording, encoding, and examining, checking, converting or transmitting data."

1.4.10.14. Logic Bombs:

"A logic bomb is a program that runs at a specific date or time to cause unwanted and/or unauthorized functions. It can affect software or data, and can cause serious damage to a system. Generally, it will enter a system as hidden content, or may be installed on the system by someone within a company. For example, a disgruntled employee may write a program designed to crash the system one month after he plans to quit the company. When this date and time arrives, the program then executes. In other words, the bomb goes off."

1.4.10.15. Salami Attacks:

"These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed e.g. a bank employee inserts a program into the bank's server that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizeable amount of money every month.

The logic bomb was programmed to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last in the bank's rosters. Then he went and opened an account in the name of Ziegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither any of the account holders nor the bank officials noticed the fault.

It was brought to their notice when person by the name of Ziegler opened his account in that bank. He was surprised to find a sizeable amount of money being transferred into his account every Saturday. Being an honest person, he reported the mistake to the bank authorities and the entire scheme was revealed."

1.4.10.16. Denial of Service attack:

"DOS Attack, (denial-of-service attack), a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DOS attacks, such as the ping of death and Teardrop attacks, exploit limitations in the TCP/IP protocols. For all known DOS attacks, there are software fixtures that system administrators can install to limit the damage caused by the attacks. But like viruses new DOS attacks are constantly being dreamed up by hackers."

1.4.10.17. Physically damaging a computer system:

This crime is committed by physically damaging a computer or its peripherals.

1.5. TOOLS AND TECHNIQUES OF CYBER CRIME

1.5.i. Unauthorized Access:

"Unauthorized access would mean any kind of access without the permission of either the rightful owner or the person in charge of a computer, computer system or computer network. Thus not only would accessing a server by cracking its password authentication system be unauthorized access, switching on a computer system without the permission of the person in charge of such a computer system would also be unauthorized access."

Packet sniffing, tempest attack, password cracking and buffer overflow are common techniques used for unauthorized access.

1.5.ii. Packet Sniffing:

"Packet Sniffing is a technology used by crackers and forensics experts alike. To understand Sniffing we must first understand the basics of data transmission. We all know that data travels in the form of packets on networks. These packets also referred to as data-grams, are of various sizes depending on the network bandwidth as well as amount of data being carried in the packet in measure of bytes. Each packet has an identification label also called a 'header'. The header carries information of the source, destination, protocol and size of packets, total number of packets in sequence and the unique number of the packet."[15]

The data carried by the packet is in an encrypted format, not as such for the sake of security as for the sake of convenience in transmitting the data. This cipher text (encrypted form) is also known as the hex of the data. When a person says 'A' sends a file to 'B', the data in files gets converted into hex and gets broken into lots of packets finally headers are attached to all packets and the data is ready for transmission.

"When being transmitted, the packets travel through a number of layers (Open System Interconnection (OSI) Model). Amongst these layers, the network layer is responsible for preparing the packet for transmission. This is the level where most hackers and adversaries are likely to attack knowing that the packets are usually not secured and are prone to spoofing and sniffing attacks."

1.5.iii. Tempest attack:

Tempest is the ability to monitor electromagnetic emissions from computers in order to reconstruct the data. This allows remote monitoring of network cables or remotely viewing monitors.

"The word TEMPEST is usually understood to stand for "Transient Electromagnetic Pulse Emanation Standard". There are some fonts that remove the high frequency information, and thus severely reduce the ability to remotely view text on the screen. PGP also provides this option of using tempest resistant fonts."

1.5.iv. Password Cracking:

A password is a type of authentication. It is secret word or phrase that a user must know in order to gain access. A pass phrase is a correspondingly larger secret consisting of multiple words.

Internal to the computer, if password information is constantly being checked and if you were queried for the password each and every time, you would find that computer would become unusable.

1.5.v. Viruses:

"A computer virus is a computer program that can infect other computer programs by modifying them in such a way as to include a (possibly evolved) copy of it. Note that a program does not have to perform outright damage (such as deleting or corrupting files) in order to be called a "VIRUS".

Many people use the term loosely to cover any sort of program that tries to hide its (malicious) function and tries to spread onto as many computers as possible. Viruses can be very dangerous."

1.5.vi. Email related crime:

E-mail has fast emerged as the world's most preferred form of communication. Billions of e-mail messages traverse the globe daily. Like any other form of communication, e-mail is also misused by criminal elements.

The ease, speed and relative anonymity of e-mail has made it a powerful tool for criminals. Some of the major e-mail related crimes are:

- E-mail spoofing
- Sending malicious codes through e-mail
- E-mail bombing
- Sending threatening e-mails
- Defamatory e-mails
- E-mail frauds

1.5.vii. Organized Crime

"Organized crime is primarily about the pursuit of profit and can be understood in Clausewitzian terms as a continuation of business by industries and the Fulton Fish Market, the toxic waste disposal and construction industries in Italy, and the banking sector and aluminum industry in Russia. From an organized crime perspective, the Internet and the growth of e-commerce can be understood as the provision of a new set of targets for infiltration and the exercise of influence a prospect that suggests that Internet technology and service firms should be particularly careful about prospective partners and financial supporters."

In sum, the synergy between organized crime and the Internet is not only very natural but also one that is likely to flourish and develop even further in future. The Internet provides both channels and targets for crime and enables them to be exploited for considerable gain with a very low level of risk.

criminal means. Criminal organizations are not the only players in illicit markets, but they are often the most important, not least because of the added "competitiveness" that is provided by the threat of organized violence. Moreover, criminal organizations tend to be exceptionally good at environmental scanning in the search for new criminal enterprises and activities. In this context, the Internet and the continuing growth of electronic commerce offer enormous new opportunities.

In recent years, there has been a massive increase in the sophistication of organized crime and drug trafficking groups. Colombian drug trafficking organizations, for example, have followed standard business practices for market and product diversification. Criminal organizations have increasingly hired financial specialists to conduct their money laundering transactions. This adds an extra layer of insulation while utilizing legal and financial experts knowledgeable about the layering of financial transactions and the availability of safe havens in offshore financial jurisdictions. Similarly, organized crime does not need to develop technical expertise about the Internet it can hire those in the intruder community who do have the expertise, ensuring through a mixture of rewards and threats that they carry out their assigned tasks effectively and efficiently."

The Internet itself provides opportunities for various kinds of theft. Online thieves can rob online banks or illicitly gain access to intellectual property. The Internet offers new means of committing old crimes such as fraud, and offers new vulnerabilities relating to communications and data that provide attractive targets for extortion, a crime that has always been a staple of organized crime.

"Organized crime has always selected particular industries as targets for infiltration and the exercise of illicit influence. In the past, these have included the New York garbage hauling and construction

CHAPTER – 2

LITERATURE REVIEW

In the space the number of human activities that can be done are almost the same that which can be done on the real earth and range from education to buying property and from selling drugs to give evidence in court via a video conference. If one wants to pay his bills through the online process there must be laws to regulate this. Thus the volume of law and regulations needed to regulate the cyber space activity would have to increase with the increase in the activities done over the cyber space and would soon be as many as it exists in the real offline world.

Many nations that boast of having cyber laws have only a few legislations to go by. Even in Pakistan the number of legislations of cyber law and legislations is limited to only about 5 pieces mainly on E- commerce, copyright and digital signatures. The same is true for most of the other nations. Many nations with limited technological knowledge have to import their cyber legislations from the US, European Union, Canada or from Australia. However even in the US and in EU where the most number of legislations exists there is still a lot of work to be done to increase the range of legislations to keep pace with the increase in the number of new human activities now taking place in the cyber space.

In this chapter we will discuss salient features of the cyber laws of the selected countries and will also look into these laws from different angles particularly from the corporate prospective.

2.1 UNITED STATES OF AMERICA The Computer Fraud and Abuse Act (CFAA)[2]

In the early 1980s law enforcement agencies faced the dawn of the computer age with growing concern about the lack of criminal laws available to fight the emerging computer crimes. Although the wire and mail fraud provisions of the federal criminal code were capable of addressing some types of computer-related criminal activity, neither of those statutes provided the full range of tools needed to combat these new crimes. *[See H.R. Rep. No. 98-894, at 6 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3692.]*

In response, Congress included in the Comprehensive Crime Control Act of 1984 provisions to address the unauthorized access and use of computers and computer networks. The legislative history indicates that Congress intended these provisions to provide "a clearer statement of proscribed activity" to "the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access." Id. Congress did this by making it a felony to access classified information in a computer without authorization, and a misdemeanor to access financial records or credit histories stored in a financial institution or to trespass into a government computer. In so doing, Congress opted not to add new provisions regarding computers to existing criminal laws, but rather to address federal computer-related offenses in a single, new statute, 18 U.S.C[3]. § 1030[4].

[2] CFAA (1984)
[3] USC Title 18 (2008)
[4] Anonymous (2008)

Even after enacting section 1030, Congress continued to investigate problems associated with computer crime to determine whether federal criminal laws required further revision. Throughout 1985, both the House and the Senate held hearings on potential computer crime bills, continuing the efforts begun in the year before. These hearings culminated in the Computer Fraud and Abuse Act (CFAA), enacted by Congress in 1986, which amended 18 U.S.C. § 1030.

In the CFAA, Congress attempted to strike an "appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses." See S. Rep. No. 99-432, at 4 (1986), reprinted in 1986 U.S.C.C.A.N. 2479, 2482. Congress addressed federalism concerns in the CFAA by limiting federal jurisdiction to cases with a compelling federal interest—i.e., where computers of the federal government or certain financial institutions are involved, or where the crime itself is interstate in nature. See id.

In addition to clarifying a number of the provisions in the original section 1030, the CFAA also criminalized additional computer-related acts. For example, Congress added a provision to penalize the theft of property via computer that occurs as a part of a scheme to defraud. Congress also added a provision to penalize those who intentionally alter, damage, or destroy data belonging to others. This latter provision was designed to cover such activities as the distribution of malicious code and denial of service attacks. Finally, Congress also included in the CFAA a provision criminalizing trafficking in passwords and similar items.

As computer crimes continued to grow in sophistication and as prosecutors gained experience with the CFAA, the CFAA required further amendment, which Congress did in 1988, 1989, 1990, 1994, 1996, 2001, and 2002.

The current version of the CFAA includes seven types of criminal activity, outlined in Table below. Attempts to commit these crimes are also crimes. 18 U.S.C. § 1030(b). Lawfully authorized activities of law enforcement or intelligence agencies are explicitly excluded from coverage of section 1030. 18 U.S.C. § 1030(f).

Table: Summary of CFAA Provisions

Offense	**Section**	**Sentence***
Obtaining National Security Information	(a)(1)	10 (20) years
Compromising the Confidentiality of a Computer	(a)(2)	1 or 5
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Knowing Transmission and Intentional Damage	(a)(5)(A)(i)	10 (20 or life)
Intentional Access and Reckless Damage	(a)(5)(A)(ii)	5 (20)
Intentional Access and Damage	(a)(5)(A)(iii)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Threats to Damage Computer	(a)(7)	5 (10)

*** The maximum prison sentences for second convictions are noted in parenthesis.**

In some circumstances, the CFAA allows victims who suffer specific types of loss or damage as a result of violations of the Act to bring civil actions against the violators for compensatory damages and injunctive or other equitable relief. 18 U.S.C. § 1030(g).

2.1.A. KEY DEFINITIONS

Two terms are common to most prosecutions under section 1030 and are discussed below: "protected computer" and "authorization." Other terms are discussed with their applicable subsection.

1. PROTECTED COMPUTER

The term "protected computer," 18 U.S.C. § 1030(e)(2), is a statutory term of art that has nothing to do with the security of the computer. In a nutshell, "protected computer" covers computers used in interstate or foreign commerce (e.g., the Internet) and computers of the federal government and financial institutions.

"Protected computer" did not appear in the CFAA until 1996, when Congress attempted to correct deficiencies identified in earlier versions of the statute. In 1994, Congress amended the CFAA so that it protected any "computer used in interstate commerce or communication" rather than a "Federal interest computer." This change expanded the scope of the Act to include certain non-government computers that Congress deemed deserving of federal protection. See S. Rep. No. 104-357, at 10 (1996), available at 1996 WL 492169 (discussing 1994 amendment). In doing so, however, Congress "inadvertently eliminated Federal protection for those Government and financial institution computers not used in interstate commerce." United States v. Middleton, 231 F.3d 1207, 1212 n.2 (9th Cir. 2000) (citing S. Rep. No. 104-357).

Congress corrected this error in the 1996 amendments to the CFAA, which defined "protected computer" as a computer used by the federal government or a financial institution, or one "which is used in interstate or foreign commerce." 18 U.S.C. 1030(e)(2) (1996). The definition did not explicitly address situations where an attacker within the United States attacks a computer system located abroad. In addition, this definition was not readily applicable to situations in which individuals in foreign countries routed communications through the United States as they hacked from one foreign country to another.

In 2001, the USA PATRIOT Act amended the definition of "protected computer" to make clear that this term includes computers outside of the United States so long as they affect "interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B) (2001). As a result of this amendment, a protected computer is now defined as a computer "exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government" or a computer "used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2).

2. WITHOUT OR IN EXCESS OF AUTHORIZATION

Many of the criminal offenses contained within the CFAA require that an intruder either access a computer without authorization or exceed authorized access. The term "without authorization" is not defined in the Act and one court found its meaning "to be elusive." EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001) (dicta); see also Secure Info Corp. v. Telos Corp., 387 F. Supp. 2d 593 (E.D. Va. 2005) (holding that defendants had authorization to use a computer system even though such access violated the terms of a license agreement binding the user who provided them with access to the system).

The term "exceeds authorized access" is defined by the CFAA to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

The legislative history of the CFAA reflects an expectation by Congress that persons who exceed authorized access are likely to be insiders, whereas persons who act without authorization are likely to be outsiders. As a result, Congress restricted the circumstances under which an insider—a user with authorized access—could be held liable for violating section 1030. "[I]insiders, who are authorized to access a computer, face criminal liability only if they intend to cause damage to the computer, not for recklessly or negligently causing damage.

By contrast, outside intruders who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass." See S. Rep. No. 99-432, at 10 (1986), reprinted in 1986 U.S.C.C.A.N. 2479; see also S. Rep. No. 104-357, at 11 (1996), available at 1996 WL 492169.

According to this view, outsiders are intruders with no rights to use a protected computer system, and, therefore, they should be subject to a wider range of criminal prohibitions. Those who act without authorization can be convicted under any of the access offenses contained in the CFAA, which can be found in 18 U.S.C. § 1030(a)(1)-(5). However, users who exceed authorized access have at least some authority to access the computer system. Such users are therefore subject to criminal liability under more narrow circumstances. The offenses that can be charged based on exceeding authorized access are limited to those set forth in subsections (a)(1), (a)(2), and (a)(4). If both the "without authorization" and "exceeds authorization" boxes are checked, the offense can be proven upon either showing. Note that subsections (a)(6) and (a)(7) are not access offenses and therefore have no authorization requirement.

> To access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.
> *18 U.S.C. § 1030(e)(6).*

2.1.B. OBTAINING NATIONAL SECURITY INFORMATION: 18 U.S.C. § 1030(a) (1)

The infrequently-used section 1030(a)(1) punishes the act of obtaining national security information without or in excess of authorization and then willfully providing or attempting to provide the information to an unauthorized recipient, or willfully retaining the information.

Any steps in investigating or indicting a case under section 1030 (a)(1) require the prior approval of the National Security Division of the Department of Justice, through the Counterespionage Section. See USAM 9-90.020. Please contact them at (202) 514-1187.

Title 18, United States Code, Section 1030(a)(1) provides:

Whoever–

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it ...

shall be punished as provided in subsection (c) of this section.

1. Knowingly Access a Computer Without or In Excess of Authorization

A violation of this section requires proof that the defendant knowingly accessed a computer without authorization or in excess of authorization. This covers both completely unauthorized individuals who intrude into a computer containing national security information as well as insiders with limited privileges who manage to access portions of a computer or computer network to which they have not been granted access. The scope of authorization will depend upon the facts of each case. However, it is worth noting that computers and computer networks containing national security information will normally be classified and incorporate security safeguards and access controls of their own, which should facilitate proving this element.

2. Obtain National Security Information

TH 7453

A violation of this section requires that the information obtained is national security information, meaning information "that has been determined by the United States Government pursuant to an Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954." An example of national security information used in section 1030(a)(1) would be classified information obtained from a Department of Defense computer or restricted data obtained from a Department of Energy computer.

3. Information Could Injure the United States or Benefit a Foreign Nation

A violation of this section requires proof that the defendant had reason to believe that the national security information so obtained could be used to the injury of the United States or to the advantage of any foreign nation. The fact that the national security information is classified or restricted, along with proof of the defendant's knowledge of that fact, should be sufficient to establish this element of the offense.

4. Willful Communication, Delivery, Transmission, or Retention

A violation of this section requires proof that the defendant willfully communicated, delivered, or transmitted the national security information, attempted to do so or willfully retained the information instead of delivering it to the intended recipient. This element could be proven through evidence showing that the defendant did any of the following: (a) communicated, delivered, or transmitted national security information, or caused it to be communicated, delivered, or transmitted, to any person not entitled to receive it; (b) attempted to communicate, deliver, or transmit national security information, or attempted to cause it to be communicated, delivered, or transmitted to any person not entitled to receive it; or (c) willfully retained national security information and failed to deliver it to an officer or employee of the United States who is entitled to receive it in the course of their official duties.

5. Penalties

Convictions under this section are felonies punishable by a fine, imprisonment for not more than ten years, or both. 18 U.S.C. § 1030(c)(1)(A). A violation that occurs after another conviction under section 1030 is punishable by a fine, imprisonment for not more than twenty years, or both. 18 U.S.C. § 1030(c)(1)(B).

2.1.C. COMPROMISING CONFIDENTIALITY: 18 U.S.C. § 1030(a) (2)

The distinct but overlapping crimes established by the three subsections of section 1030(a)(2) punish the unauthorized access of different types of information and computers. Violations of this section are misdemeanors unless aggravating factors exist. Also, some intrusions may violate more than one subsection. For example, a computer intrusion into a federal agency's computer might be covered under the latter two subsections.

Section 1030(a)(2) does not impose a monetary threshold for a violation, in recognition of the fact that some invasions of privacy do not lend themselves to monetary valuation but still warrant federal protection. If not authorized, downloading sensitive personnel information from a company's computer (via an interstate communication) or gathering personal data from the National Crime Information Center would both be serious violations of privacy which do not easily lend themselves to a dollar valuation of the damage. Although there is no monetary threshold for establishing an offense under section 1030(a)(2), the value of the information obtained during an intrusion is important when determining whether a violation constitutes a misdemeanor or a felony.

Title 18, United States Code, Section 1030(a)(2) provides:

Whoever–

(2) Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains–

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) Information from any department or agency of the United States; or

(C) Information from any protected computer if the conduct involved an interstate or foreign communication ...

shall be punished as provided in subsection (c) of this section.

1. Intentionally Access a Computer

A violation of this section requires that the defendant actually be the one to access a computer without authorization rather than merely receive information that was accessed without authorization by another. For example, if A obtains information in violation of section 1030(a)(2) and forwards it to B, B has not violated this section, even if B knew the source of the information. See Role Models America, Inc. v. Jones, 305 F. Supp. 2d 564 (D. Md. 2004). Of course, B might be subject to prosecution for participating in a criminal conspiracy to violate this section.

2. Without or In Excess of Authorization

Please see page 4 for the discussion of access without or in excess of authorization.

3. Obtained Information

The term "obtaining information" is an expansive one which includes merely viewing information online without downloading or copying it. See S. Rep. No. 99-432, at 6; America Online, Inc. v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255 (N.D. Iowa 2000). Information stored electronically can be obtained not only by actual physical theft, but by "mere observation of the data." Id. The "crux of the offense under subsection 1030(a)(2)(C) ... is the abuse of a computer to obtain the information."

"Information" includes intangible goods, settling an issue raised by the Tenth Circuit's decision in United States v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991). In Brown, the appellate court held that purely intangible intellectual property, such as a computer program, did not constitute goods or services that can be stolen or converted. In the 1996 amendments to section 1030, Congress clarified this issue, stating that section 1030(a)(2) would "ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected." S. Rep. No. 104-357, at 7, available at 1996 WL 492169.

4. Financial Institution or Consumer Reporting Agency

To prove a violation of section 1030(a)(2)(A), obtaining information related to the Fair Credit Reporting Act (FCRA), the violation must be willful. See Ausherman v. Bank of America Corp., 352 F.3d 896 at 900 n.4 (4th Cir. 2003). To prove willfulness under the FCRA, the government must show that the defendant knowingly and intentionally committed an act in conscious disregard for the rights of a consumer.

5. Department or Agency of the United States

Whether a company working as a private contractor for the government constitutes a "department or agency of the United States" for purposes of prosecution under subsection (a)(2)(B) has not been addressed by any court. However, the argument that private contractors are intended to be covered by this section may be undercut by section 1030(a)(3), which includes language permitting prosecution of trespass into government systems and non-government systems, if "such conduct affects that use by or for the Government of the United States." The existence of this language suggests that if Congress had intended to extend the reach of section 1030(a)(2) beyond computers owned by the federal government, it would have done so using language it used elsewhere in section 1030.

6. Protected Computer

The term "protected computer" is defined in section 1030(e)(2) and is discussed in the "Key Definitions" discussion on page 3.

Note that a violation of this subsection must involve an actual interstate or foreign communication and not merely the use of an interstate communication mechanism, as other parts of the CFAA allow. The intent of this subsection is to protect against the interstate or foreign theft of information by computer, not to give federal jurisdiction over all circumstances in which someone unlawfully obtains information via a computer. See S. Rep. No 104-357. Therefore, using the Internet or connecting by telephone to a network may not be sufficient to charge a violation of this subsection where there is no evidence that the victim computer was accessed using some type of interstate or foreign communication.

7. Penalties

Violations of section 1030(a)(2) are misdemeanors punishable by a fine or a one-year prison term, unless aggravating factors apply. 18 U.S.C. § 1030(c)(2)(A). Merely obtaining information worth less than $5,000 is a misdemeanor, unless committed after a conviction of another offense under section 1030. 18 U.S.C. § 1030(c)(2)(C). A violation or attempted violation of section 1030(a)(2) is a felony if:

- committed for commercial advantage or private financial gain,
- committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or
- the value of the information obtained exceeds $5,000.

18 U.S.C. § 1030(c)(2)(B). If the aggravating factors apply, a violation is punishable by a fine, up to five years' imprisonment, or both.

Any reasonable method can be used to establish the value of the information obtained. For example, the research, development, and manufacturing costs or the value of the property "in the thieves' market" can be used to meet the $5,000 valuation. See, e.g., United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988). The terms "for purposes of commercial advantage or private financial gain" and "for the purpose of committing any criminal or tortious act" are taken from copyright law (17 U.S.C. § 506(a)) and the wiretap statute (18 U.S.C. § 2511(2)(d)), respectively.

2.1.D. TRESPASSING IN A GOVERNMENT COMPUTER: 18 U.S.C. § 1030(a)(3)

Section 1030(a)(3) protects against "trespasses" by outsiders into federal government computers, even when no information is obtained during such trespasses. Congress limited this section's application to outsiders out of concern that federal employees could become unwittingly subject to prosecution or punished criminally when administrative sanctions were more appropriate. S. Rep. No. 99-432, at 7, 1986 U.S.C.C.A.N. at 2485. However, Congress intended interdepartmental trespasses (rather than intradepartmental trespasses) to be punishable under section 1030(a)(3).

Note that section 1030(a)(2) applies to many of the same cases in which section 1030(a)(3) could be charged. In such cases, section 1030(a)(2) may be the preferred charge because a first offense of section 1030(a)(2) may be charged as a felony if certain aggravating factors are present, while a first offence of section 1030(a)(3) is only a misdemeanor.

> *Title 18, United State Code, Section 1030(a)(3) provides:*
> *Whoever–*
>
> *(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States ....*
>
> *shall be punished as provided in subsection (c) of this section.*

1. Intentionally Access

The meaning of this term under this section is identical to the meaning under section 1030(a)(2), discussed on page 16.

2. Without Authorization

By requiring that the defendant act without authorization to the computer and not criminalizing merely exceeding authorized access to a computer, section 1030(a)(3) does not apply to situations in which employees merely "'exceed authorized access" to computers in their own department. S. Rep. No. 99-432. However, Congress also offered that section 1030(a)(3) applies "where the offender's act of trespass is interdepartmental in nature." Id. at 8. Thus, while federal employees may not be subject to prosecution under section 1030(a)(3) as insiders as to their own agency's computers, they may be eligible for prosecution as outsiders in regard to intrusions into other agencies' computers.

3. Nonpublic Computer of the United States

"Nonpublic" includes most government computers, but not Internet servers that, by design, offer services to members of the general public. For example, a government agency's database server is probably nonpublic, while the same agency's web servers and domain name servers are "public."

The computer must be "of"—meaning owned or controlled by—a department or agency of the United States.

The computer must also be either exclusively for the use of the United States, or at least used "by or for" the Government of the United States in some capacity. For example, if the United States has obtained an account on a private company's server, that server is used "by" the United States even though it is not owned by the United States.

4. Affected United States' Use of Computer

Demonstrating that the attacked computer is affected by an intrusion should be simple. Almost any network intrusion will affect the government's use of its computers because any intrusion potentially affects the confidentiality and integrity of the government's network and often requires substantial measures to reconstitute the network.

Section 1030(a)(3) "defines as a criminal violation the knowing unauthorized access or use of the system for any unauthorized purpose." Sawyer v. Department of Air Force, 31 M.S.P.R. 193, 196 (M.S.P.B. 1986). Notably, it is not necessary to demonstrate that the intruder obtained any information from the computer, or that the intruder's trespass damaged the computer. It is not even necessary to show that the intruder's conduct "adversely" affected the government's operation of a computer. Under § 1030(a)(3), there are no benign intrusions into government computers.

5. Statutory Penalties

Violations of this subsection are punishable by a fine and up to one year in prison, 18 U.S.C. § 1030(c)(2)(A), unless the individual has previously been convicted of a section 1030 offense, in which case the punishment increases to a maximum of ten years in prison, 18 U.S.C. § 1030(c)(2)(c).

6. Relation to Other Statutes

Section 1030(a)(3) is not charged often, and few cases interpret it. This lack is probably because section 1030(a)(2) applies in many of the same cases in which section 1030(a)(3) could be charged. In such cases, section 1030(a)(2) may be the preferred charge because statutory sentencing enhancements sometimes allow section 1030(a)(2) to be charged as a felony on the first offense. A violation of section 1030(a)(3), on the other hand, is only a misdemeanor for a first offense.

2.1.E. ACCESSING TO DEFRAUD AND OBTAIN VALUE: 18 U.S.C. § 1030(a)(4)

When deciding how to charge a computer hacking case, prosecutors should consider this section as an alternative to section 1030(a)(2) where evidence of fraud exists, particularly because this section is a felony whereas subsection (a)(2) is a misdemeanor (unless certain aggravating factors apply).

Prosecutors may also want to consider charges under the wire fraud statute, 18 U.S.C. § 1343, which requires proof of many elements similar to those needed for section 1030(a)(4), but carries stiffer penalties. For more detail on the comparison, please see page 29. For more discussion about wire fraud, please see page 90.

> *Title 18, United State Code, Section 1030(a)(4) provides:*
>
> *Whoever–*
>
> *(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period ...*
>
> *shall be punished as provided in subsection (c) of this section.*

1. Knowingly Access Without or In Excess of Authorization

Please see page 4 for the discussion of the concept of access without or in excess of authorization.

2. With Intent to Defraud

The phrase "knowingly and with intent to defraud" is not defined by section 1030. Very little case law under section 1030 exists as to its meaning, leaving open the question of how broadly a court will interpret the phrase. On one hand, courts might interpret "intent to defraud" as requiring proof of the elements of common law fraud.[5] On the other hand, courts might give more liberal meaning to the phrase "intent to defraud" and allow proof of mere wrongdoing or dishonesty to suffice.

In examining the phrase "to defraud" in the mail and wire fraud statutes,[6] the Supreme Court rejected the notion that every "scheme or artifice that in its necessary consequence is one which is calculated to injure another [or] to deprive him of his property wrongfully" constitutes fraud under the mail fraud provision. Fasulo v. United States, 272 U.S. 620, 629 (1926). In Fasulo, the court stated that "broad as are the words 'to defraud,' they do not include threat and coercion through fear or force." Id. at 628. Instead, the Supreme Court placed emphasis on the central role of deception to the concept of fraud—"the words 'to defraud' ... primarily mean to cheat, ... usually signify the deprivation of something of value by trick, deceit, chicane, or overreaching, and ... do not extend to theft by violence, or to robbery or burglary." Id. at 627 (construing Hammerschmidt v. United States, 265 U.S. 182 (1924)).

3. Access Furthered the Intended Fraud

The defendant's illegal access of the protected computer must "further" a fraud. Accessing a computer without authorization—or, more often, exceeding authorized access—can further a fraud in several ways. For example:

- This element is met if a defendant alters or deletes records on a computer, and then receives something of value from an individual who relied on the accuracy of those altered or deleted records. In United States v. Butler, 16 Fed. Appx. 99 (4th Cir. 2001) (unpublished disposition), the defendant altered a credit reporting agency's records to improve the credit ratings of his coconspirators, who then used their improved credit rating to make purchases. In United States v. Sadolsky, 234 F.3d 938 (6th Cir. 2000), the defendant used

[5] The elements of common law fraud (1955)
[6] "scheme to defraud" (2001)

his employer's computer to credit amounts for returned merchandise to his personal credit card.

- This element is met if a defendant obtains information from a computer, and then later uses that information to commit fraud. For example, in United States v. Lindsley, 2001 WL 502832 (5th Cir. 2001) (unpublished), the defendant accessed a telephone company's computer without authorization, obtained calling card numbers, and then used those calling card numbers to make free long-distance telephone calls.

- This element is met if a defendant uses a computer to produce falsified documents which are later used to defraud. For example, in United States v. Bae, 250 F.3d 774 (D.C. Cir. 2001), the defendant used a lottery terminal to produce back-dated tickets with winning numbers, and then turned those tickets in to collect lottery prizes.

4. Obtains Anything of Value

This element is easily met if the defendant obtained money, cash, or a good or service with measurable value. Two more difficult cases arise when the defendant obtains only the use of a computer and when the defendant obtains only information.

Use of the computer as a thing of value

The statute recognizes that the use of a computer can constitute a thing of value, but this element is satisfied only if the value of such use is greater than $5,000 in any one-year period.

5. Statutory Penalties

A violation of section 1030(a)(4) is punishable by a fine and up to five years in prison, unless the individual has been previously convicted of a section 1030 offense, in which case the punishment increases to a maximum of ten years in prison. 18 U.S.C. § 1030(c)(3).

6. Relation to Other Statutes

In appropriate cases, prosecutors may also want to consider charges under the wire fraud statute, 18 U.S.C. § 1343, which requires proof of many elements similar to those needed for section 1030(a)(4). Unlike section 1030(a)(4), however, which is punishable by a maximum of 5 years in prison (assuming the defendant does not have other prior § 1030 convictions), wire fraud carries stiffer penalties and is punishable by a maximum of 20 years in prison, or 30 years if the violation affected a financial institution. Compare 18 U.S.C. § 1030(a)(3) with 18 U.S.C. § 1343.

2.1.F. Damaging a Computer or Information: 18 U.S.C. § 1030(a)(5)

Criminals can cause harm to computers in a wide variety of ways. For example, an intruder who gains unauthorized access to a computer can send commands that delete files or shut the computer down. Alternatively, intruders can initiate a "denial of service attack" that floods the victim computer with useless information and prevents legitimate users from accessing it. In a similar way, a virus or worm can use up all of the available communications bandwidth on a corporate network, making it unavailable to employees. In addition, when a virus or worm penetrates a computer's security, it can delete files, crash the computer, install malicious software, or do other things that impair the 30 Prosecuting Computer Crimes computer's integrity. Prosecutors can use section 1030(a)(5) to charge all of these different kinds of acts.

Section 1030(a)(5) criminalizes a variety of actions that cause computer systems to fail to operate as their owners would like them to operate. Damaging a computer can have far-reaching effects. For example, a business may not be able to operate if its computer system stops functioning or it may lose sales if it cannot retrieve the data in a database containing customer information. Similarly, if a computer that operates the phone system used by police and fire fighters stops functioning, people could be injured or die as a result of not receiving emergency services. Such damage to a computer can occur following a successful intrusion, but it may also occur in ways that do not involve the unauthorized access of a computer system.

Title 18, United State Code, Section 1030(a)(5) provides:

Whoever–

(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subsection (A), caused (or, in the case of an attempted offense, would, if completed, have caused)–

(i) loss to 1or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security ...

shall be punished as provided in subsection (c) of this section.

The differences between the conduct criminalized by the three subsections of section 1030(a)(5)(A) are important to note. That section criminalizes three different types of conduct, based on mental state and authority to access. In basic terms, subsection (5)(A)(i) prohibits anyone from knowingly damaging a computer (without authorization) while subsection (5)(A)(ii) prohibits unauthorized users from causing damage recklessly and subsection (5)(A)(iii) from causing damage negligently.

The latter two subsections require that the defendant "access" the computer without authorization. These criminal prohibitions hold intruders accountable for any damage they cause while intentionally trespassing on a computer, even if they did not intend to cause that damage. See S. Rep. No. 104-357, at 11 (1996), available at 1996 WL 492169 (noting that "anyone who knowingly invades a system without authority and causes significant loss to the victim should be punished ... even when the damage caused is not intentional").

By contrast, section 1030(a)(5)(A)(i) requires proof only of the knowing transmission of something to damage a computer without authorization. The government does not need to prove "access." Because it is possible to damage a computer without "accessing" it, this element is easier to prove (except for the mental state requirement). For example, most worms and Trojans spread though self-replication, without personally accessing the affected systems.

4. Penalties

Section 1030(a)(5)(A) sets forth three mental states for the causing of damage, with varying penalty levels for each. Where the individual acts intentionally, the maximum sentence is ten years' imprisonment. 18 U.S.C. § 1030(c)(4)(A). If the individual accesses a protected computer without authorization and recklessly causes damage under subsection (5)(A)(ii), the maximum sentence is five years in prison. 18 U.S.C. § 1030(c)(4)(B). In either case, if the offense follows a conviction for any crime under section 1030, the maximum sentence rises to 20 years' imprisonment. § 1030(c)(4)(C). If the attacker accesses a computer without authorization and causes damage with no culpable mental state (i.e., accidentally or negligently), the crime is a misdemeanor with a maximum penalty of one year imprisonment. 18 U.S.C. § 1030(c)(2)(A).

But, violations of section 1030(a)(5)(A)(iii) that follow a previous conviction under section 1030 result in a ten year maximum penalty. 18 U.S.C. § 1030(c)(3)(B).

In 2002, Congress added an additional sentencing provision that raised the maximum penalties for certain of these crimes that result in serious bodily injury or death. If the offender intentionally damages a protected computer under § 1030(a)(5)(A)(i) and "knowingly or recklessly causes or attempts to cause serious bodily injury," the maximum penalty rises to 20 years' imprisonment, 44Prosecuting Computer Crimes and where the offender knowingly or recklessly causes or attempts to cause death, the court may impose life in prison. See 18 U.S.C. § 1030(c)(5).

Table: Penalty Summary for Section 1030(a)(5)(A)Section

	Statutory Penalty
Intentional Damage § 1030(a)(5)(A)(i)	10-year felony 20-year felony for subsequent convictions or serious bodily injury Life imprisonment if offender causes or attempts to cause death
Reckless Damage § 1030(a)(5)(A)(ii)	5-year felony 20-year felony for subsequent convictions
Damage § 1030(a)(5)(A)(iii)	Misdemeanor 10-year felony for subsequent convictions

5. Relation to Other Statutes

In many cases, intruders cause damage to systems even though their primary intent is to steal information or commit a fraud in violation of sections 1030(a)(2) or (a)(4). For example, intruders commonly try to make it difficult for system administrators to detect them by erasing log files that show that they accessed the computer network. Deleting these files constitutes intentional "damage" for purposes of section 1030(a)(5). Similarly, intruders commonly modify system programs or install new programs to circumvent the computer's security so that they can access the computer again later. This activity impairs the integrity of the computer and its programs and therefore meets the damage requirement.

As long as the government can meet one of the other requirements under § 1030(a)(5)(B)—such as $5,000 in loss, or damage that affects a computer used in furtherance of the national defense—a charge under § 1030(a)(5) is appropriate in addition to any other charges under § 1030.

Prosecutors should also consider section 1030(a)(5) in cases where an individual breaks into a federal government computer in violation of § 1030(a)(3), a misdemeanor. If the act causes damage, as well as causes one of the enumerated harms, prosecutors may be able to charge one of the felony offenses in § 1030(a)(5).

When faced with conduct that damages a protected computer, prosecutors should also consider several other statutes that punish the same conduct when particular circumstances are present. For example, where the criminal act causes damage to a computer for communications that is "operated or controlled by the United States," or "used or intended to be used for military or civil defense functions," prosecutors should consider charging 18 U.S.C. § 1362, a ten-year felony. Other potentially applicable statutes are discussed in Chapter 3, "Other Network Crime Statutes."

2.1.G. Trafficking in Passwords: 18 U.S.C. § 1030(a)(6)

Section 1030(a)(6) prohibits a person from knowingly and with intent to defraud trafficking in computer passwords and similar information when the trafficking affects interstate or foreign commerce, or when the password may be used to access without authorization a computer used by or for the federal government. First offenses of this section are misdemeanors.

> *Title 18, United States Code, Section 1030(a)(6) provides:*
>
> *Whoever–*
>
> *(6) Knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if–*
>
> *(A) such trafficking affects interstate or foreign commerce;*

> *or*
> *(B) such computer is used by or for the Government of the United States ....*
>
> *shall be punished as provided in subsection (c) of this section.*

6. Penalties

Violations of section 1030(a)(6) are misdemeanors punishable by a fine or a one-year prison term for the first offense. See 18 U.S.C. § 1030(c)(2)(A). If the defendant has a previous conviction under section 1030, the maximum sentence increases to ten years' imprisonment. See 18 U.S.C. § 1030(c)(2)(C).

7. Relation to Other Statutes

Given the shared statutory definition, section 1030(a)(6) cases often overlap with access device cases under section 1029. Passwords are also access devices under section 1029. See, e.g., United States v. Fernandez, 1993 WL 88197 (S.D.N.Y. 1993) (holding that the plain meaning of the term "access device" covers "stolen and fraudulently obtained passwords which may be used to access computers to wrongfully obtain things of value"). For more information on section 1029, see Chapter 3, "Other Network Crime Statutes."

2.1.H. Threatening to Damage a Computer: 18 U.S.C. § 1030(a)(7)

Section 1030(a)(7), which prohibits extortion threats to damage a computer, is the high-tech variation of old-fashioned extortion. This section applies, for example, to situations in which intruders threaten to penetrate a system and encrypt or delete a database. Other scenarios might involve the threat of distributed denial of service attacks that would shut down the victim's computers. Section 1030(a)(7) enables the prosecution of modern-day extortionists who threaten to harm or damage computer networks—without causing physical damage—unless their demands are met.

Title 18, United States Code, Section 1030(a)(7) provides:
Whoever–

(7) With intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer ...

shall be punished as provided in subsection (c) of this section.

4. Penalties

A violation of section 1030(a)(7) is punishable by a fine and up to five years in prison. 18 U.S.C. § 1030(c)(3)(A). If the defendant has a previous conviction under section 1030, the maximum sentence increases to 10 years' imprisonment. 18 U.S.C. § 1030(c)(3)(B).

5. Relation to Other Statutes

The elements of section 1030(a)(7) generally parallel the elements of a Hobbs Act (18 U.S.C. § 1951, interference with commerce by extortion) violation with some important differences. First, the intent to extort from any person money or other thing of value is the same under section 1030(a)(7) and under section 1951. However, in contrast to section 1951, section 1030(a)(7) does not require proof that the defendant delayed or obstructed commerce. Proving that the threat was transmitted in interstate or foreign commerce is sufficient.

At least one case has recognized the similarities between the two statutes. In United States v. Ivanov, 175 F. Supp. 2d 367 (D. Conn. 2001), the defendant hacked into the victim's network and obtained root access to the victim's 1. Computer Fraud and Abuse Act 51 servers. He then proposed that the victim hire him as a "security expert" to prevent further security breaches, including the deletion of all of the files on the server. Without much discussion, the court determined that the analysis under section 1030(a)(7) was the same as that for the Hobbs Act. See id. at 372.

2.2. CONVENTION ON CYBER CRIME[7] Budapest, 23.11.2001

Salient articles are as under: -

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognizing the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

2.2.1. Article 2 . Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

2.2.2. Article 3 . Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic

[7]. Council of Europe (2001)

law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

2.2.3. Article 4 . Data interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

2.2.4. Article 5 . System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

2.2.5. Article 6 . Misuse of devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

   a the production, sale, procurement for use, import, distribution or otherwise making available of:

   i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

2.2.6. Article 7 . Computer-related forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

2.2.7. Article 8 . Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a. any input, alteration, deletion or suppression of computer data;

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

2.2.8. Article 12 . Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

   a. a power of representation of the legal person;

   b. an authority to take decisions on behalf of the legal person;

   c. an authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

2.2.9. Article 20 . Real-time collection of traffic data

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

   a. collect or record through the application of technical means on the territory of that
   Party, and

   b. compel a service provider, within its existing technical capability:

      i. to collect or record through the application of technical means on the territory of that Party; or

      ii. to co-operate and assist the competent authorities in the collection or recording of,

      traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

2.2.10. Article 23. General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2.2.11. Article 24. Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties,

including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

2.2.12. Article 25. General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

2.2.13. Article 32 . Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorization of another Party:

A access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

B access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

2.2.14. Article 33. Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

2.2.15. Article 34 . Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

2.2.16. Article 38 . Territorial application

1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.

2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.

[redacted]

2.3 MODELS FOR CYBER LEGISLATION IN ECONOMIC AND SOCIALCOMMISSION FOR WESTERN ASIA (ESCWA) MEMBER COUNTRIES[8]

2.3.1. MODELS FOR CYBER LEGISLATION

A review of national laws regulating the various legal aspects related to cyberspace, in addition to an analysis on the current status of relevant international conventions and agreements, revealed five main legal topics, namely: (a) data protection and processing, including privacy rights; (b) e-commerce; (c) e-transactions, including, for example, e-banking and e-payment; (d) cyber crime; and (e) intellectual property.

In the ESCWA region, the analysis revealed that, while cyber-related laws have been enacted in some countries, most still lack adequate and/or comprehensive cyber legislation. Within that context, the main topics for those member countries which have initiated such legislation relate to e-commerce, including e-signature, acceptance of e-documents and e-contracts; as well as to intellectual property issues, which are largely addressed under general copyright laws, rather than under specific cyber laws related to intellectual property.

This study analyses the status of cyber legislation of all the ESCWA members, namely: Bahrain, Egypt, Iraq, Jordan, Kuwait, Lebanon, Oman, Palestine, Qatar, Saudi Arabia, the Syrian Arab Republic, the United Arab Emirates and Yemen. A description of the current situation of cyber legislation in the ESCWA region is set forth below according to applicable national legislation in force, whether purely domestic or as decrees and regulations implementing international conventions and treaties related to

[8]. Models for Cyber Legislation (2007)

cyberspace. This study highlights the absence of cyber legislation through a presentation of the legal topics and corresponding laws for each ESCWA member country.

The analysis is based on a comparison with the relevant cyber topics and legal frameworks stated in corresponding laws in Europe, the United States of America and Asia; and with the articles of various international conventions regulating cyber crimes and related legal issues, including security of e-transactions, e-commerce, procedural law and e-signature. At the outset, the analysis detects the presence or absence of cyber legislation in each member country and, subsequently, examines whether the existing legislation is adequate and sufficiently comprehensive. Moreover, it defines the necessary mechanism for a legislative body to study and enact a domestic cyber law in such specified subjects as e-trade, e-banking and compute crime protection.

In order to gather the required information and statistics for this study, research was undertaken on the available cyber-related conventions and treaties and on existing cyber laws in the United States of America, member countries of the European Union (EU), Canada and Australia. The research led to the establishment of an index detailing the topics of cyber-related legal issues as treated in international conventions and national laws.

This chapter comprises the following three sections:

(a) Survey of legal texts, including international conventions, directives and treaties; and national laws of selected countries. The summary highlights the main topics of each reviewed convention, agreement and national law based on the list of indexed topics;

(b) Cyber legislation in the ESCWA region, including full legal texts and articles of laws on such cyber-related topics as e-commerce, consumer protection, intellectual property and e-transactions. Additionally, ratifications made by ESCWA member countries to international conventions are outlined;

(c) Analysis of current cyber or cyber-related legislation in the ESCWA region in terms of whether such laws are exhaustive for all topics, compared to international conventions and foreign cyber laws.

2.3.1.A. SURVEY OF LEGAL TEXTS

This survey comprises two major sections, namely: (a) international conventions, agreements and legal texts, including directives; and (b) national cyber or cyber-related laws of selected countries outside the ESCWA region.

1. *International conventions and agreements*

The reviewed conventions and agreements are set forth below, categorized by subject and according to the cyber-related legislation.

(a) *Cyber crime and the protection of computer systems and network*

In the area of cyber crime, the major legal texts consist of the following:

(i) Convention on Cybercrime, the Council of Europe Treaty No. 185 (Budapest, 23 November 2001): defines the main aspects and nature of cyber and computer crimes;

(ii) Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, Council of Europe Treaty No. 189 (Strasbourg, 28 January 2003): supplements the provisions of the Convention on Cybercrime regarding the criminalization of acts of a racist and xenophobic nature committed through computer systems.

(b) *Protection of personal data*

In the area of protection of personal data, the major legal texts consist of the following:

(i) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty No. 108 (Strasbourg, 28 January 1981), along with Amendments adopted by the Committee of Ministers in Strasbourg on 15 June 1999: aims to secure in the territory of each party and for every individual, irrespective of nationality or residence, respect for rights and fundamental freedoms and, in particular, the right to privacy with regard to automatic processing of personal data;

(ii) Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding Supervisory Authorities and Trans-border Data Flows (Strasbourg, 8 November 2001);

(iii) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data: obliges signatories to enact legislation concerning the automatic processing of personal data in order to protect the privacy of such personal data;

(iv) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications): complements Directive 95/46/EC and harmonizes the provisions required to ensure an equivalent level of protection of fundamental rights and freedoms and, in particular, the right to privacy with respect to the processing of personal data in the electronic communications sector and to ensure the free movement of such data and of electronic communications equipment and services in the EU;

(c) *Electronic communications*

In the area of electronic communications, the major legal texts consist of the following:

(i) Draft declaration on freedom of communication on the Internet (Strasbourg, 8 April 2002);

(ii) Community-COST Concertation Agreement on a Concerted Action Project in the Field of Tele informatics (COST project 11 bis, 1980);

(iii) Guidelines for the Regulation of Computerized Personal Data Files, adopted by General Assembly resolution 45/95 of 14 December 1990;

(iv) Bucharest Declaration on Combating Counterfeiting and Piracy (12 July 2006);

(v) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications);

(iv) Cooperation Agreement between the European Economic Community and the Kingdom of Sweden on the Interconnection of the Community Network for Data Transmission (Euronet) and the Swedish Data Network for Information-Retrieval Purposes (14 December 1981).

(d) *Computer programs*

In the area of computer programs, the major legal texts consist of the following:

(i) Organization for Economic Co-operation and Development (OECD) Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (25 July 2002);
(ii) Directive 91/250/EEC of 14 May 1991 on the Legal Protection of Computer Programs;
(iii) Council Resolution 96/C 376/01 of 21 November 1996 on new Policy Priorities regarding the Information Society;
(iv) Council Framework Decision 2005/222/JHA of 24 February 2005 on Combating Attacks against Information Systems;
(v) Interpol Information Technology (IT) Security and Crime Prevention Methods.

(e) *E-commerce*

In the area of e-commerce, the major legal texts consist of the following:

(i) Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures;
(ii) United Nations Commission on International Trade Law (UNCITRAL): Recommendation on the Legal Value of Computer Records (1985);
(iii) United Nations Convention on the Use of Electronic Communications in International Contracts, adopted by the General Assembly on 23 November 2005;
(iv) Community-COST Concertation Agreement on a Concerted Action Project in the Field of Tele informatics (COST project 11 bis, 1980);
(v) Treaty Establishing the European Community (Nice Consolidated Version, 1 January 1958)

2. National cyber or cyber-related laws of selected countries outside the ESCWA region

Title
Belgium
Loi visant à transposer certaines dispositions de la directive services financiers à distance et de la directive vie privée et communications électroniques
Loi transposant en droit belge la Directive européenne 2001/29/CE du 22 mai 2001 sur l'harmonisation de
certains aspects du droit d'auteur et des droits voisins dans la société de l'information
La nouvelle loi belge sur le commerce électronique
Loi modifiant le Code de la taxe sur la valeur ajoutée (facture

électronique)
Loi sur certains aspects juridiques des services de la société de l'information
Arrêté royal visant à réglementer l'envoi de publicités par courrier électronique
Loi relative aux opérations effectuées au moyen d'instruments de transfert électronique de fonds
Projet de loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification
Arrêté royal organisant le contrôle et l'accréditation des prestataires de service de certification qui délivrent des certificats qualifiés
Signature électronique et les services de certification
France
Loi no 2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information
Décret n° 2005-1450 du 25 novembre 2005 relatif à la commercialisation à distance de services financiers auprès des consommateurs
Title
Loi du 21 Juin 2004 pour la confiance dans l'économie numérique
Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation
Loi no 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés
Règlement no 2002-13 relatif à la monnaie électronique et aux établissements de monnaie électronique
Loi no 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
Code Pénal Articles 226-16 à 24
Luxemburg
Règlement grand-ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité "commerce électronique"
Germany
Federal Data Protection Act of 20 December 1990 (BGBl.I 1990 S.2954), amended by law of 14 September 1994 (BGBl. I S. 2325)
Sweden
Personal Data Act (1998:204) of 29 April 1998
Switzerland
Ordonnance sur la conduite de la guerre électronique
Loi Fédérale sur les services de certification dans le domaine de la signature électronique No. 943.03
Swiss Informatics Society Code of Ethics
Romania
Anti-Corruption Law Title III on Preventing and Fighting Cyber Crime

Canada
Electronic Information and Documents Act, 2000 (Saskatchewan)
Some computer-related offences found in the 1998 Criminal Code of Canada
Personal Information Protection and Electronic Documents Act, 2000
Electronic Commerce Act (Newfoundland)
Electronic Transactions Act (Manitoba)
Electronic Transactions Act (Alberta)
Electronic Commerce Act (Yukon)
Electronic Commerce Act (Prince Edward Island)
Electronic Commerce Act (Ontario)
Electronic Commerce Act (Nova Scotia)
United States of America
Computer Security Act of 1987
Uniform Electronic Transactions Act
The Privacy Act of 1974 5 U.S.C. 552a
Electronic Signatures in Global and National Commerce Act (E-SIGN), at 15 U.S.C. 7001
United States Code Annotated Title 18: Crimes and Criminal Procedure Part I - Crimes, Chapter 47: Fraud and False Statements 1029. Fraud and related activity in connection with access devices
United States Code Annotated Title 18: Crimes and Criminal Procedure Part I - Crimes, Chapter 47: Fraud and False Statements 1030. Fraud and related activity in connection with computers
United States Code Annotated Title 18: Crimes and Criminal Procedure Part I - Crimes, Chapter 65: Malicious Mischief 1362. Communication lines, stations or systems
United States Code Annotated Title 18: Crimes and Criminal Procedure Part I - Crimes, Chapter 119: Wire and Electronic Communications Interception and Interception of Oral Communications 2510. Definitions
Title
United States Code Annotated Title 18: Crimes and Criminal Procedure Part I - Crimes, Chapter 121: Stored Wire and Electronic Communications and Transactional Records Access 2701. Unlawful access to stored communications
United States Code Annotated Title 18: Crimes and Criminal Procedure Part II - Criminal Procedure, Chapter 206: Pen Registers and Trap and Trace Devices
Provisions of Section 225 ("Cyber Security Enhancement Act") of the Homeland Security Act of 2002, amending Title 18 of the United States Code
Field guidance on new authorities that relate to computer crime and electronic evidence enacted in the United States Patriot Act of 2001
No Electronic Theft ("NET") Act
Anti-cyber squatting Consumer Protection Act
Act to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the

Internet
United Kingdom of Great Britain and Northern Ireland
Data Protection Act 1998
Computer Misuse Act 1990
Electronic Communications Act 2000
European Union
Council Resolution of 15 July 1974 on the Community Policy on Data Processing
Recommendation No R (85) 10 adopted on 28 June 1985 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications
Recommendation No (87) 15 adopted on 17 September 1987 concerning the regulating of the use of personal data in the police sector
Commission Recommendation 87/598/EEC of 8 December 1987 concerning a European code of conduct relating to electronic payments [Official Journal L 365 of 24.12.1987]
Recommendation No (88) 2 on piracy in the field of copyright and neighboring rights adopted on 18 January 1988
Recommendation No (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes adopted on 13 September 1989
Council Decision 92/242/EEC of 31 March 1992 in the Field of Information Security
European Commission Green Paper of 27 July 1995 on Copyright and Related Rights in the Information Society [COM(95) 382 final - not published in the Official Journal]
European Parliament and Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data [Official Journal L281 of 23 November 1995]
Recommendation No (95) 13 adopted on 11 September 1995 concerning problems of criminal procedural law connected with information technology
Council Resolution of 21 November 1996 on New Policy-Priorities Regarding the Information Society(96/C 376/01)
Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases
Commission Communication of 18 April 1997: A European Initiative in the Sector of Electronic Commerce
Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the Protection of Consumers in Respect of Distance Contracts
Commission Recommendation 97/489/EC of 30 July 1997 on Transactions by Electronic Payment Instruments and in Particular the Relationship Between Issuer and Holder
Directive 97/55/EC of the European Parliament and of the Council of 6 October 1997 amending Directive 84/450/EEC concerning Misleading Advertising so as to Include Comparative Advertising

Directive 97/66/EC on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector
Title
Communication from the Commission of 11 April 2000 to the Council and the European Parliament, entitled "The Organization and Management of the Internet", International and European Policy Issues1998-2000 [COM(2000) 202 final - not published in the Official Journal]
Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 Laying Down a Procedure for the Provision of Information in the Field of Technical Standards and Regulations
Directive 1999/93/EC on a Community framework for electronic signatures
Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market (Directive on Electronic Commerce)
Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society
Regulation (CE) No 45/2001 of the European Parliament and of the Council of 18 December 2001 on the Protection of Individuals with regard to the Processing of Personal Data by the Institutions and Bodies of the Community and on the Free Movement of Such Data
The Electronic Commerce (EC Directive) Regulations 2002 of 30 July 2002
Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications)
Communication from the Commission of 22 January 2004 on Unsolicited Commercial Communications or "spam" [COM(2004) 28 final - not published in the Official Journal]
Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 Establishing the European Network and Information Security Agency
Council Framework Decision 2005/222/JHA of 24 February 2005 on Attacks Against Information Systems
Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 Establishing a Multiannual Community Programme on Promoting Safer Use of the Internet and New Online Technologies
Communication from the Commission of 31 May 2006: A Strategy for a Secure Information Society – Dialogue, Partnership and Empowerment [COM(2006) 251 final – not published in the Official Journal]
United Nations entities
56/80 Model Law on Electronic Signatures adopted by UNCITRAL
51/162 Model Law on Electronic Commerce adopted by UNCITRAL
United Nations Manual on the Prevention and Control of Computer-Related Crime
Xxx Ref see note to author division Recommendation of the UN 15th conference - criminal law related to computer crimes (Rio de Janeiro,

Brazil, 4-9 October 1994)
Model Law on Electronic Commerce with Guide to Enactment adopted by UNCITRAL
Global
IT Security and Crime Prevention Methods
Association of South East Asian Nations (ASEAN)
Malaysia
Computer Crimes Act 1997
Digital Signature Regulations 1998
Singapore
Electronic Transactions Act 1998

2.31.B. CYBER LEGISLATION IN THE ESCWA REGION

The translations of the Arabic legal texts set forth below are for the purpose of this study and are not to be considered official translations (see annex II for the Arabic version of these texts).

1. *Bahrain*

In Bahrain, the major legal texts consist of the following:

(a) E-Commerce Law of 14 September 2002 and the amendments of article 21 thereof by Law No. 13 of 2006;

(b) Decree No. 9 of 12 January 2003 on the creation of a central data centre;

(c) Decree No. 28 of 2002 on electronic transactions;

(d) Law of Telecommunications No. 48 of 2002;

(e) Executive Decision No. 25 of 9 July 2005 on the establishment and formation of the Higher Committee for Information Technology and Telecommunications;

(f) Ministerial Decision No. 2 of 19 June 2006 on technical aspects accepted by official bodies for electronic transactions;

(g) Decision No. 3 of 21 January 2001 concerning the formation of a committee regulating the e-commerce;

(h) Law No. 22 of 25 June 2006 on copyright and neighboring rights, whose implementing regulations have not yet been issued, annulled the Copyright Law No. 10 of 1993.

2. *Egypt*

In Egypt, the major legal texts consist of the following:

(a) E-Signature Law of 21 April 2004;

(b) Telecommunications Law No. 10 of 2003;

(c) Law No. 82 of 2 June 2002 on intellectual property pertaining to trademarks, commercial data, geographical indications, patents of invention, utility models, layout designs of integrated circuits, undisclosed information, industrial designs and models, copyright and related rights and plant varieties. The implementing regulations related to copyright and related rights of the Law were issued as a ministerial decree on 14 April 2005;

(d) Decree No. 327 of 2005 on establishing a division for the combating of computer and Internet crimes;

3. *Iraq*

In Iraq, cyber laws or amendments to existing laws concerning cyber-related legal aspects have not been enacted.

4. *Jordan*

In Jordan, the major legal texts consist of the following:

(a) E-Transactions Law No. 85 of 2001;

(b) Temporary law of 2003 on applying IT resources in government entities;

(c) Copyright Law No. 22 of 1992 and its amendments of 1998, 1999 and 2005 governing the protection of copyright and related rights in Jordan.

5. *Kuwait*

In Kuwait, the major legal texts consist of a draft law on e-commerce, which is in the process of enactment; and Copyright Law No. 5 of 1999 on the protection of copyright for material published in all media.

6. *Lebanon*

(a) *Intellectual property*

In the area of intellectual property, the major legal texts consist of the following:

(i) Artistic and Literary Ownership Law No. 75, enacted on 3 April 1999 and entered into force on 6 June 1999, governs copyright protection;

(ii) Ministerial Directive No. 4 of 25 May 2006 on the protection of computer programs and combating piracy in Lebanon.

(b) *Consumer protection*

In the area of consumer protection, the draft law on consumer protection was established by Decree No. 13068 of 5 August 2004, which was approved as amended by the joint parliamentary committees and the Parliament.

(c) *E-commerce (e-banking)*

In the area of e-commerce (e-banking), the major legal texts consist of the following:

(i) Monetary and Credit Law of 1 August 1963, articles 33, 70, 80 and 174;

(ii) Law No. 133 of 26 October 1999 appointing the Central Bank regulator for credit cards and e-transactions. The enacted regulations concerning e-transactions are applicable through a decision issued on 30 March 2000 by the Central Bank;

(iii) Circulars issued by the Central Bank concerning e-payments and use of magnetic cards are as follows: (a) "Electronic banking" of 23 December 2005; (b) "Electronic banking and financial transactions" of 3 July 2003; (c) "ATMs and credit cards" of 26 August 2002; (d) "Electronic clearing house for credit cards and payment cards and debit cards issued in the Lebanese market and used on ATMs" of 24 January 2003; and (e) "List of credit cards used in Lebanon" of 7 November 2002.

(d) *Money laundering*

In the area of combating money laundering, the major legal texts consist of the following:

(i) Law No. 318 of 20 April 2001 (Combating Money Laundering);

(ii) Circular No. 7818 of 18 May 2001 concerning the supervision of banking and financial operations in order to combat money laundering;

(iii) Circular No. 7299 of 10 June 1999 concerning ATM and payment cards (debit and credit);

(iv) Procedure amendments to civil and criminal procedure codes to comply with e-commerce and cyber crime prevention and prosecution needs.

(e) *E-commerce and e-transactions*

In the area of e-commerce and e-transactions, a new draft law was tendered to the Legislative Committee of the Parliament and a study thereof is still underway.

7. *Oman*

In Oman, the major legal texts consist of the following:

(a) Sultanate Decree No. 72 on money laundering, articles 2 and 5 thereof;

(b) The Copyright Law, issued by Royal Decree No.37/2000 of 21 May 2000, became effective on 3 June 2000.

8. *Palestine*

In Palestine, the major legal texts consist of the following:

(a) Draft law concerning the country code top-level domain name (ccTLD) for Palestine, namely, ".ps" that will soon be enacted;

(b) Civil and Commercial Procedure Law No. 4 of 2001, including article 19 thereof on the proof of e-signature;

(c) Law No. 12 of 2004 on financial securities and article 26 thereof on e-signatures having the same validity as written signatures;

(d) Executive Decision No. 35 of 2004 by the Council of Ministers on accessing the Internet through a Government computer centre;

(e) Executive Decision No. 39 of 2004 by the Council of Ministers and annexed to Arbitration Law No. 3 of 2000, including article 19 thereof on the validity of contracts executed through electronic mail;

(f) Executive Decision No. 74 of 2005 by the Council of Ministers on a national strategy for telecommunications and information technology;

(g) Executive Decision No. 269 of 2005 by the Council of Ministers on general policies of the use on the computer and Internet in official institutions;

(h) Executive Decision No. 65 of 2005 by the Council of Ministers on the adoption of the E-Palestine Initiative.

9. *Qatar*

In Qatar, the major legal texts consist of the following:

(a) Draft law on cyber crime to be enacted soon;

(b) Telecommunications Law No. 34 of 2006;

(c) Copyright Law No. 25 of 22 July and published in the Official Gazette No. 14 of 12 August 1995. The implementing regulations have not yet been issued, thereby delaying the implementation of the Law.

10. *Saudi Arabia*

In Saudi Arabia, the major legal texts consist of the following:

(a) Telecommunications Law of 2001;

(b) Completed draft laws on e-transactions and cyber crimes, expected to be enacted in the near term;

(c) Ministerial Decision No. 6667 concerning the conditions for practicing IT and telecommunications counseling;

(d) Copyright Law issued as per the Royal Decree No. M/41 of 30 August 2003 and published in the Official Gazette No. 3959 of 19 September 2003. The implementing regulations of the Law were published in the Official Gazette of 4 June 2004 and entered into force on 2 August 2004.

11. *Syrian Arab Republic*

Cyber laws or amendments to existing laws concerning cyber-related legal aspects have not been enacted in the Syrian Arab Republic. However, a draft law on e-signature has been presented to the Council of Ministers for adoption.

Copyright protection in the Syrian Arab Republic is governed by Law No. 12 of 2001. While the Syrian Copyright Protection Department (CPD) has started to process copyright applications, official fees have yet to be set.

12. *United Arab Emirates*

In the United Arab Emirates, the major legal texts consist of the following:

(a) Federal Law No. 2 of 2006 on combating information technology crimes;

(b) Law No. 2 of 2002 on e-commerce and e-transactions (Dubai);

(c) Free Zone Law of Technology, E-Commerce and Information of 2000 (Dubai);

(d) Customs Law of 1998, including articles 4, 24 and 118 on the validity of documents and information received electronically;

(e) Law No. 1 of 2007, issued by the Dubai International Financial Center (DIFC), and Data Protection Law 2001, which is applicable in the jurisdiction of DIFC;

(f) Copyright and Authorship Protection Law No. 7 of 2002.

13. *Yemen*

In Yemen, the major legal texts consist of the following:

(a) Law No. 40 of 28 December 2006 concerning e-payment, e-banking and financial operations, e-contract and e-signature;

(b) Press Law No. 20 of 1991;

(c) Law No. 19 of 1994 on intellectual property rights (IPRs) whose stipulated protection for copyright has been delayed by the non-issuance of the implementing regulations.

2.3.1.C. ANALYSIS OF CURRENT CYBER OR CYBER-RELATED LEGISLATION IN THE ESCWA REGION

Generally, cyber or cyber-related legislation in the ESCWA region is either rudimentary or incomplete. There are wide disparities between the countries of the ESCWA region concerning the enactment of cyber laws. Specifically, while some countries, including Bahrain and the United Arab Emirates, have already introduced several cyber laws, others are still at the stage of reviewing drafts or drawing up legal texts.

However, most ESCWA member countries have acknowledged the importance of regulating cyberspace and the use of computer systems and the Internet. This fact can be ascertained by various e-government and draft legislation efforts undertaken across the region.

The comparison of international conventions, treaties and foreign local cyber or cyber-related laws with those enacted in the ESCWA region revealed a number of issues that are set forth below.

1. *Data protection and privacy rights*

Inadequate or non-existent disclosure control mechanisms represent the main cause for privacy problems, particularly because uniquely identifiable data related to a person or persons can be collected and stored in a digital format. Generally, the main types of data affected by data privacy issues relate to the following: health information, criminal justice, financial information, genetic information and location information.

The legal protection of the right to privacy in general, and of data privacy in particular, varies greatly across the world.

Article 12 of the Universal Declaration of Human Rights states that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"[9].

The protection of privacy rights has necessitated that personal data stored or transferred using a computer or computer systems and networks must be regulated and protected through legal texts and directives.

At the international level, several conventions and directives have been promulgated and ratified by many countries in order to protect personal data, thereby protecting privacy rights. For example, EU has enacted conventions and directives that are applicable in its member countries and whose contents are included in their local laws. Within the framework of those directives and legal texts, EU addressed various issues, including the quality of the data to be processed and the criteria for making data processing legitimate, and the protection of such data against illegal disclosure or dissemination. Prominent among those directives and conventions are the following: (a) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications); and (b) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data.

The United States of America has a different perspective with regard to privacy rights, given that the regulation thereof sometimes contradicts the First Amendment on freedom of speech. Federal laws,

[9] The Universal Declaration of Human Rights.

including the Privacy Act of 1974, stipulate the conditions for the disclosure of records and the access thereto.

In order to comply with European regulations on data protection and privacy rights, the Department of Commerce in the United States has provided for a "safe harbor arrangement" whereby United States companies are compelled to comply with EU Directive 95/46/EC on the protection of personal data when dealing with their European counterparts.

Moreover, EU member countries have integrated the main principles for the protection and processing of personal data in their local laws. In addition, some EU regulations stipulate the protection of individuals with regard to the processing of personal data by EU institutions and bodies and on the free movement of such data.

In the United Kingdom of Great Britain and Northern Ireland, for example, the Data Protection Act of 1998 stipulates eight principles that are mandatory to the processing of personal data. According to the Protection Act, data must be fairly and lawfully processed; processed for limited purposes; adequate, relevant and not excessive; accurate; not kept longer than necessary; processed in accordance with the rights of the data subject; secure; and not transferred to countries without adequate protection.

The same principles were adopted in France under Law No. 78 of 17 January 1978 concerning freedom and data protection. Additionally, the Penal Code in France stipulates penalties for offences and infractions made against personal data, including imprisonment for up to five years and fines reaching 300,000 Euros. The Penal Code also criminalizes offences caused by negligence or failing to apply to the measures for adequate protection or processing of data.

Similarly, Sweden issued the Personal Data Act (1998:204) on 29 April 1998, which fully complies with the principles for data protection and processing as set by EU Directive 95/46/EC on the protection of personal data.

Consequently, the international protection for data processing in automatic or semi-automatic systems follows the principles established by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe Treaty No. 108 (Strasbourg, 28 January 1981), by which the quality of the data to be automatically processed must have the following attributes: "(a) be obtained and processed fairly and lawfully; (b) be stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) be adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) be accurate and, where necessary, kept up to date; (e) be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored".

In the Arab region in general, and in the ESCWA region in particular, there is still an absence of specific and adequate laws protecting data processing and privacy rights. While some articles exist in national laws, these relate mainly to civil status, statistics or storing banking information. Data protection legislation is still lacking in many countries of the ESCWA region. In Tunisia, by contrast, chapter 6 of the E-Commerce and E-Transactions Law includes provisions to protect personal data. Other North African Arab countries, including Algeria and Morocco, have also applicable laws relating to the protection of data. Against that background, the status of ESCWA member countries is summarized below.

(a) *Bahrain*: Existing cyber laws are silent on data protection and processing, and there is no evidence of a new draft being prepared or studied;

(b) *Egypt*: Article 2 of the Telecommunications Law No. 10 of 2003 defines the telecommunications service based on such principles as data being made public and rights of users being safeguarded. There is no evidence of other legislation concerning the protection or the processing of data;

(c) *Iraq*: There is no evidence of legal provisions concerning data protection or processing;

(d) *Jordan*: The E-Transactions Law is silent on data protection. While the temporary Law of 2003 concerns applying IT resources in Government entities, it is similarly silent regarding data protection. There is no evidence of a new draft being prepared or studied;

(e) *Kuwait*: There is no evidence of any legal provisions concerning data protection or processing;

(f) *Lebanon*: There is no legislation concerning data protection and processing. While the draft law on e-commerce and e-transactions included a chapter dealing with the protection of data processing, it is now in Parliament pending further study and possible amendments prior to enactment;

(g) *Oman*: There is no evidence of applicable laws or provisions concerning data protection and processing, nor of legislation being prepared or studied;

(h) *Palestine*: There is no evidence of legal provisions concerning data protection or processing;

(i) *Qatar*: Existing cyber laws are silent on data protection. Article 35 of the earlier Telecommunications Law issued in 1987 defined the restrictions on receiving telecoms messages or signals not intended for the recipient or, if received unintentionally, the prohibition of keeping or disseminating such messages or signals. However, the new Telecommunications Law of 2006 Decree No. 34 represents a substantial progress in this field, stipulating, in articles 50 and 52, restrictions concerning consumer protection and data protection. Moreover, article 50 prohibits service providers from using consumer information to make unsolicited advertising; and article 52 prohibits service providers from breaching privacy rights of clients and to protect and safely store the collected client data.9 Article 52 is partially compliant with the provisions of EU Directive 95/46/EC on the protection of personal data regarding the principles of processing and protecting data. The search did not reveal a new draft being prepared or studied;

(j) ***Saudi Arabia***: There is no evidence of legal provisions concerning data protection or processing;

(k) ***Syrian Arab Republic***: There is no evidence of legal provisions concerning data protection or processing;

(l) ***United Arab Emirates:*** The Data Protection Law of January 2007 applies in the jurisdiction of the Dubai International Financial Centre (DIFC) and articles 8 and 10 thereof protect the processing of personal and sensitive data in line with EU and OECD directives. The Law specifies personal data as any information relating to an identifiable natural person; and sensitive personal data as revealing or concerning, directly or indirectly, racial or ethnic origin, communal original, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life;

(m) *Yemen*: There is no evidence of legal provisions concerning data protection or processing.

Box 1. The main provisions of the Dubai International Financial Centre Authority Data Protection Law of 2007

General requirements

Data Controllers must ensure that the Personal Data that they Process is:

- Processed fairly, lawfully and securely;
- Processed for specified, explicit and legitimate purposes in accordance with the Data Subject's rights and not
- further Processed in a way incompatible with those purposes or rights;
- Adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed;
- Accurate and, where necessary, kept up to date; and
- Kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data was collected or for which they are further Processed.

Every reasonable step must be taken by Data Controllers to ensure that Personal Data which is inaccurate or incomplete, having regard to the purposes for which it was collected or for which it is further Processed, is erased or rectified.

Processing of sensitive personal data

Sensitive Personal Data shall not be Processed unless:

- The Data Subject has given his written consent to the Processing of that Sensitive Personal Data;
- Processing is necessary for the purposes of carrying out the obligations and specific rights of the Data Controller;
- Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his consent;
- Processing is carried out in the course of its legitimate activities with

appropriate guarantees by a foundation, association or any other non-profit-seeking body on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the Personal Data are not disclosed to a Third Party without the consent of the Data Subjects;

- The Processing relates to Personal Data which are manifestly made public by the Data Subject or is necessary for the establishment, exercise or defence of legal claims;

- Processing is necessary for compliance with any regulatory or legal obligation to which the Data Controller is subject;

- Processing is necessary to uphold the legitimate interests of the Data Controller recognized in the international financial markets, provided that such is pursued in accordance with international financial standards and except where such interests are overridden by compelling legitimate interests of the Data Subject relating to the Data Subject's particular situation;

- Processing is necessary to comply with any regulatory requirements, auditing, accounting, anti-money laundering or counter terrorist financing obligations or the prevention or detection of any crime that apply to a Data Controller;

- Processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Personal Data is Processed by a health professional subject under national laws or regulations established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy;

- Processing is required for protecting members of the public against: (a) financial loss arising from dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, management consultancy, IT services, accounting or other commercial activities (either in person or indirectly by means of outsourcing); (b) dishonesty, malpractice or other seriously improper conduct by, or the unfitness or incompetence of, persons concerned in the provision of banking, insurance, investment, financial or other services;

- Authorized in writing by the Commissioner of Data Protection.

In subsequent articles, the Law stipulates the rules to follow when applying for data transfers outside the DIFC jurisdiction with adequate level of protection or with the absence of adequate levels of protection. Moreover, the Law provides, in part 3 thereof, the rights of Data Subjects to perform the following:

- To access and rectify, erase or block Personal Data;
- To object to processing.

The Law is considered complete in terms of protecting personal data and provides for safe use and processing regulations inside DIFC.

2. ***Protection of privacy and freedom of information in the electronic communications sector***

Despite the consensus that the right to privacy is a fundamental one, it is not always respected online. Several countries have introduced legislation addressing the illegal collection, storage, modification, disclosure or dissemination of personal data, and interference in communications of private bodies and persons.

The countries of the ESCWA region lack adequate laws and regulations with regard to privacy and freedom of information. The only issue addressed is the protection of communication in various telecommunications laws across the region, including, for example, Egypt. Other provisions for the protection of privacy may be found in penal codes.

With the notable exception of the Data Protection Law of 2007 of Dubai in the United Arab Emirates, there is no evidence of any law that specifically mentions privacy protection online or in the electronic communications sector in the ESCWA region.

Box 3. Country code top-level domain names (ccTLD)

All ESCWA member countries have ccTLD registers that accredit the granting of the domain name. However, the ESCWA region still lacks provisions for domain name disputes. In Lebanon, for example, the Lebanese Domain Registry(LBDR) requests that any applicant for an ".lb" domain name must first apply to register the root domain (in the form"www.abcdefgh.com.lb"). The LBDR validates the relevant ccTLD as long as the corresponding trademark is valid. Hence, a dispute over the domain name can be litigated as a trademark infringement lawsuit before the court.

5. *E-transactions, e-commerce and related fields*

The major aspects of e-transactions are the validation and acceptance of the source that delivers an electronic document and of the content of such a document, as well as the authentication, validation and acceptance of e-signature.

The need to prove the authenticity of an electronic document is a major aim for legislators across the world, given that electronic documents represent the main tool for e-business in general, and for procedural legal requirements when two contracting parties, or sender and a receiver of electronic records, are dealing with each other over distance. The need to accept the validity of an electronic contract or document was aimed at facilitating commerce, especially in the light of the substantial growth in distance trading.

The legal aspects pertaining to e-transactions and e-commerce in countries outside the ESCWA region are summarized below.

In the United Kingdom, the Electronic Communications Act 2000 stipulates the provisions concerning the facilitation, among others, of electronic commerce and data storage. Under article 7 of that Law, the United Kingdom acknowledges as proof the legal power of an e-signature and the certification thereof, and the acceptance of such to admit the authenticity of the signed record or communication.

In the United States, one of the applicable laws in relation to e-signature is the Uniform Electronic Transactions Act (UETA), whose scope is inherently limited by the fact that it only applies to transactions related to business, commercial and consumer, and governmental matters. Consequently, transactions with no relation to the above-mentioned are not subject to this Act.

Moreover, the Electronic Signatures in Global and National Commerce Act (E-SIGN) regulates the activity of certificate authorities and sets the conditions for the practical application of digital signatures. However, E-SIGN does not correspond to the recommendations of the World Trade Organization (WTO), UNCITRAL and other influential organizations; and digital signature systems described therein are incompatible with international standards. For that reason, the Law will be amended to simplify the procedure of digital signatures.

In EU, article 5 of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures states that member countries "shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings". Moreover, member countries "shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is: in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification-service-provider, or not created by a secure-signature-creation device".

The above article has set the base for European countries to amend or enact their related laws to follow similar principles. Examples include the Law of Electronic Signature in Switzerland, which defines the provisions for identifying the legal evidential power of e-signature, the rules to accept a signature, namely, certification and authentication thereof, and the rules to determine which authentication bodies or service providers have the authority to certify such authenticity; and the Signature Law of 2001 in Belgium, which stipulates the rules of the certification of service providers.

In countries of the ASEAN region, including Malaysia and Singapore, e-transaction laws have also been enacted and the topics treated therein are mainly the same as in international conventions and European countries. In Singapore, the Electronic Transactions Act of 1998 has elaborate articles concerning, among others, the recognition of foreign certification authorities, the revocation of certificates and the revocation without the consent of subscribers.

A glance at the e-commerce legislation in the ESCWA region reveals that those countries that have an applicable and applied law on e-commerce typically include the following legal topics: (a) electronic contracting at distance; (b) e-signature; (c) acceptance of e-documents (e-proof); and (d) e-banking and monetary transactions (e-transactions and e-payment). Other related e-commerce issues, including publicity over the Internet, are either mentioned in consumer protection laws or in other related legislations.

The countries of the ESCWA region that have applicable legislation in that area are set forth below:

(a)*Bahrain*: Law No. 28/2002 concerning electronic transactions stipulates provisions relating to e-signature, e-proof and accepting e-documents in transactions in general. Saving or keeping a document can be in an electronic form, and the Law recognizes the validity of the kept document in the electronic form. Moreover, the Law considers that e-documents have the same evidential power as written documents.

Article 6 recognizes the validity of e-signature as having an evidential power of expressing the will of the signatory on the signed document; articles 10 and 11 stipulate e-contract acceptance of expressing the consent and the execution of the content of the contract when such consent is sent and received in an electronic form; and article 12 defines the conditions of e-contracts in both business-to-consumer (B2C) and business-to-business (B2B) forms.

Summarizing the contents, the Law stipulates the acceptance of the following: (i) electronic forms when dealing between parties and the conditions for public entities to accept electronic forms and dealing; (ii) the evidential power of electronic records, being the same as for the written records; (iii) e-signature; (iv) electronic records as original ones, under the conditions stipulated in article 7 thereof; (v) saving and keeping the electronic documents and records; and (vi) e-contract;

(b) *Egypt*: Article 14 of the Law on E-Signature provides e-signatures with the same evidential legal power as written signatures in civil, commercial and administrative matters. Moreover, the acceptance of the e-signature and writing is confirmed; and hence, the legal evidential power is accepted to an e-signature and e-document in general when the signature relates to the signatory. The Law also specifies the terms for electronic certification processes and provides for penal sanctions of imprisonment and fines for offences of certification;

(c) *Iraq*: There is no evidence of legal provisions concerning e-transactions or e-commerce;

(d) *Jordan*: The E-Transactions Law No. 85 of 2001 applies to electronic transactions, electronic records, electronic signatures and any electronic data messages. In the area of electronic records, the Law stipulates the following:

(i) Electronic transactions are approved by any government department or official institution, entirely or partially;

(ii) The electronic record will fulfill its evidential weight, including its original form character, if it fulfills the following conditions: a. the information stated in the record can be retained and stored in a manner whereby it may be referred to at any time; b. the possibility of retaining the electronic record in the form it had been generated, sent, received, or in any form that may prove that it accurately represents the information stated in the record during its generation, sending or receiving; and c. the information stated in the record is enough to verify its origin, receiving party, and date and time of transmittal and receipt.

Chapter 4 of the Law stipulates provisions relating to transferable electronic documents and defines those as being electronic documents to which the conditions of a negotiable bond shall apply; chapter 5 stipulates provisions relating to the electronic transfer of funds; and chapter 6 stipulates provisions relating to authentication and electronic signatures.

Article 31 of the Law recognizes the validity of an e-signature with the following provisos: (i) it is distinguishable and unique in its connection to the pertinent person; (ii) it is sufficient to identify its owner; (iii) it is generated in a manner or means specific to that person and under his control; and (iv) it is connected to the record related to him in a way that does not allow modification to that record after signing such without altering the signature. The Law is silent concerning other issues related to e-commerce;

(e) *Kuwait*: While there is no applicable legislation on e-commerce, a new draft law is pending enactment by Parliament. This draft, entitled the e-commerce law, stipulates the following main topics: (i) legal acknowledgment of e-documents; (ii) recognition of the validity and evidential power of e-signatures; (iii) acknowledgment of an e-document as an original; and (iv) acceptance of an e-document as a valid proof expressing consent in transactions and contracts. There is no specific date as to when that draft will be enacted;

(f) *Lebanon*: Lebanese legislation is silent on that issue. Electronic documents are not yet considered as proof per se; and procedural legislation must be amended before the electronic proof can stand as valid and have evidential weight. In the area of e-payment and money transfers, a set of decisions issued by the Central Bank regulates such transactions, in addition to those governing ATM systems. The said decision co-exists with applicable banking laws;

(g) *Oman*: There is no evidence of legal provisions concerning e-transactions or e-commerce;

(h) *Palestine*: Electronic documents, including letters and e-mails, have the same legal evidential power in commercial and civil matters according to article 19 of the Civil and Commercial Procedure Law No. 4 of 2001. That article also recognizes the legal evidential power of an e-mail. The same provisions have been reiterated in Arbitration Law No. 3 of the year 2000 and by Executive Decision No. 9 of 2004.

Moreover, article 26 of Law No. 12 of 2004 on financial securities provides the possibility of legally accepting electronic signatures as evidence;

(i) *Qatar*: There is no evidence of legal provisions concerning e-transactions or e-commerce;

(j) *Saudi Arabia*: A draft law on e-transactions is pending enactment by the legislative body in Saudi Arabia. That draft is aimed at: (i) accepting the validity of e-signatures and e-documents; (ii) enhancing the use of e-transactions at both local and foreign levels; and (iii) preventing the misuse and counterfeiting of e-signatures;

(k) ***Syrian Arab Republic*****:** There is no evidence of legal provisions concerning e-transactions or e-commerce;

(l) ***United Arab Emirates*****:** Federal and local laws in the United Arab Emirates and, more specifically, in Dubai, have in general accepted the electronic proof of documents and admitted the validity of e-contracts. Law No. 2 of 2002 (Dubai) stipulates the formation and validity of e-contracts. In the area of e-signatures, the Law stipulates that an e-signature stands as a written signature with the same evidential power when the said signature complies with authentication conditions mentioned in the Law;

(m) ***Yemen*****:** Law No. 40 of 2006 concerning e-banking and e-payment stipulates, in chapter 4, the provisions of the legal effects of e-records, e-messages and e-signatures. According to those provisions, an electronic document of whatever nature, including letters, contracts and records, has the same legal validity as a written document in terms of proof, and is equally binding on the parties.

Concerning e-payment, the Law stipulates the provisions relating thereto in chapter 6, according to which electronic payment is accepted for the settlement of a debt and as a means of payment. Additionally, chapter 6 defines the rules that financial institutions have to abide by in money transactions; and chapter 7 provides for a legislator to set the rules of certification of an electronic record.

7. *Cyber crime*

This section offers a brief overview of the main international legal texts relating to cyber crime and the status of cyber crime laws in the ESCWA region.

The Convention on Cybercrime, issued by Council of Europe Treaty No. 185 (Budapest, 23 November 2001), defines the nature and main aspects of cyber and computer crime, as well as the need for cooperation and coordination between member countries in order to combat cyber crime and protect legitimate interests. The Convention acts as a deterrent by criminalizing actions that jeopardize the confidentiality, integrity and availability of computer systems, networks and computer data.

The cited offences are as follows:

(a) Offences against the confidentiality, integrity and availability of computer data and systems, namely, illegal access, illegal interception, data interference, system interference and misuse of devices;

(b) Computer-related offences, including computer-related forgery and computer-related fraud;

(c) Content-related offences, including offences related to child pornography, xenophobia, racial content and harmful content;

(d) Offences related to infringements of copyright and related rights.

Moreover, the Convention addresses provisions relating to procedural law and to the investigation of the aforementioned offences.

Council of Europe Treaty No. 189 (Strasbourg, 28 January 2003), the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems, supplements the provisions of the Convention on Cybercrime and cites the following offences:

(a) Dissemination of racist and xenophobic material through computer systems;

(b) Racist and xenophobic motivated threat;

(c) Racist and xenophobic motivated insult;

(d) Denial, gross minimization, approval or justification of genocide or crimes against humanity.

The Convention and the Additional Protocol constitute the main international legal texts dealing with cyber crime and the European countries have amended or enacted their laws to be compliant with the Convention.

In the United Kingdom, the Computer Misuse Act of 1990 is the main applicable law for the prevention of cyber crime. The Act was created to criminalize unauthorized access to computer systems and to deter the use of computers for committing criminal offences or from impairing or hindering access to data stored in a computer. The basic offence is to attempt or achieve access to a computer or the data it stores by inducing a computer to perform any function with intent to secure access.

In the United States, cyber crime is subject to many laws and regulations in order to cover all possible unauthorized access to computer systems or attempts to fraud in connection with access devices. Relevant acts include the Access Device Fraud; the Computer Fraud and Abuse Act; the Can-Spam Act; and the Trade Secrets Act.

In the Arab region, such topics as sexuality, xenophobic and racial issues, discrimination, and religious and certain foreign political matters are considered to be under the purview of public order and any misbehaviour relating to any of the above is accountable under law and, more often than not, under criminal law. In the ESCWA region, while most countries have not yet enacted laws on preventing or combating computer crimes, some initiatives are beginning to show. The status of legislation in a selection of ESCWA countries is summarized below:

(a) *Bahrain*: Article 7 of Ministerial Decision No. 2 of 19 June 2006 concerning technical specifications accepted by official bodies for electronic transactions stipulates that electronic records cannot contain macros or scripts that can alter the record or the data contained therein;

(b) *Oman*: Articles 2 and 5 of Decree No. 72 on money laundering stipulates the means of controlling money transfers in order to uncover money laundering attempts;16

(c) *Palestine*: Executive Decision No. 269 of 2005 issued by the Council of Ministers concerning the confirmation of the general policies on the use of the computer and Internet in official institutions stipulates that access to pornography by official employees is misbehaviour. While that Decision does not stand as preventive against cyber crimes in general, it does regulate the use of computers against misuse in Government offices;

(d) *Saudi Arabia*: A new draft law, which is currently undergoing amendments before final enactment, is set to deal with such cyber crimes as hacking, assisting or covering terrorism, interception of transmissions, deletion, alteration, suppression, and change or destruction of computer data;

(e) *United Arab Emirates*: Federal Law No. 2 of 2006 stipulates combating cyber crime, with imprisonment and fines for the following offences:

(i) Unauthorized or illegal access to a computer system or network which leads to the deletion, cancellation, destruction, dissemination, damage, redirection or suppression of computer data;
(ii) Hindering or intercepting the access to a computer system or program;
(iii) Counterfeiting any e-document recognized by the federal State;
(iv) System interference: inserting what may cause a computer system or network to stop working adequately and to cause destruction, deletion, suppression or alteration of computer data or programs;
(v) Deletion or alteration of medical results or diagnosis;
(vi) Illegal intentional interception of transmissions of computer data;
(vii) Using computer networks or any technical means to threaten a person or extort him to do or abstain from doing any act;
(viii) Electronic theft using a computer system or network;
(ix) Any offence against public morals using a computer system or network, including sexual, religious or private information relating to families, etc.;
(x) Inciting prostitution;
(xi) Human trafficking (advertising or assisting in);
(xii) Illegal money transfers;

(xiii) Assisting terrorism by creating web sites or decoys to cover operations.

According to the main principles of the Law, it is deemed unlawful to use the Internet or computer systems or networks for the following:

(a) To gain access intentionally and without authority or allow others to gain access to a web site or information system; access medical records, local and federal Government records and confidential Government information; intentionally stop or delay the Internet or computer system; and impede or intentionally prevent others from using the Internet or other computer systems, devices or technology;

(b) To erase, delete, remove, damage or amend software programs or data, or any information contained in such software programs or data;

(c) To commit fraud; induce, commit or facilitate slavery; sell or procure illegal drugs; launder money; tape communications; threaten or blackmail; organize or facilitate terrorist activities; and gain access to the particulars or serial numbers of credit cards or other electronic cards;

(d) To produce, prepare, distribute or save, with the intention of using or distributing, displaying or offering to third parties, anything that constitutes an offence to public morals, or to operate a business for such purposes;

(e) To persuade or instigate a male or female to perform an adulterous or grossly lewd act, or to assist in the performance of such an act, or the performing of such an act;

(f) To gain unauthorized access to a web site to alter, delete or inflict damage upon the web site, or to use the Uniform Resource Locator (URL) of the web site for unauthorized purposes;

(g) To deride Islam, Islamic religious beliefs, other religions or religious beliefs which are protected in accordance with

Islamic doctrine, and abuse any of the recognized heavenly religions by using obscene language or embellishing signs.

Penalties and judicial procedures can be summarized as follows:

(a) A court will confiscate devices, software or tools used to commission a crime and any money generated by crime specified under the Law;

(b) A court will deport foreign nationals who commit an offense under the Law;

(c) A court may apply a more severe penalty if an offence has been committed under another law or code that provides for a more severe penalty.

The Federal Law complies with almost every cyber crime law as cited in the European Convention on Cybercrime, with the exception of articles relating to copyright and IPRs in general, which the United Arab Emirates have protected in separate IPR laws. Those IPR laws are still in force and prevail over the provisions of Federal Law No. 2 of 2006 when there has been an infringement of an IPR, whether online or through a computer system. Despite the fact that such a crime is considered a cyber crime, the lack of appropriate provisions in the Federal Law is compensated by existing IPR laws.

Furthermore, cyber crimes are generally prosecuted under criminal law provisions when the national legislation of a given country lacks the adequate cyber crime legislation. The main issue in such an event is the application of criminal procedural law in finding evidence of the crime itself, as the evidence would also be electronic in most of the cases. Thus, such cybercrimes are crimes committed on the computer system or network, not usual crimes committed using a computer system or network. For example, fraud can be committed using e-mails in order to deceive victims. Such a crime is not labeled a cyber crime merely because the tool of the fraud included a computer system or network, or the use of electronic means to facilitate the commitment of the crime itself.

2.3.2. RECOMMENDATIONS FOR DRAFTING A MODEL CYBER LAWIN THE ESCWA REGION

Those countries of the ESCWA region that still lack cyber legislation or have not yet amended their current laws to include cyber-related legal aspects and issues, need to reach a state where issues pertaining to cyber legislation are adequately regulated, thereby progressing in the electronic evolution and the use of computer systems and networks. The recommendations set below are intended to clarify, to the most possible extent, the plan that those countries could follow to achieve the stated goals.

The enactment of a cyber-related law or a set of legislative decrees at a national level is not the only alternative to regulate cyber-related legal issues. In fact, other alternatives are available, namely, to substitute the enactment of a national law or to assist in the enactment thereof by reducing the amount of prerequisites that are necessary for the enactment process.

With the exception of some ESCWA member countries, the region in general still lacks proper legislation that deals directly with cyber-related topics. That can be attributed to various reasons, including: (a) the underestimation of the importance of and need for such legislation by the legislative bodies of a country; (b) the fact that the judicial body does not have a backlog of cyber-related cases; (c) that the judicial body has been able to use the existing laws and provisions by analogy and broad interpretation to overcome or to adjudicate cases and lawsuits involving or having a cyber character.

In those ESCWA member countries where the process of enacting cyber legislation has begun, there is evidence to suggest that such enactments are related in large part to an increase in foreign investment inside the country over the past decade, and that such investment has increasingly used electronic means. That influence has prompted national legislators to actively review existing laws and to amend the provisions thereof by enacting new cyber legislation in such specific fields as e-transactions, e-proof and e-signature.

Notwithstanding the above, waiting for an increase in foreign investment in order to enact cyber legislation does not represent the best approach for those countries still lacking such legislation. Rather, the opposite argument could be more persuasive, with foreign investment being attracted to a country that has already enacted cyber legislation.

Consequently, the availability of adequate cyber legislation is one factor that could contribute to the economic growth of a country and simplify litigation before the courts.

As the current situation stands, the countries of the ESCWA region can be grouped into three categories, namely: (a) countries with substantial initiatives on cyber legislation, including Bahrain and the United Arab Emirates; (b) countries and territory with some cyber legislation, including Egypt, Jordan, Palestine and Yemen; and (c) countries with no cyber legislation, including Iraq, Kuwait, Lebanon, Oman, Qatar, Saudi Arabia and the Syrian Arab Republic.

While the countries in the first two categories have dealt with various cyber legislation issues, some major topics still lack legislative embodiment even in those countries. Those topics are summarized below.

(a) *Data protection*: While the United Arab Emirates issued the Data Protection Law of 2007, it is not a federal law and applies only in the jurisdiction of the Dubai International Financial Centre (DIFC).

Other countries still lack adequate legislation protecting data storage and processing. Some articles have been introduced, including telecommunications laws, under which secrecy of communication is not to be breached. However, those provisions, where they exist, do not reach the required level of protection of data;

(b) *Cyber crime*: Cybercrime, defined as both computer-related crime and content-related crime, is still a topic that is comparatively neglected in the ESCWA region. The only initiative was made by the United Arab Emirates in the enactment of Federal Law No. 2 of 2006 on Combating Information Technology Crimes, in compliance with EU cybercrime laws, which punishes both content-related and computer-related crimes;

(c) *Censorship and freedom of expression*: For national political reasons, that issue is totally and intentionally ignored in the countries of the ESCWA region;

(d) *Privacy on the Internet*: There is no evidence of any legislation in any ESCWA member country concerning the protection of privacy on the Internet. In the absence of adequate legislation, the courts usually deal with privacy-related offences through intellectual property laws or penal laws;

(e) *E-commerce*: The countries of the ESCWA region lack legislation on consumer-to-consumer (C2C) and business-to-consumer (B2C) relationships. E-commerce is closely related to trade in general, and thus is also subject to the provisions of commercial laws. However, such laws need to be amended in order to implement legal issues that are solely related to e-business. While some of the major issues could be treated within e-transaction laws, including e-signature and attribution, such topics as consumer protection and advertising on the Internet have not been addressed. Advertising on the Internet has not yet been legislatively treated in the countries of the ESCWA region;

(f) *Telecommunications*: While the countries of the ESCWA region have enacted laws regulating telecommunications, there is no legislation concerning electronic telecommunications. By contrast, the countries of EU have embodied articles in their telecommunications laws that provide for rules concerning electronic communications. In France, for example, the Code governing postal communications establishes provisions concerning communications in electronic forms.

In order to be closer to foreign legal integration of cyber legislation, the countries of the ESCWA region need to address the above topics; either by ratifying relevant international conventions; or by enacting national laws that are compliant with international directives, agreements and/or national laws. Specifically, those ESCWA member countries without cyber legislation could follow the process described below.

Generally, most national constitutions recognize international conventions and treaties, once the country is a signatory, as part of the local legislation and may take precedence over locally enacted laws.

Therefore, countries without cyber laws could start by ratifying an international treaty or convention that treats a cyber-related topic, including, for example, e-signature or e-proof. In so doing, a country would only have to amend existing laws in order to comply with the provisions of the treaty or convention and to delete any contradictions therewith.

The first step would be to assess the legislation status of the country in question in order to set a clear list of the laws that need to be amended in order to comply with cyber-related legal topics, and to define what cyber-related topics have to be subject to a nationally enacted law, in the event that no available international or regional treaty or convention can be ratified to complete the local legislation on that specified issue.

As mentioned above, the need for a cyber-related legislation, whether through ratification of an international treaty or convention or enactment of a national law, will usually be backed by the judicial system and the interest groups, who, if adequately informed, could lobby legislators to proceed with the enactment process. Consequently, the main focus for attracting the attention of such groups is to create, among others, working plans through workshops, seminars for lawyers and judges, and conferences for interest groups. Those working plans could help to boost the knowledge of both the interest groups and the legislators of the necessity of such a law.

Subsequently, legislators may opt for one out of three approaches in order to present a cyber law, namely: (a) to draft a local law; (b) to ratify an international treaty, thereby saving time in terms of drafting a local law; and (c) to adopt a model law that is available on a regional or international level.20

2.3.2.A. MECHANISM FOR ENACTING CYBER LEGISLATION

The working plan for enacting a new law is set forth below:

(a) *Creating a specialized focus group*: Such as group is usually formed by the following: (i) concerned ministry professionals in a given field, including the ministries of trade, economy and telecommunications; (ii) professionals from ICT companies and organizations; and (iii) legal professionals, including lawyers and legal counsellors in related fields, with knowledge and experience of the subject field. That group could establish a template comprising a checklist of the main topics that deal with the subject of the law, for example e-commerce, data protection or cyber crime. That checklist can be expanded and/or amended in the light of foreign laws on the same subject or of international treaties or conventions.

The focus group shall consult international conventions dealing with the subject of the law to be enacted and foreign initiatives and laws on the same subject. Such a review of foreign laws must also comprise the original law was enacted by the foreign State and any subsequent amendments, so as to allow lessons to be drawn from necessary revisions and amendments after the law was enacted. Moreover, the focus group is encouraged to review the reasons and necessities for enacting the law in order to ascertain whether similar needs apply locally.

Finally, the focus group will be able to put down recommendations concerning the main topics that are to be treated in the law;

(b) *The model law and focus group*: When the recommendations of the first focus group are set, a preliminary draft of the law, referred to as a model law, is completed. The focus group is then enlarged and additional professionals are invited to discuss the model law, article by article. Those discussion boards are usually include professionals from both the public and private sectors who represent the main subjects to the application of the provisions of the law upon enactment, namely, Internet service providers, intellectual property law firms, telecommunications firms, judiciary police officers combating cyber crime, and officials of chambers of commerce dealing with issues related to e-commerce.

After the completion of the study and discussion meetings, the focus group would have a draft law ready to be submitted to the ministry concerned;

(c) *Interviews and workshops*: When the draft law is ready, interviews with key persons will be needed in order to discuss the law and its projected impact on the public and private sectors. Additionally, workshops with members of parliament should be held in order to acquaint them with the draft. Such interviews and workshops are aimed at explaining the law and building the understanding thereof to the members of the parliamentary committee that will study the draft and make necessary amendments, thereby making it compliant with existing legislation and ensuring that the provisions and procedures of the new draft do not contradict established laws;

(d) *Discussion sessions*: The final phase before enacting the law relates to discussion sessions concerning the draft. Those sessions will group experts in the related fields and aim at ensuring the draft law covers all possible situations that can occur from the application of its provisions;

(e) *Regional directives*: The example of the EU Council regarding the issuance of directives relating to cyber legislation issues represents a paradigm for enhancing the state of cyber legislation in the ESCWA region. The League of Arab States or the Gulf Cooperation Council (GCC) could represent adequate bodies to issue directives concerning such topics as cyber crime or data protection. Naturally, while these directives could not be applied as international treaties that are enforceable as local laws, member countries could be given set time periods in order to amend their existing laws or introduce regulations that are compliant with the provisions of such directives. Essentially, enacting local laws based on directives could be an easier course, given that such directives would already have been issued based on focus groups and studies.

2.3.2.B. CONCLUSIONS

This study provided an overview of the cyber laws enacted and in force in the ESCWA region; and of the initiatives currently underway, aimed at achieving and completing cyber legislation and at adapting existing laws to international texts and directives.

Some countries of the region have already proceeded with the enactment and promulgation of various cyber laws, particularly countries of the GCC and Egypt. Others are still either awaiting the legislative body to pass cyber legislation, or studying and drafting the text of such laws.

This study revealed that, in general, the countries of the ESCWA region are following international and foreign laws as models when drafting national legislation. That is highlighted by the laws enacted in the most advanced countries of the ESCWA region regarding cyber issues, principally the Computer Crime Law and the Data Protection Law of the United Arab Emirates (Dubai).

In the future, the countries of the region could reach a point where cyber-related legal topics are addressed either by the ratification of international conventions, or though the enactment of national laws. The initiatives carried out by the European Community, as well as the acquired experience of other international organizations, could help to encourage ESCWA member countries in terms of the enactment of national cyber laws. Furthermore, those ESCWA member countries seeking to join WTO will have to comply with the standards required by the Organization and will have to amend their laws in order to meet those standards, including, for example, by enacting intellectual property laws that are compliant with the TRIPS Agreement.

2.4 REPUBLIC OF INDIA[10]

2.4.1 ANALYSIS OF THE STATUTORY PROVISONS:

The Information Technology Act 2000 was undoubtedly a welcome step at a time when there was no legislation on this specialised field. The Act has however during its application has proved to be inadequate to a certain extent. The various loopholes in the Act are-

1. *The hurry in which the legislation was passed, without sufficient public debate, did not really serve the desired purpose*

   Experts are of the opinion that one of the reasons for the inadequacy of the legislation has been the hurry in which it was passed by the parliament and it is also a fact that sufficient time was not given for public debate.

2. *"Cyber laws, in their very preamble and aim, state that they are targeted at aiding e-commerce, and are not meant to regulate cybercrime"*(6) -

   Mr. Pavan Duggal holds the opinion that the main intention of the legislators has been to provide for a law to regulate the e-commerce and with that aim the I.T. Act 2000 was passed, which also is one of the reasons for its inadequacy to deal with cases of cyber crime.

   At this point I would like to express my respectful dissent with Mr. Duggal. I feel that the above statement by Mr. Duggal is not fundamentally correct. The reason being that the preamble does state that the Act aims at legalising e-commerce. However it does

[10] CYBER CRIME (2009)

not stop here. It further amends the I.P.C., Evidence Act, Banker's Book Evidence and RBI Act also. The Act also aims to deal with all matters connected therewith or incidental thereto. It is a cardinal rule of interpretation that *"text should be read as a whole to gather the meaning". It seems that the above statement has been made in total disregard of this rule of interpretation.* The preamble, if read as a whole, makes it very clear that the Act equally aims at legalising e-commerce and to curb any offences arising there from.

3. *Cyber torts-*

The recent cases including Cyber stalking cyber harassment, cyber nuisance, and cyber defamation have shown that the I.T. Act 2000 has not dealt with those offences. Further it is also contended that in future new forms of cyber crime will emerge which even need to be taken care of. Therefore India should sign the cyber crime convention. However the I.T. Act 2000 read with the Penal Code is capable of dealing with these felonies.

4. *Cyber crime in the Act is neither comprehensive nor exhaustive-*

Mr. Duggal believes that we need dedicated legislation on cyber crime that can supplement the Indian Penal Code. The contemporary view is held by Mr. Prathamesh Popat who has stated- "The IT Act, 2000 is not comprehensive enough and doesn't even define the term 'cyber crime". Mr. Duggal has further commented, "India, as a nation, has to cope with an urgent need to regulate and punish those committing cyber crimes, but with no specific provisions to do so. Supporters of the Indian Penal Code School vehemently argue that IPC has stood the test of time and that it is not necessary to incorporate any special laws on cyber crime. This is because it is debated by them that the IPC alone is sufficient for all kinds of crime. However, in practical terms, the argument does not have appropriate backing. It has to be distinctly understood that cyber crime and cyberspace are completely new whelms, where numerous new possibilities and opportunities emerge by the day in the form of new kinds of crimes."

I feel that a new legislation on cyber crime is totally unwarranted. The reason is that the new legislation not come alone but will bring with it the same confusion, the same dissatisfaction and the same desire to supplant it by further new legislation. Mr. Duggal has stated above the need to supplement IPC by a new legislation. If that is the issue then the present legislation along with the Penal Code when read harmoniously and co- jointly is sufficient to deal with the present problems of cyber crime. Further there are other legislations to deal with the intellectual property crimes on the cyber space such as the Patents Act, Copy Right Act, Trade Marks Act.

5. *Ambiguity in the definitions-*

The definition of hacking provided in section 66 of the Act is very wide and capable of misapplication. There is every possibility of this section being misapplied and in fact the Delhi court has misapplied it. The *infamous* has made it very clear that what may be the fate of a person who is booked under section 66 or the constant threat under which the netizens are till s. 66 exists in its present form.

Further section 67 is also vague to certain extent. It is difficult to define the term *lascivious information or obscene pornographic information.* Further our inability to deal with the cases of cyber pornography has been proved by *the Bal Bharati case*.

6. *Uniform law-*

Mr. Vinod Kumar holds the opinion that the need of the hour is a worldwide uniform cyber law to combat cyber crime. Cyber crime is a global phenomenon and therefore the initiative to fight it should come from the same level. E.g. the author of the love bug virus was appreciated by his countrymen.

7. *Lack of awareness-*

One important reason that the Act of 2000 is not achieving complete success is the lack of awareness among the s about their rights. Further most of the cases are going unreported. If the people are vigilant about their rights the law definitely protects their right. E.g. the Delhi high court in October 2002 prevented a person from selling *Microsoft pirated software* over an auction site. Achievement was also made in the case before the court of metropolitan magistrate Delhi wherein a person was convicted for *online cheating* by buying Sony products using a *stolen credit* card.

8. *Jurisdiction issues-*

Jurisdiction is also one of the debatable issues in the cases of cyber crime due to the very universal nature of cyber space. With the ever-growing arms of cyber space the territorial concept seems to vanish. New methods of dispute resolution should give way to the conventional methods. The Act of 2000 is very silent on these issues.

9. *Extra territorial application-*

Though S.75 provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.

10. *Raising a cyber army-*

By using the word 'cyber army' by no means I want to convey the idea of virtual army, rather I am laying emphasis on the need for a well equipped task force to deal with the new trends of hi tech crime. The government has taken a leap in this direction by constituting cyber crime cells in all metropolitan and other important cities. Further the establishment of the ***Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI)*** is definitely a welcome step in this direction. There are many cases in which the C.B.I has achieved success. The present position of cases of cyber crime is –

Case 1: When a woman at an MNC started receiving obscene calls, CBI found her colleague had posted her personal details on Mumbaidating.com.

Status: Probe on

Case 2: CBI arrested a man from UP, Mohammed Feroz, who placed ads offering jobs in Germany. He talked to applicants via e-mail and asked them to deposit money in his bank account in Delhi.

Status: Charge sheet not filed

Case 3: The official web-site of the Central Board of Direct Taxes was hacked last year. As Pakistan-based hackers were responsible, authorities there were informed through Interpol.

Status: Pak not cooperating.

11. *Cyber savvy bench-*

Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the *P.I.L., which the Kerela High Court* has accepted through an email. The role of the judges in today's word may be gathered by the statement- judges carve 'law is' to 'law ought to be'. *Mr T.K. Vishwanathan*, member secretary, *Law Commission*, has highlighted the requirements for introducing e-courts in India. In his article published in The Hindu he has stated "*if there is one area of Governance where IT can make a huge difference to Indian public is in the Judicial System*".

12. *Dynamic form of cyber crime-*

Speaking on the dynamic nature of cyber crime FBI Director Louis Freeh has said, "*In short, even though we have markedly improved our capabilities to fight cyber intrusions the problem is growing even faster and we are falling further behind.*" The (de)creativity of human mind cannot be checked by any law. Thus the only way out is the liberal construction while applying the statutory provisions to cyber crime cases.

13. *Hesitation to report offences-*

As stated above one of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force. This was proved by the *Delhi time theft case*. "The police are a powerful force today which can play an instrumental role in preventing cyber crime. At the same time, it can also end up wielding the rod and harassing innocent s, preventing them from going about their normal cyber business. "This attitude of the administration is also revelled by incident that took place at *Merrut and Belgam*. (for the facts of these incidents refer to naavi.com). For complete realisation of the provisions of this Act a cooperative police force is require.

2.4.2. PREVENTION OF CYBER CRIME:

Prevention is always better than cure. It is always better to take certain precaution while operating the net. A should make them his part of cyber life. Saileshkumar Zarkar, technical advisor and network security consultant to the Mumbai Police Cyber crime Cell, advocates the 5P mantra for online security*: Precaution, Prevention, Protection, Preservation and Perseverance.* A netizen should keep in mind the following things-

1. To prevent cyber stalking avoid disclosing any information pertaining to one-self. This is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Always use latest and up date anti virus software to guard against virus attacks.
4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination
5. Never send your credit card number to any site that is not secured, to guard against frauds.
6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
7. It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
8. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9. Use of firewalls may be beneficial.
10. Web servers running public sites must be physically separate protected from internal corporate network.

Adjudication of a Cyber Crime - On the directions of the Bombay High Court the Central Government has by a notification dated 25.03.03 has decided that the Secretary to the Information Technology Department in each state by designation would be appointed as the AO for each state.

2.4.3. CONCLUSION:

Capacity of human mind is unfathomable. It is not possible to eliminate cyber crime from the cyber space. It is quite possible to check them. History is the witness that no legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties (to report crime as a collective duty towards the society) and further making the application of the laws more stringent to check crime.

Undoubtedly the Act is a historical step in the cyber world. Further I all together do not deny that there is a need to bring changes in the Information Technology Act to make it more effective to combat cyber crime. I would conclude with a word of caution for the pro-legislation school that it should be kept in mind that the provisions of the cyber law are not made so stringent that it may retard the growth of the industry and prove to be counter-productive.

2.5 ISLAMIC REPUBLIC OF PAKISTAN

2.5.1. ELECTRONIC TRANSACTION ORDINANCE, 2002[11]

The relevant provisions of the Ordinance are enumerated as under:

2.5.1.i RECOGNITION AND PRESUMPTION

3. Legal recognition of electronic forms.—"No document, record, information, communication or transaction shall be denied legal recognition, admissibility, effect, validity, proof or enforceability on the ground that it is in electronic form and has not been attested by any witness."

7. Legal recognition of electronic signatures. — "The requirement under any law for affixation of signatures shall be deemed satisfied where electronic signatures or advanced electronic signatures are applied."

8. Proof of electronic signature. — "An electronic signature may be proved in any manner, in order to verify that the electronic document is of the person that has executed it with the intention and for the purpose of verifying its authenticity or integrity or both."

[11] Ordinance No.LI of 2002: (2009)

9. Presumption relating to advanced electronic signature.—"In any proceedings, involving an advanced electronic signature, it shall be presumed unless evidence to contrary is adduced, that:

(a) the electronic document affixed with an advanced electronic signature, as is the subject-matter of or identified in a valid accreditation certificate is authentic and has integrity; or

(b) the advanced electronic signature is the signature of the person to whom it correlates, the advanced electronic signature was affixed by that person with the intention of signing or approving the electronic document and the electronic document has not been altered since that point in time."

12. Certified copies.—"Where any law requires or permits the production of certified copies of any records, such requirement or permission shall extend to printouts or other forms of display of electronic documents where, in addition to fulfillment of the requirements as may be specified in such law relating to certification, it is verified in the manner laid down by the appropriate authority."

2.5.1.ii OFFENCES

34. Provision of false information, etc. by the subscriber.--(1) "Any subscriber who:

(a) Provides information to a certification service provider knowing such information to be false or not believing it to be correct to the best of his knowledge and belief;

(b) Fails to bring promptly to the knowledge of the certification service provider any change in circumstances as a consequence whereof any information contained in a certificate accepted by the subscriber or authorized by him for publication or reliance by any person, ceases to be accurate or becomes misleading, or

(c) Knowingly causes or allows a certificate or his electronic signatures to be used in any fraudulent or unlawful manner, shall be guilty of an offence under this Ordinance.

(2) The offence under sub-section (1) shall be punishable with imprisonment either description of a term not exceeding seven years, or with fine which may extend to ten million rupees, or with both."

35. Issue of false certificate, etc.— "(1) Every director, secretary and other responsible officer, by whatever designation called, connected with the management of the affairs of a certification service provider, which:

(a) Issues, publishes or acknowledges a certificate containing false or misleading information;

(b) Fails to revoke or suspend a certificate after acquiring knowledge that any information contained therein has become false or misleading;

(c) Fails to revoke or suspend a certificate in circumstances where it ought reasonably to have been known that any information contained in the certificate is false or misleading;

(d) Issues a certificate as accredited certification service provider while its accreditation is suspended or revoked; shall be guilty of any offence under this Ordinance."

(2) "The offence under sub-section (l) shall be punishable with imprisonment either description of a term not exceeding seven years, or with fine which may extend to ten million rupees, or with both.

(3) The certification service provider or its employees specified in sub-section (1), shall also be liable, upon conviction, to pay compensation for any foreseeable damage suffered by any person or subscriber as a direct consequence of any of the events specified in clauses (a) to (d) of sub-section (1).

(4) The compensation mentioned in sub-section (3) shall be recoverable as arrears of land revenue."

36. Violation of privacy of information.—"Any person who gains or attempts to gain access to any information system with or without intent to acquire the information contained therein or to gain knowledge of such information, whether or not he is aware of the nature or contents of such information, when he is not authorized to gain access, as aforesaid, shall be guilty of an offence under this Ordinance punishable with either description of a term not exceeding seven years, or fine which may extend to one million rupees, or with both."

37. Damage to information system, etc.—"(1) Any person who does or attempts to do any act with intent to alter, modify, delete, remove, generate, transmit or store any information through or in any information system knowingly that he is not authorized to do any of the foregoing, shall be guilty of an offence under this Ordinance.

(2) Any person who does or attempts to do any act with intent to impair the operation of, or prevent or hinder access to, any information contained in any information system, knowingly that he is not authorized to do any of the foregoing, shall be guilty of an offence under this Ordinance.

(3) The offences under sub-section (1) and (2) of this section will be punishable with either description of a term not exceeding seven years or fine which may extend to one million rupees, or with both."

38. Offences to be non-bail-able, compoundable and cognizable.— All offences under this Ordinance shall be non-bail-able, compoundable and cognizable.

39. Prosecution and trial of offences.—No Court inferior to the Court of Sessions shall try any offence under this Ordinance.

2.5.1.iii Amendments in Order Qanoon-e-Shahadat 1984

- "By way of amendment an new section 46 (a) has been inserted which is reproduced as under:

  "46-A. Relevance of information generated, received or recorded by automated information system.— Statements in the form of electronic documents generated, received or recorded by an automated information system while it is in working order, are relevant facts."

- "By way of amendment in article 59 Electronic document made by or through information system has also been made relevant fact as to the opinion of Experts and as such the functioning specification programming and operation of information system have been made relevant facts."

- In article 73 regarding the primary evidence, explanation 3 (a) has been inserted which is reproduced as under:

"*Explanation 3.*—A printout or other form of output of an automated information system shall not be denied the status of primary evidence solely for the reason that it was generated, sent, received or stored in electronic form if the automated information system was in working order at all material times and, for the purposes hereof, in the absence of evidence to the contrary, it shall be presumed that the automated information system was in working order at all material times."

"Explanation 4.—"A printout or other form of reproduction of a Electronic Document, other than a Document mentioned in Explanation 3 above, first generated, sent, received or stored in electronic form, shall be treated as primary evidence where a security procedure was applied thereto at the time it was generated, sent, received or stored."

❖ Regarding the proof of electronic signature and electronic document a new article 78 (a) has been inserted which is reproduced as under:

"*78-A. Proof of electronic signature and electronic document.*—If an electronic document is alleged to be signed or to have been generated wholly or in part by any person through the use of an information system, and where such allegation is denied, the application of a security procedure to the signature or the electronic document must be proved."

❖ By way of amendment in article 85 a new clause (6) has been inserted which is reproduced as under:

"(6) Certificates deposited in a *repository** pursuant to the provisions of the Electronic Transactions Ordinance, 2002."

* *"repository" means an information system for storing and retrieving certificates or other information related thereto established under section 23;*

2.5.2 ELECTRONIC FUNDS TRANSFER ACT 2007[12]

The relevant provisions of the act are reproduced as under:

56. Criminal Liability.- Whoever knowingly and willfully gives false information or inaccurate information or fails to provide information which he is required to disclose by this Act or any instruction issued there-under, or otherwise fails to comply with any provision of this Act shall be punished with imprisonment of either description which may extend to three years, or with fine which may extend to three million rupees, or with both.

57. Violations Affecting Electronic Commerce.- Whoever –

(1) knowingly, in a transaction effected by electronic commerce, uses or attempts or conspires to use any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained Debit Instrument to obtain money, goods, services or anything else of value aggregating five thousand rupees or more, or

(2) knowingly receives, conceals, uses or transports money, goods, services or anything else of value aggregating five thousand rupees or more obtained by use of any counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained Debit Instrument, or

[12] Payment Systems and Electronic Fund Transfers Act, 2007: (2009)

(3) knowingly receives, conceals, uses, sells, or transports one or more tickets for transportation, and which have been purchased or obtained with one or more counterfeit, fictitious, altered, forged, lost, stolen or fraudulently obtained Debit Instrument,

shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine which may extend to one million rupees, or with both.

Explanation.- For the purpose of this section e-commerce means the activity of buying, selling or contracting for goods, services and making payments using internet or worldwide web through communication networks including of wireless networks, within or outside Pakistan.

58. Cheating by Use of Electronic Device.- Whosoever cheats by pretending to be some other person, or by knowingly substituting one person for another, or representing that he or any other person is a person other than he or such other person really is, or by cheating by impersonation, fraudulently or dishonestly uses any credit or debit card, or code or any other means of access to an Electronic Fund Transfer device, and thereby causes any wrongful gain to himself or any wrongful loss to any other person, shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine which shall not be less than the wrongful loss caused to any person, or with both.

2.5.3 PREVENTION OF ELECTRONIC CRIME ORDINANCE 2009[13]

2.5.3.i OFFENCES AND PUNISHMENTS

3. Criminal access.-

Whoever intentionally gains unauthorized access to the whole or any part of an electronic system or electronic device with or without infringing security measures, shall be punished with imprisonment of either description for a term which may extend to two years, or with fine not exceeding three hundred thousand rupees, or with both.

4. Criminal data access.-

Whoever intentionally causes any electronic system or electronic device to perform any function for the purpose of gaining unauthorized access to any data held in any electronic system or electronic device or on obtaining such unauthorized access shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or with both.

5. Data damage.-

Whoever with intent to illegal gain or cause harm to the public or any person, damages any data shall be punished with imprisonment of either description for a term which may extend to three years, or with fine, or with both:

[13] Prevention of Electronic Crimes Ordinance (2009)

Explanation.- For the purpose of this section the expression ;data damage; includes but not limited to modifying, altering, deleting, deterioration, erasing, suppressing, changing location of data or making data temporarily or permanently unavailable, halting electronic system, choking the networks or affecting the reliability or usefulness of data.

6. System damage.

Whoever with intent to cause damage to the public or any person interferes with or interrupts or obstructs the functioning, reliability or usefulness of an electronic system or electronic device by inputting, transmitting, damaging, deleting, altering, tempering, deteriorating or suppressing any data or services or halting electronic system or choking the networks shall be punished with imprisonment of either description for a term which may extend to three years, or with fine or, with both:

Explanation.- For the purpose of this section the expression ;services; include any kind of science provided through electronic system.

7. Electronic fraud.-

Whoever for wrongful gain interferes with or uses any data, electronic system or electronic device or induces any person to enter into a relationship or with intent to deceive any person, which act or omission is likely to cause damage or harm to that person or any other person shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine, or with both.

8. Electronic forgery.-

Whoever for wrongful gain interferes with data, electronic system or electronic device, with intent to cause damage or injury to the public or to any person, or to make any illegal claim or title or to cause any person to part with property or to enter into any express or implied contract, or with intent to commit fraud by any input, alteration, deletion, or suppression of data, resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of the fact that me date is directly readable and intelligible or not shall be punished with imprisonment of either description for a term which may extend to seven years, or with fine or with both.

9. Misuse of electronic system or electronic device.

(I) Whoever produces, possesses, sells, procures, transports, imports, distributes or otherwise makes available an electronic system or electronic device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established under this Ordinance or a password, access code, or similar data by which the whole or any part of an electronic system or electronic device is capable of being accessed or its functionality compromised or reverse engineered, with the intent that it be used for the purpose of committing any of the offences established under this Ordinance, is said to commit offence of misuse of electronic system or electronic devices:

Provided that the provisions of this section shall not apply to the authorized testing .or protection of an electronic system for any lawful purpose.

(2) Whoever commits the offence described in sub-section (1) shall be punishable with imprisonment of either description for a term which may extend to three years, or with fine, or with both.

10. Unauthorized access to code.-

Whoever discloses or obtains any password, access as to code, system design or any other means of gaining access to any electronic system or data with intent to obtain wrongful gain, do reverse engineering or cause wrongful loss to any person or for any other unlawful purpose shall be punished with imprisonment of either description for a term which may extend to three years, or with, or with both.

11. Misuse of encryption.-

Whoever for the purpose of commission of an offence or concealment of incriminating evidence, knowingly and willfully encrypts any incriminating communication or data contained in electronic system relating to that crime or incriminating evidence commits the offence of misuse of encryption shall be punished with imprisonment of either description for a term which may extend to five years, or with fine, or with both.

12. Malicious code.-

(I) Whoever willfully writes, offers, makes available, distributes or transmits malicious code through an electronic system or electronic device, with intent to cause harm to any electronic system or resulting in the corruption, destruction, alteration, suppression, theft or loss of data commits the offence of malicious code:

Provided that the provision of this section shall not apply to the authorized testing, research and development or protection of an electronic system for any lawful purpose;

Explanation.- For the purpose of this section the expression ;malicious code; includes but not limited to a computer program or a hidden function in a program that damages data or compromises the electronic systems performance or uses the electronic system resources without proper authorization, with or without attaching its copy to a file and is capable of spreading over electronic system with or without human intervention including virus, worm or Trojan horse.

(2) Whoever commits, the offence specified in sub-section (1) shall be punished with imprisonment of either description for a term which may extend to five years, or with fine or with both.

13. Cyber stalking.-

(I) Whoever with intent to coerce, intimidate, or harass any person uses computer, computer network, internet, network site, electronic mail or any other similar means of communication to,-

(a) Communicate obscene, vulgar, profane, lewd, lascivious, or indecent language, picture or image;
(b) Make any suggestion or proposal of an obscene nature;
any illegal or immoral act;
(d) Take or distribute pictures or photographs of any person without his consent or knowledge;
(e) Display or distribute information in a manner that substantially increases the risk of harm or violence to any other person, commits the offence of cyber stalking.

(2) Whoever commits the offence specified in sub-section (I) shall be punishable with imprisonment of either description for a term which may extend to seven years with fine not exceeding three hundred thousand rupees, or with both:

Provided that if the victim of the cyber stalking under sub-section (1) is a minor the punishment may extend to ten years or with foe not less than one hundred thousand rupees, or with both.

14. Spamming.-

(I) Whoever transmits harmful, fraudulent, misleading, illegal or unsolicited electronic messages in bulk to any person without the express permission of the recipient, or causes any electronic system to show any such message or involves in falsified online user account registration or falsified domain name registration for commercial purpose commits the offence of spamming.

(2) Whoever commits the offence of spamming as described in sub-section (1) shall be punishable with fine not exceeding fifty thousand rupees if he commits this offence of spamming for the first time and for every subsequent commission of offence of spamming he shall be punished with imprisonment of three months or with fine, or with both.

15. Spoofing. –

(I) Whoever establishes a website, or sends an electronic message with a counterfeit source intended to be believed by the recipient or -visitor or its electronic system to be an authentic source with intent to gain unauthorized access or obtain valuable information which later can be used for any unlawful purposes commits the offence of spoofing.

(2) Whoever commits the offence of spoofing specified in sub-section (!) shall be punished with imprisonment of either description for a lean which may extend to three years, or with fine, or with both.

16. Unauthorized interception.-

(1) Whoever without lawful authority intercepts by technical means, transmissions of data to, from or within an electronic system including electromagnetic emissions from an electronic system carrying such data commits the offence of unauthorized interception.

(2) Whoever commits the offence of unauthorized interception described in subsection (I) shall be punished with imprisonment of either description for a term which may extend to five years, or with fine not exceeding five hundred thousand rupees, or with both.

17. Cyber terrorism.-

(1) Any person, group or organization who, with terroristic intent utilizes, accesses or causes to be accessed a computer or computer network or electronic system or electronic device or by any available means, and there by knowingly engages in or attempts to engage in a terroristic act commits the offence of cyber terrorism.

Explanation 1.; For the purposes of this section the expression; terroristic intent; means to act with the purpose to alarm, frighten, disrupt harm, damage, or carry out an act of violence against any segment of the population, the Government or entity associated therewith.

Explanation 2.; For the purposes of this section the expression; terroristic act; includes, but is not limited to.-

(a) Altering by addition, deletion, or change or attempting to alter information that may result in the imminent injury, sickness, or death to any segment of the population;

(b) Transmission or attempted transmission of a harmful program with the purpose of substantially disrupting or disabling any computer network operated by the Government or any public entity;

(c) Aiding the commission of or attempting to aid the commission of an act of violence against the sovereignty of Pakistan, whether or not the commission of such act of violence is actually completed- or

(d) stealing or copying., or attempting to steal or copy, or secure classified information or data necessary to manufacture any farm of chemical, biological or nuclear weapon, or any other weapon of mass destruction, (2) Whoever commits the offence of cyber terrorism and causes death of any person shall be punishable with death or imprisonment for life and with fine and in any other case he shall be punishable with imprisonment of either description for a term which may extend to ten years, or with fine not less than ten million rupees, or with both.

18. Enhanced punishment for offences involving sensitive electronic systems.-

(1) Whoever causes criminal access to any sensitive electronic system in the course of the commission of any of the offences established under this Ordinance shall, in addition to the punishment prescribed for that offence, be punished with imprisonment of either description for a term which may extend to ten years, or with fine not exceeding one million rupees, or with both.

(2) For the purposes of any prosecution under this section, it shall be presumed, until contrary is proved, that the accused had the requisite knowledge that it was a sensitive electronic system.

19. Of abutments, aids or attempts to commits offence.-

(I) Any person who knowingly and willfully abets die commission of or-who aids to commit or does any act preparatory to or in furtherance of the commission of any offence under this Ordinance shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence.

(2) Any person who attempts to commit an offence under this Ordinance shall be punished for a term which may extend to one-half of the longest term of imprisonment provided for that offence:

Explanation .- For aiding or abetting an offence to be committed under this section, it is immaterial whether the offence has been committed or not.

20 Other offences.-

Whoever commits any offence, other than those expressly provided under this Ordinance, with the help of computer, electronic system, electronic device or any other electronic means shall be punished, in addition to the punishment provided for that offence, with imprisonment of either description for a term which may extend to two years, or with fine not exceeding two hundred thousand rupees, or with both.

21 Offences by corporate body

A corporate body shall be held liable for an offence under this Ordinance if the offence is committed on its instructions or for its benefit. The corporate body shall be punished with fine not less man one hundred thousand rupees or the amount involved in the offence whichever is the higher Provided that such punishment shall not absolve the criminal liability of the natural person who has committed the offence:

Explanation.- For the purposes of this section corporate body, includes a body of persons incorporated under any law such as trust, waqf an association, a statutory body or a company.

CHAPTER – 3

COMPUTER FORENSICS, COLLECTION AND PRESERVATION OF DIGITAL EVIDENCE[14]

3.1. Cyber Forensics Defined

In attempting to define cyber forensics, one common problem is determining exactly what is and what is not or should not, be included in defining this extensive field.

At its broadest level, cyber forensics is defined as the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

At the grassroots level, this becomes the process of extracting information and data from computer storage media and guaranteeing its accuracy and reliability. In essence, cyber forensics is an archeological dig, designed to uncover (or discover) what happened on a specific hard drive, within a specific computer, during a specific period of time. Ultimately, cyber forensics is the combination of law and science (computer science).

[14] Albert J.Marcella

The computer forensic expert or investigator knows how to extract evidence, based upon personal testing and validation of the findings, in accordance with the prescribed laws, for the extraction, collection and preservation of said evidence.

So, what actually is computer forensics? Computer forensics is about evidence from computers that is sufficiently reliable to stand up in court and be convincing. You might employ a computer forensics specialist to acquire evidence from computers on your behalf. On the other hand, you may want one to criticize the work of others. The field is a rapidly growing one, with a solid core but with many controversies at its edges.

3.2. Computer Forensic Computing:

Forensic computing or computer forensics is the process of identifying preserving analyzing and presenting digital evidence in a manner that is legally acceptable or the application of computer science to the investigative legal processes. It is used to uncover the proverbial smoking gun and to organize voluminous amounts of data specialists also draw on an array of methods for discovering data that resides in a computer system or recovering deleted encrypted or damaged file information. The process draws upon many disciplines and involves the application of information technology to the search for digital evidence. It comprises three primary activities:

- Media and electronic device analysis - the examination of various types of storage media;
- Data communications analysis - which encompasses the two main activities of network intrusion or misuse and data interception.
- Research and development.

While computer crime is the most obvious example of where forensic computing is required. Any kind of crime may contain digital evidence from a variety of electronic devices that needs to be examined e.g. e-mail between victim and suspect in a sexual assault case, electronic spreadsheets with financial implications in a fraud or dug case or a victim's email calendar or to do list in a murder case. In fact evidence recovered from a computer may prove vital to an investigation despite the suspect computer being incidental to the actual offence.

At a basic level computer forensics is the analysis of information contained within and created with computer systems and computing devices typically in the interest of figuring out what happened when it happened how it happened and who was involved.

This can be for the purpose of performing a root cause analysis of a computer system that had failed or is not operating properly or to find out who is responsible for misuse of computer systems or perhaps who committed a crime using a computer system or against a computer system. This being said computer forensic techniques and methodologies are commonly used for conducting computing investigations again in the interest of figuring out what happened when it happened how it happened and who was involved.

3.2.1. Identification:

In the initial phase this has to do with identifying the possible containers of computer related evidence such as hard drives floppy disks and log files to name a few. Understand that a computer or hard drive itself is not evidence it is a possible container of evidence.

In the analysis phase this has to do with identifying the information and data that is actually pertinent to the situation at hand. Sifting through Gigabytes of information conducting keyword searches looking through log files etc.

3.2.2. Preservation:

When performing a computer forensics analysis we must do everything possible to preserve the original media and data. Typically this involves making a forensic image or forensic copy of the original media and conducting our analysis on the copy versus the original.

3.2.3. Extraction:

Any evidence found relevant to the situation at hand will need to be extracted from the working copy media and then typically saved to another form of media as well as printed out.

3.2.4. Interpretation:

This is a biggie. Understand that just about anyone can perform a computer forensics "analysis." Some of the GUI tools available make it extremely easy. Being able to find evidence is one thing the ability to properly interpret it is another story. Entire books could be written citing examples of when computer forensics experts misinterpreted their results of a forensic analysis. We'll cite one example.

3.3. COLLECTION OF EVIDENCE[15]:

There are two basic forms of collection: freezing the scene and honey-potting. The two aren't mutually exclusive. You can collect frozen information after or during any honey-potting.

[15] John R.Vacca

- **Freezing** the scene involves taking a snapshot of the system in its compromised state. The necessary authorities should be notified (the police and your incident response and legal teams), but you shouldn't go out and tell the world just yet. You should then start to collect whatever data is important onto removable nonvolatile media in a standard format. Make sure the programs and utilities used to collect the data are also collected onto the same media as the data. All data collected should have a cryptographic message digest created, and those digests should be compared to the originals for verification.

- **Honey-potting** is the process of creating a replica system and luring the attacker into it for further monitoring. A related method (sandboxing) involves limiting what the attacker can do while still on the compromised system, so he can be monitored without (much) further damage. The placement of misleading information and the attacker's response to it is a good method for determining the attacker's motives. You must make sure that any data on the system related to the attacker's detection and actions is either removed or encrypted; otherwise they can cover their tracks by destroying it. Honey-potting and sandboxing are extremely resource intensive, so they may be infeasible to perform. There are also some legal issues to contend with, most importantly entrapment. As previously mentioned, you should consult your lawyers.

3.4 EVIDENCE SEARCH AND SEIZURE

Again, remembering that your specific needs will vary at some point in time, the steps listed here are not meant to be taken in a literal sense. They are not concrete but they may not be perfect for every case you work. Prior to search and seizure, you already have the proper documents filled out and paperwork filed as well as permission form the proper authority to search and seize the suspect's machine (PC, Server, Tapes, etc.).

3.4.1 Step 1: Preparation

Before the investigation, make sure you are prepared! You should sterilize all media that is to be used in the examination process. If you cannot afford new media for each case, then you must make sure that the reusable media is free of viruses and that all data has been wiped from the media. Document the wiping and scanning process. Also, check to make sure that all computer forensic tools (software) are licensed for use. And check to make sure that all lab equipment is in working order.

This is the time to make sure you have a good choice for your computer forensic examiner! Is the computer forensic examiner able to testify in court if necessary? Is the examiner able to explain the methodology used in real-world, simple to understand terminology? Or will the jurors be wondering what bytes, bits, slack space, and hidden files are? What is reasonable doubt in relation to something completely foreign? Better yet, there should be reasonable doubt when used in high-technology. It is reasonable to acquit, because some jurors would not understand, if a file is hidden, how someone else could find it!

When posed with the question of how to explain something se technical to a very nontechnical jury, give the analogy of comparing the computer to a library. The jurors know what a library is. Ask them if they would use the card catalog to look up a book in the library to find what shelf the book is located on. So, use the directory structure to find files on a piece of evidence. Furthermore, if you went through the library, would you not find books on the shelves that were not in the card catalog? The same on the computer. If you do a physical search, you will find data that is not cataloged.

3.4.2 Step 2: Snapshot

Your team needs to take a snapshot of the actual evidence scene. You should photograph the scene, whether it is a room in a home or in a business. Digital cameras seem to be the emerging standard here.

You should also note the scene. Take advantage of your investigative skills here. Note pictures, personal items, and the like. Later on in the examination, these items may prove useful (e.g., for password cracking).

Next, photograph the actual evidence. For simplicity, let us assume, for example, that the evidence is a PS in a home office. Take a photograph of the monitor. What is on the screen? Take a photograph of the PC. Remove the case cover carefully and photograph the internals.

In addition, document in your journal of the PC the hardware, the internal drives, peripheral components, serial numbers, and so on. Make sure you document the configuration of the cables and connections as well (IDE, SCSI, etc.).

You should also label the evidence according to your methodology. And you should photograph the evidence again after the labels have been applied.

Remember to document everything that goes on (who did what, how, why, and at what time). Also make sure that you have your designated custodian for the chain of custody initial each item after double-checking the list you have created at the scene. So, you should now have noted the configuration, the components, and son on. The custodian of the evidence should double-check your list and put his/her initials next to your while at the scene. It is imperative to do this checking at the scene so as dispel the possibility of evidence tainting at a later date.

Finally, you should videotape the entry of all personnel. This may not always be possible, and in some cases or departments, this may be cost prohibitive. However, what you are doing here is taping the actual entrance of your team into the suspect's scene. By capturing your entrance and what you possess on tape, you are setting the stage for refuting any claims that evidence was planted at the scene, and so on. However, when there is a suspicious point of the defence, the transport of the evidence rightly so, by taping the entrance and the transport to the lab, you have a verifiable trail of what you did, when you did it, and how you did it. Is this overkill? I s this possible for every case you work? The taping process is a very solid means of supporting your work and it may one day the required in your methodology.

3.4.3 Step 3: Transport

Assuming you have the legal authority to transport the evidence to you lab: you should pack the evidence securely. Be careful to guard against electrostatic discharge. Also, photograph/videotape and document the handling of evidence leaving the scene to the transport vehicle. Finally, you should also photograph/videotape and document the handling of evidence from transport vehicle to the lab examination facility.

3.4.4 Step 4: Examination

Now, you should prepare the acquired evidence for examination in your lab: This would involve unpacking the evidence and documenting according to you methodology (date, time, examiners, etc.). You should also visually examine the evidence, noting and documenting any unusual configurations (PC), marks, and so on. In other works, you should seize the PC from a home office. This PC usually has a hard drive of size 8 GB

Now, it is time to make an exact image of the hard drive. There are many options here on what tool to use to image the drive. You could use EnCase. You could use the UNIX command DD. You could use Byte Back. You could also use Safe Back. This list could g on and on. It is wise to have a variety of tools in your lab. Each of these tools has its respective strengths. It is recommended here that you work with as many of them as you can. Become so familiar with them that you know their strengths and weaknesses and how to apply each of them. The important note to remember here is: Turn off virus-scanning software.

Next you should record the time and date of the Complementary Metal Oxide Semiconductor (CMOS). This is very important, especially when time zones come into play. For examples, the evidence was seized in California (PDT) and analyzed in Georgia (EDT).

Note: It is crucial to remove the storage media (hard drives, etc.) prior to powering on the PC to check the CMOS!

Do not boot the suspect machine! You can make the image in a number of ways the key is that you wan to do it from a controlled machine. A machine that you know works in a non-destructive/non-corrupt manners.

When making the bit stream image, note and document how the image was created. You should also note the date, time, and examiner. Note the tool used. Again, you are working from your methodology.

Also, when making the image, make sure that the tool you use does not access they file system of the target evidence media. You do not want to make any writers, you do not want to mount the file system, nor do you want to do anything that will change the file-access time for any file on that target evidence media.

After making the image, seal the original evidence media in a electrostatic-safe container, catalog it, and initial the container. Make sure that anyone who comes in contact with this container also inscribes his or her initials on the container. The container should be locked in a safe room upon completion of the imaging.

It may be a wise choice to then make a second bit stream image of your first image. You may need to send this to the suspect's residence or place of work especially if the seized machine was used in the workplace. Finally, the examination of the acquired image begins.

3.5. PRESERVATION OF THE DIGITAL CRIME SCENE

The computer investigator not only needs to be worried about destructive process and devices being planted by the computer owner, he or she also needs to be concerned about the operating system of the computer and applications. Evidence is easily found in typical storage areas (spreadsheet, database, and word processing files). Unfortunately potential evidence can also reside in file slack, erased files, and the Windows swap file. Such evidence is usually in the form of data fragments and can be easily overwritten by something as simple as the booting of the computer or the running of Microsoft Windows. When Windows starts, it potentially creates new files and opens existing ones as a normal process. This situation can cause erased files to be overwritten, and data previously stored in the Windows swap file can be altered or destroyed. Furthermore, all of the Windows operating systems (Windows 2000, XP and especially 2003) have a habit of updating directory entries for files as a normal operating process. As you can imagine, file dates are important from an evidence standpoint.

3.5.1 Evidence Collection Procedure

When the time arrives to begin collecting evidence, the first rule that must be followed is *doing not rush*. Tensions will probably be high and people will want to find answers as quickly as possible. However, if the investigators rush through these procedures, mistakes will be made and evidence will be lost.

The investigation team will need to bring certain tools with them to the incident site. They will need a copy of their incident-handling procedure, an evidence collection notebook, and evidence identification tags. Depending on the type of incident and whether the team will be able to retrieve an entire system or just the data, they may also need to bring tools to produce reliable copies of electronic evidence, including media to use in the copying process. In some cases, legal counsel will want photographs of the system prior to search and seizure. If this is something your legal counsel wants as part of the evidence, also include a Polaroid camera in the list of tools.

Policy and procedure should indicate who is to act as incident coordinator. When an incident is reported, this individual will contact the other members of the response team as outlined in the Incident Response Policy. Upon arrival at the incident site, this individual will be responsible for ensuring that every detail of the incident-handling procedure is followed. The incident coordinator will also assign team members the various tasks outlined in the incident-handling procedure and will serve as the liaison to the legal team, law enforcement officials, management, and public relations personnel. Ultimate responsibility for ensuring that evidence is properly collected and preserved, and that the chain of custody is properly maintained, belongs to the incident coordinator.

One team member will be assigned the task of maintaining the evidence notebook. This person will record the 'who, what, where, when, and how' of the investigation process. At a minimum, items to be recorded in the notebook include:

- Who initially reported the suspected incident along with time, date, and circumstances surrounding the suspected incident.
- Details of the initial assessment leading to the formal investigation.
- Names of all persons conducting the investigation.
- The case number of the incident.
- Reasons for the investigation.

- A list of all computer systems included in the investigation, along with complete system specifications. Also include identification tag numbers assigned to the systems or individual parts of the system.
- Network diagrams.
- Applications running on the computer systems previously listed.
- A copy of the policy or policies that relate to accessing and using the systems previously listed.
- A list of administrators responsible for the routine maintenance of the system.
- A detailed list of steps used in collecting and analyzing evidence. Specifically, this list needs to identify the date and time each task was performed, a description of the task, who performed the task, where the task was performed, and the results of the analysis.
- An access control list of who had access to the collected evidence at what date and time.

Note: A separate notebook should be used for each investigation. Also, the notebook should not be spiral-bound. It should be bound in such a way that it is obvious if a page or pages have been removed.

3.5.2. Storage and Analysis of Data

Finally, the chain of custody must be maintained throughout the analysis process. One of the keys to maintaining the chain is a secure storage location. If the corporation uses access control cards or video surveillance in other parts of the building, consider using these devices in the forensics lab. Access control cards for entering and exiting the lab will help verify who had access to the lab at what time. The video cameras will help determine what they did once they were inside the lab. At a minimum, the lab must provide some form of access control; a log should be kept detailing entrance and exit times of all individuals. It is important that evidence never be left in an unsecured area. If a defense lawyer can show that unauthorized persons had access to the evidence, it could easily be declared inadmissible.

Pieces of evidence should be grouped and stored by case along with the evidence notebook. In an effort to be as thorough as possible, investigators should follow a clearly documented analysis plan. A detailed plan will help prevent mistakes (which could lead to the evidence becoming inadmissible) during analysis. As analysis of evidence is performed, investigators must log the details of their actions in the evidence notebook. The following should be included at a minimum:

- The date and time of analysis
- Tools used in performing the analysis
- Detailed methodology of the analysis
- Results of the analysis [6]

Again, the information recorded in the evidence notebook must be as detailed as possible to demonstrate its trustworthiness. A trial lawyer well versed in the technological world, who knows how to ask the right questions, may find that the *method or circumstances of preparation indicate lack of trustworthiness* (under Fed. R. Evid. 803(6)), to such a degree that a court will sustain, or at least consider, a challenge to the admissibility of the evidence. A properly prepared evidence notebook will help to defeat such a challenge.

Once all evidence has been analyzed and all results have been recorded in the evidence notebook, a copy of the notebook should be made and given to the legal team. If the legal team finds that sufficient evidence exists to take legal action, it will be important to maintain the chain of custody until the evidence is handed over to the proper legal authorities. Legal officials should provide a receipt detailing all of the items received for entry into evidence.

3.5.3. Risk Analysis for evidence collection[16]

Technically the main goal of computer forensics is to identify, collect, preserve, and analyze data in a way that preserves the integrity of the evidence collected so it can be used effectively in a legal case.

The following five are the necessary basic steps in that order to conduct a computer forensic examination. Although documentation is listed as the last step, a well-trained examiner should understand that documentation is continuous throughout the entire examination process.

[16] Thakore: (2009)

1. Policy and Procedure Development
2. Evidence Assessment
3. Evidence Acquisition
4. Evidence Examination
5. Documenting and Reporting

3.5.4. Digital Evidences:

Data from computer systems, networks, wireless communications, and storage devices collected in a way that is admissible as evidence in a court of law.

Basic types of data are collected in computer forensics.

Persistent data is the data that is stored on a local hard drive (or another medium) and is preserved when the computer is turned off.

Volatile data is any data that is stored in memory, or exists in transit, that will be lost when the computer loses power or is turned off. Volatile data resides in registries, cache, and random access memory (RAM). Since volatile data is ephemeral, it is essential an investigator knows reliable ways to capture it.

Network data is the data obtained from network communication. This data includes protocol, IP addresses, ports, number of packets and information in packets.

3.5.5. Evidence Collection:

Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidentiary value. This relates not just to the physical integrity of an item or device, but also to the electronic data it contains.

Certain types of computer evidence require special collection, packaging, and transportation. Consideration should be given to protect data that may be susceptible to damage or alteration from electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices.

Electronic evidence should be collected according to guidelines maintained by the United States Department of Justice. The United States Department of Justice's Cyber Crime web site lists recent court cases involving computer forensics and computer crime, and it has guides about how to introduce computer evidence in court and what standards apply. The important point for forensics investigators is that evidence must be collected in a way that is legally admissible in a court case.

In the absence of departmental guidelines outlining procedures for electronic evidence collection follow your agency's protocol regarding evidence collection. Every agency should develop policies and procedures that establish the parameters for operation and function. An effective way to begin this task is to develop a mission statement that incorporates the core functions of the agency, whether those functions include high-technology crime investigations, evidence collection, or forensic analysis.

3.5.6. Risks Involved:

If computer forensics is practiced badly, you risk destroying vital evidence or having forensic evidence ruled inadmissible in a court of law. Also, you or your organization may run afoul of new laws that mandate regulatory compliance and assign liability if certain types of data are not adequately protected.

The risks associated with collecting and preserving digital evidences can be broadly classified as Integrity Risks and Legal Risks.

Integrity Risks - loss of some or whole part of evidence due to the technology applied to collect evidence. Examples

(1) To reduce the risk of manipulating the evidences on a disk the first step in the investigation process is to clone or image the disk. The investigator has to take care of the original disk while talking an image or clone, as it may crash during copying and evidence may be lost. The reason why one first copies and then hashes is to reduce the risk of crashing the disk when hashing it.

(2) When doing live data collection every user and kernel space tool used to collect data by nature changes the state of the target system. By running any tools on a live system we load them into memory and create at least one process which can overwrite possible evidence. By creating a new process, the memory management system of the operating system allocates data in main memory and then can overwrite other unallocated data in main memory or in the swap file system

(3) During live data collection the signs of intrusions found in images of main memory can be entrusted, because they could be created by acquisition tools.

So before taking any action it must be decided whether to acquire some data from a live compromised system or not. It is very often worth it to collect such information.

(4) Programs used to monitor network traffic can become overloaded and fail to retain all packets captured by the

kernel. Although TCP is designed to retransmit dropped packets, network sniffers are not active participants in the communication channel and will not cause packets to be resent. (E.g. Network monitoring programs like tcp dump, Snort, and Net Witness read network traffic that is buffered in memory by libpcap. If the program cannot read the data quickly enough, libpcap records this fact before discarding unread packets to make space for new ones. The number of packets that were not read by the packet capture program are reported by libpcap when the collection process is terminated. Although it may not be possible to infer the content of lost data-grams, it is useful to quantify the percentage loss.)

(5) Network-monitoring applications may show only certain types of data (e.g., only Internet Protocol data) and may introduce error or discard information by design or unintentionally during operation.

3.5.7. **Legal Risks -** Those companies or individuals that fail to address the regulatory standards risk losing business, paying hefty fines and incurring additional restrictions on future business operations. Examples

(1) Before intercepting the employees email the organization must adopt a policy in which under extenuating circumstances and employees email activities are placed under surveillance. If the policies are not clearly outlined before the surveillance begins the activity could be a breach to the employees' private emails.

(2) Violations of any one of the statutes during the practice of computer forensics could constitute a federal felony punishable by a fine and/or imprisonment. It is always advisable to consult a legal counsel if you are in doubt about the implications of any computer forensics action on behalf of your organization.

(3) HP's investigators acknowledged in a memo that they used an electronic ruse to try to trick CNET's News.com journalist Dawn

Kawamoto into revealing her sources for stories that included HP's confidential information. HP sent a tracer (Web Bug) to discover Journalist's sources. By and large, the Web bug is a widely used legal tool but under certain situations, the use of a Web bug might be considered a violation of false advertising laws if HP used the Web bug to spy on someone, particularly when it espouses a privacy policy that says it doesn't do such things.

3.5.8. Risk Analysis:

The investigator before collecting evidences should first know all the risks involved when using a specific tool to collect evidences. Not calculating risks before collecting evidences may lead to loss of evidences. The risk assessment should be thus carried out before collection process is started. In some cases Risk analysis is valuable even after evidence collection process so as not to repeat the mistake again.

CHAPTER – 4

EVIDENTIARY VALUE OF FORENSIC PROOFS AND PRESENTATION IN THE LAW COURT

4.1 Seizing Evidence[17]

Evidence has to satisfy two tests: admissibility (i.e., it must conform to certain legal rules which are applied by a judge) and weight (i.e., it must be understood by, and be sufficiently convincing to the court—whether there is a jury or a judge acting as a trier of fact) [28].

Once obtaining management authority to proceed (internal company investigation, or via obtaining the appropriate warrant or in unnecessary via a warrantless search) the investigator should do the following:

- Isolate the suspect equipment and eventually identify, isolate, collect, secure and retain data resident within the suspect machine
- Do not alert Suspect (either distract or remove the suspect from the area)

Computer evidence, like all other evidence, must be handled carefully and in a manner that preserves its evidentiary value. This relates not just to the physical integrity of an item or device, but also to the electronic data it contains. Certain types of computer evidence, therefore, require special collection, packaging, and transportation.

[17] Marcella & Menendez

Consideration should be given to protect data that may be susceptible to damage or alteration from electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices.

When dealing with digital evidence, the following general forensic and procedural principles should be applied:

- Actions taken to secure and collect digital evidence should not affect the integrity of that evidence.
- Persons conducting an examination of digital evidence should be trained for that purpose.
- Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved, and available for review [29].

Managers have the responsibility of ensuring that personnel under their direction are adequately trained and equipped to properly handle electronic evidence. Actions that have the potential to alter, damage, or destroy original evidence may be closely scrutinized by the courts.

Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device. As such, electronic evidence is latent evidence in the same sense that fingerprints or DNA (deoxyribonucleic acid) evidence are latent. In its natural state, we cannot "see" what is contained in the physical object that holds our evidence. Equipment and software are required to make the evidence visible. Testimony may be required to explain the examination process and any process limitations.

By its very nature, electronic evidence is fragile. It can be altered, damaged, or destroyed by improper handling or improper examination. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion. The nature of electronic evidence is such that it poses special challenges for its admissibility in court.

Evidence can also be found in files and other data areas created as a routine function of the computer's operating system. In many cases, the user is not aware that data is being written to these areas. Passwords, Internet activity, and temporary backup files are examples of data that can often be recovered and examined. There are components of files that may have evidentiary value including the date and time of creation, modification, deletion, access, user name or identification, and file attributes. Even turning the system on can modify some of this information [30].

Isolating the suspect equipment, ensuring protection of the suspect equipment, and isolating and protecting the suspect equipment from tampering are critical steps in preserving the chain of evidence. Further securing the investigation scene entails taking pictures of the subject's workspace, addressing the issue of latent finger prints, and always being vigilant for the existence of finely crafted electronic booby traps. Booby traps designed to activate if certain sequential keystrokes are not entered properly and to destroy via erasure potentially critical data, hence the destruction of evidence.

STOP, LOOK, LISTEN... Keyboards, the computer mouse, diskettes, CDs, or other components may have latent fingerprints or other physical evidence that should be preserved. Chemicals used in processing latent prints can damage equipment and data. Therefore, latent prints should be collected after electronic evidence recovery is complete [30].

Documentation of the scene creates a permanent historical record of the scene. Documentation is an ongoing process throughout the investigation, thus it is important to accurately record the location and condition of computers, storage media, other electronic devices, and conventional evidence.

When dealing with electronic evidence, general forensic and procedural principles should be applied:

1. Actions taken to secure and collect electronic evidence should not change that evidence.
2. Persons conducting examination of electronic evidence should be trained for the purpose.
3. Activity relating to the seizure, examination, storage, or—transfer of electronic evidence should be fully documented—preserved, and available for review [30].

4.2. Chain of Evidence

The investigator has several tasks ahead of him or her and must follow certain procedures to ensure that the evidence is solid and will hold up in court. The basic criterions, which must exist in order for this to occur, are as follows:

1. No possible evidence is damaged, destroyed, or otherwise compromised by the procedures used to investigate the computer
2. Extracted and possibly relevant evidence is properly handled and protected from later mechanical or electromagnetic damage
3. A continuing chain of custody is established and maintained
4. All procedures and findings are thoroughly documented [31]

The identification of evidence and chain of evidence rules require that the proponent of the evidence show that the evidence has not been tampered with, and that there has not been any irregularity which altered its probative value. *State vs. Roszkowski*, 129 N.J. Super. 315, 323 A2d 531 (App. Div. 1974).

The gathering of evidence in the initial phase of an investigation hinges on proof of admissibility in court that unequivocally and without doubt the conclusions reached by the investigator, usually by way of induction, are sustainable, logical, and defensible.

Ensuring the chain of evidence requires that the forensic investigator log all actions performed on the equipment under review, document any access to the equipment, as well as documenting and identifying who retains control of equipment access log itself.

Additionally, the investigator must identify where the log is stored, document where and how the equipment is stored, and document how the equipment is secured from unauthorized access or use (tampering) (Figure below).

The chain of evidence is designed to demonstrate, without a doubt:

- Who obtained the evidence?
- Where and when the evidence was obtained?
- Who secured the evidence?
- Who had control or possession of the evidence?

Industry standards and expert advice in the area of incident handling have traditionally limited the scope of the "crime scene" to the computer system itself. In a corporate intranet broadening the scope to include the immediate physical work environment around the computer system will significantly improve the context of computer-based evidence [32].

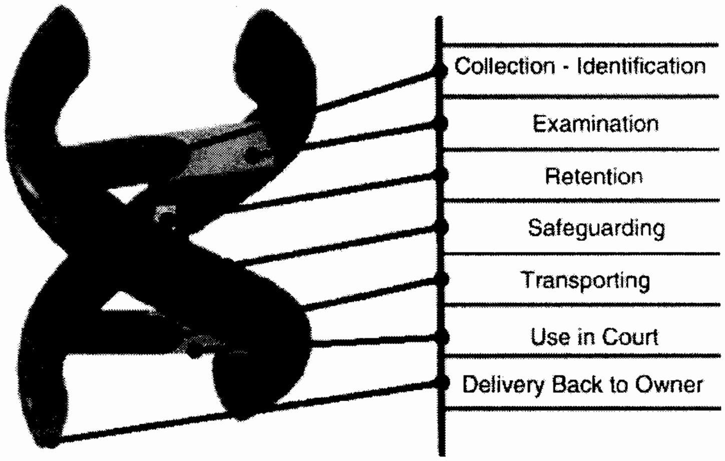


Figure: The "sequencing" of the chain of evidence.

4.3. Chain of Custody

The chain of custody begins when an item of evidence is collected, and the chain is maintained until the evidence is disposed of. The chain of custody assures continuous accountability. This accountability is important because, if not properly maintained, an item (of evidence) may be inadmissible in court.

The purpose of the chain of custody is that the proponent of a piece of evidence must demonstrate that it is what it purports to be. Said differently, there is reliable information to suggest that the party offering the evidence can demonstrate that the piece of evidence is actually in fact, what the party claims it to be, and can further demonstrate its origins and the handling of the evidence because it was acquired.

The chain of custody is a chronological written record of those individuals who have had custody of the evidence from its initial acquisition until its final disposition. These persons in the chain of custody must be identified on an appropriate and official "internal" Evidence or Property Custody Document, which is initiated when the evidence is acquired. Each individual in the chain of custody is responsible for an item of evidence to include its care, safekeeping, and preservation while it is under his or her control.

Because of the sensitive nature of evidence, an evidence custodian should be appointed to assume responsibility for the evidence when not in use by the cyber forensics investigator or other competent authority involved in the investigation. It is important to establish procedures for creating a "custody chain," to include a "running log" of who has had contact with (access to) an item of evidence, for how long, and for what reason(s) (why?).

The organizational representative directly responsible for "first response" to a cyber investigation and who will be the organization's immediate and single source point of contact with the cyber forensics investigator should begin immediately to determine and document a "backward" chain of custody before the investigator arrives.

Collecting information regarding the environment and use of the computer or machine under investigation, in an attempt to answer questions such as the following, prior to the arrival of the forensics investigator, should be of immediate importance:

- Who had access to the machine?
- What level of authorization did all of those individuals having access to the machine have?
- What was the machine used for?
- What external devices did the machine connect to or interact with?
- Which and how many servers did the machine "touch"?
- Where and how will you store and safeguard the machine and the evidence after seizure?
- Will you or an external third-party be responsible for the storage and safeguarding of the seized machine and associated evidence?

It is important to note regarding the above ... establishing (obtaining) answers to these questions is cross applicable to establishing authenticity and a solid foundation for the organization's (or the investigator's) case, even more so than a chain of custody record or log.

At the very least, the evidence or property custody document should include the following information:

- Name or initials of the individual collecting the evidence
- Each person or entity subsequently having custody of it
- Dates the items were collected or transferred
- Department (or Agency or Unit or Team) name and case number
- Victim's or suspect's name
- A brief description of the item seized

4.4. Relevancy and Its Limits

❖ Definition of "Relevant Evidence"

"Relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

- **Relevant Evidence Generally Admissible; Irrelevant Evidence Inadmissible**

All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence that is not relevant is not admissible.

- **Exclusion of Relevant Evidence on Grounds of Prejudice, Confusion, or Waste of Time**

Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence. These rules govern the introduction of evidence in proceedings, both civil and criminal, in Federal courts. Although they do not apply to suits in state courts, the rules of many states have been closely modeled on these provisions.

- **Preliminary Questions (a) Questions of admissibility generally.**

Preliminary questions concerning the qualification of a person to be a witness, the existence of a privilege, or the admissibility of evidence shall be determined by the court, subject to the provisions of subdivision (b). In making its determination it is not bound by the rules of evidence except those with respect to privileges [12].

4.5 Authentication

Before a party may move for admission of a computer record or any other evidence, the proponent must show that it is authentic. This includes laying a "foundation" or demonstrating a basis for why the evidence is relevant and useful. The government must offer evidence "sufficient to support a finding that the [computer record or other evidence] in question is what its proponent claims." Fed. R. Evid. 901(a). See *United States vs. Simpson*, 152 F.3d 1241, 1250 (10th Cir. 1998).

The standard for authenticating computer records is the same as for authenticating other records. The degree of authentication does not vary simply because a record happens to be (or has been at one point) in electronic form. See *United States vs. DeGeorgia*, 420 F.2d 889, 893 n.11 (9th Cir. 1969); *United States vs. Vela*, 673 F.2d 86, 90 (5th Cir. 1982).

But see *United States vs. Scholle*, 553 F.2d 1109, 1125 (8th Cir. 1977) (stating in dicta that "the complex nature of computer storage calls for a more comprehensive foundation").

For example, witnesses who testify to the authenticity of computer records need not have special qualifications. The witness does not need to have programmed the computer himself, or even need to understand the maintenance and technical operation of the computer. See *United States vs. Moore*, 923 F.2d 910, 915 (1st Cir. 1991). Instead, the witness simply must have first-hand knowledge of the relevant facts to which he or she testifies.

4.5. Best Evidence Rule

The best evidence rule provides that the original of a "writing, recording, or photograph" is required to prove the contents thereof. Fed. R. Evid. 1002. A writing or recording includes a "mechanical or electronic recording" or "other form of data compilation." Fed. R. Evid. 1001(1). Photographs include "still photographs, x-ray films, video tapes, and motion pictures." Fed. R. Evid. 1001(2).

An original is the writing or recording itself, a negative or print of a photograph or, "[i]f data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately." Fed. R. Evid. 1001(3) [14].

Fed. R. Evid. 1001(3). Thus, an accurate printout of computer data always satisfies the best evidence rule. See *Doe vs. United States*, 805 F. Supp. 1513, 1517 (D. Hawaii. 1992). According to the Advisory Committee Notes that accompanied this rule when it was first proposed, this standard was adopted for reasons of practicality. Although strictly speaking the original of a photograph might be thought to be only the negative, practicality and common usage require that any print from the negative be regarded as an original. Similarly, practicality and usage confer the status of original upon any computer printout. Advisory Committee Notes, Proposed Federal Rule of Evidence 1001(3) (1972) [13].

In practice, this also includes "mirror imaged" drives or computer hard disk drives and peripherals, so long as the examiner can establish that the mirror image is an exact and precise duplicate and as well as substantiating the methods used to create the mirror image.

4.7. Opinions and Expert Testimony

❖ Testimony by Experts

If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is sufficiently based upon reliable facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case [15].

In *Daubert vs. Merrell* Dow Pharmaceuticals, 509 U.S. 579 (1993), the Supreme Court held that when expert evidence based upon "scientific knowledge" is offered at trial, the judge, upon proper motion by a litigant who challenges the admissibility of the testimony, should act as a gatekeeper and first determine whether the proffered evidence is "reliable"—whether it is evidence that can be trusted to be scientifically valid.

In the aftermath of Daubert, a number of courts had to address the unresolved issue whether the Daubert factors by which reliability was to be tested should also be applied to experts off erring opinion testimony that was not based on clearly identified scientific principles, but which sprung from "technical or other specialized knowledge." Because the clear majority of informed opinion seemed to favor applying a Daubert-like standard to all expert opinion testimony, the Advisory Committee on the Rules of Evidence endorsed that requirement by including the above language in the amendment.

After the drafters first proposed this Amendment, the Supreme Court clarified its Daubert opinion in the case of *Kumho Tire Co. V. Carmichael*, 119 S.Ct. 1167 (1999) by mandating that the trial judges' duty to act as gatekeepers, charged with insuring that only reliable expert opinion evidence be admitted, apply to all forms of expert testimony.

In the Committee Note that follows the Amended language of Rule 702, the drafters emphasized again the nonexclusive checklist courts are to use in judging whether proffered scientific expert opinion testimony meets the Daubert criteria of reliability:

The specific factors explicated by the Daubert Court are:

1. Whether the expert's technique or theory can be or has been tested—that is, whether the expert's theory can be challenged in some objective sense, or whether it is instead simply a subjective, conclusory approach that cannot reasonably be assessed for reliability

2. Whether the technique or theory has been subject to peer review and publication
3. The known or potential rate of error of the technique or theory when applied
4. The existence and maintenance of standards and controls
5. Whether the technique or theory has been generally accepted in the scientific community

In Kumho Tire, the Court recognized that these same factors might not be applicable to all forms of expert opinion testimony, and stressed that these factors constituted not mandates but flexible guidelines, and that courts could look at other factors that, depending on the particular circumstances of a case, were likely to permit an assessment of the reliability of the nonscientific expert opinion testimony offered to the tribunal. The Court also specifically declared that the gate keeping function of trial judges "applies not only to testimony based on 'scientific' knowledge, but also to knowledge based on 'technical' and 'other specialized' knowledge."

While in 1993 the Daubert Court was explicit in stating that the trial judge's focus in determining reliability was to be directed solely toward examining the "principles and methodology, not on the conclusions they generate," in the later case of *General Electric vs. Joiner*, 522 U.S. 136 (1997) the Court backpedaled from this announced position and recognized that "conclusions and methodology are not entirely distinct from one another." The problem of considering both methodology as well as the conclusion is also covered by the language of the proposed amendment to Rule 702, in that it directs a trial court to determine not only whether the methods used by an expert and the principles upon her analysis rests have been determined to be reliable, but also whether "the witness has applied the principles and methods reliably" to the facts that are in controversy in the particular case [16].

The Daubert decision changed the approach to admissibility in at least two significant aspects: (1) henceforth, the test for admissibility of evidence based upon "scientific knowledge" was not to be merely general acceptance in a particular field, but whether proof of "reliability" (validity) of a technique or scientific method could be established; and (2) this determination of reliability was to be made by the trial judge, upon whom the duty now falls to keep evidence based on unreliable "science" from breeching the gates of the edifice where justice is to be dispensed. Is it fair to equate "unreliable science" with "junk science"?

4.8. SPECIAL NEEDS OF EVIDENTIAL AUTHENTICATION[18]

There's a wealth of mathematical algorithms deal with secure encryption, verification, and authentication of computer-based material. These display varying degrees of security and complexity, but all of them rely on a *second channel* of information, whereby certain elements of the encryption/decryption/ authentication processes are kept secret. This is characterized most plainly in the systems of public and private key encryption but is also apparent in other protocols.

Consider the investigative process where computers are concerned. During an investigation, it is decided that evidence may reside on a computer system. It may be possible to seize or impound the computer system, but this risk violating the basic principle of *innocent until proven guilty*, by depriving an innocent party of the use of his or her system. It should be perfectly possible to copy all the information from the computer system in a manner that leaves the original system untouched and yet makes all contents available for forensic analysis.

When this is done, the courts may rightly insist that the copied evidence is protected from either accidental or deliberate

[18] John R.Vacca

> modification and that the investigating authority should prove that this has been done. Thus, it is not the content that needs protection, but its integrity.
>
> This protection takes two forms: a secure method of determining that the data has not been altered by even a single bit since the copy was taken and a secure method of determining that the copy is genuinely the one taken at the time and on the computer in question. For the purpose of this chapter, these elements are collectively referred to here as the digital image verification and authentication protocol [1].

It is argued that when considering forensic copies of computer contents, encryption of data is not the point at issue. Neither are the provisions of the many digital signature protocols appropriate to the requirements of evidential authentication (see sidebar, "Digital IDs and Authentication Technology").

4.9. ELECTRONIC RECORDS AND THE COURTS[19]

4.9.1 Print-outs of electronic records

Parties to disputes in Victoria often rely on print-outs of electronic records (such as database tables, email, websites and spreadsheets). The courts routinely allow such print-outs to be tabled in evidence. This is largely because most documentary evidence in most cases is not disputed by the other party. In situations where the other party disputes the printed version of the record, the court must assess the admissibility and weight of the document.

4.9.2 Electronic records in electronic form

Until recently, Victorian courts have not specifically allowed for the introduction of electronic records in electronic form. This was not the result of an active decision against the use of electronic-

[19] Justine Heazlewood. (2009)

format records, but rather due to technology limitations within the court system.

In its first Practice Note of 2002, the Supreme Court of Victoria changed this position, making specific provision for the exchange of evidence between parties, and its supply to the court, in electronic formats. This Practice Note applies to civil proceedings only at this stage.

In the Practice Note, the Supreme Court places a strong emphasis on agreement between the parties as to the kind of technology and formats used, and their method of exchange.

The Court has also prescribed the exchange of hard-copy versions in the event that parties cannot agree on electronic formats. Example acceptable electronic formats listed in the Practice Note are ASCII, Word Perfect, Microsoft Word, XML, HTML, Microsoft Excel, TIFF and RTF. However, parties can agree on other formats for their own exchange of documents. The court requires documents supplied to it to be in one of these named formats.

The issue is even further advanced in the Commonwealth jurisdiction. The uniform evidence legislation (uel) makes very specific provision for the admissibility of digital documents. Combined with the Electronic Transactions Act, it also affirms that electronic / digital records have the same "value" and weight as paper-based records in evidence.

4.9.3 VERS and electronic evidence

The Standard for the Management of Electronic Records (VERS Standard) specifies:

- system requirements for electronic records management
- what contextual information must be retained to make records sensible in the long term
- a format for long-term preservation of electronic records.

This Standard is mandatory for all permanent public records and is a highly recommended option for long-term temporary records. Following the VERS Standard for your electronic recordkeeping meets all the core requirements of electronic records in evidence:

- The system requirements specify standard and recognized processes, security and integrity measures.
- The long-term format is as open, published and easily accessible as is practicable, and will be readable well into the future.
- The use of digital signatures makes it possible to verify the authenticity of the record and demonstrate that it has not been tampered with.

For these reasons, VERS records are more likely to be admissible as evidence and prove their contents than records stored in other forms.

4.9.4. Recommendation on the Legal Value of Computer Records (1985)[20]

UNCITRAL has made the following recommendations to the State parties and to the International Organizations in respect of legal value of computer records:

1. To review the legal rules affecting the use of computer records as evidence in litigation in order to eliminate unnecessary obstacles to their admission, to be assured that the rules are consistent with developments in technology, and to provide appropriate means for a court to evaluate the credibility of the data contained in those records;

2. To review legal requirements that certain trade transactions or trade related documents be in writing, whether the written form is a condition to the enforceability or to the validity of the transaction or document, with a view to permitting, where appropriate, the transaction or document to be recorded and transmitted in computer-readable form;

[20] United Nations Commission on International Trade Law (UNCITRAL). (2009)

3. To review legal requirements of a handwritten signature or other paper based method of authentication on trade related documents with a view to permitting, where appropriate, the use of electronic means of authentication;

4. To review legal requirements that documents for submission to governments be in writing and manually signed with a view to permitting, where appropriate, such documents to be submitted in computer-readable form to those administrative services which have acquired the necessary equipment and established the necessary procedures;

The General Assembly called upon Governments and International Organizations to take action where appropriate, in conformity with the Commissions' recommendations so as to ensure legal security in the context of the widest possible use of automated data processing in international trade

4.9.5. SUMMERY OF UNCITRAL MODEL LAW

1. There should not be any discrimination between data message and paper document.

2. Data message is equivalent to writing and original.

3. Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message or referred to in the data message.

4. Where the law requires information to be in writing, that requirement is met by data message if the information contained therein is accessible so as to usable for subsequent reference.

5. Where law requires a signature of a person, that requirement is met in relation to a data message by following the electronic process7.

6. Where the law requires information to be presented or retained in its original form that requirement is met by a data message by following the criteria laid down in model law.

4.9.6. Admissibility and Evidential weight of data message[21]

In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) On the sole ground that it is a data message; or

(b) If it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored, or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

The purpose of Article 6 of UNCITRAL Model Law is to establish both the admissibility of data messages as evidence in legal proceedings and their evidential value.

With respect to admissibility, data messages should not be denied admissibility as evidence in legal proceedings on the sole ground that they are in electronic form. As regards the assessment of the evidential weight of a data message, the evidential value of data messages should be assessed depending on whether they were generated, stored or communicated in a reliable manner.

4.9.7. UNCITRAL Model Law on Electronic Signatures (2001)

The purpose of this Convention is that the increased use of electronic authentication techniques as substitutes for handwritten

[21] Dr. Mohammed Zaheeruddin: (2009)

signatures and other traditional authentication procedures has suggested the need for a specific legal framework to reduce uncertainty as to the legal effect that may result from the use of such modern techniques (electronic signatures).

This Convention calls for uniform legislative provisions to establish the basic rules relating to electronic signatures.

The new Model Law equally reflects the principle that no discrimination should be made among the various techniques that may be used to communicate or store information electronically, a principle that is often referred to as 'technology neutrality'. Article 6 (1) of the Model Law provides that an electronic signature satisfies the requirement of an actual signature if the electronic signature is "as reliable as was appropriate for the purpose for which the data message was generated or communicated in light of all the circumstances. An electronic signature is deemed to be reliable if the signature creation data are linked exclusively to the signatory and under that person's exclusive control and if any alterations of the signature or accompanying data to which it relates are detectable.

4.9.8. Legal recognition of electronic communication

A communication or a contract shall not be denied validity or enforceability on the sole ground that is in the form of an electronic communication. Where a law requires that a communication or a contract should be in writing, that requirement is met by an electronic communication.

The Conventions has addressed the issues of Time and Place of dispatch and receipt of electronic communications, what constitutes an invitation to make offer, Use of automated message systems for contract formation, availability of contract terms and consequences of error in electronic communications.

4.10. THE UNITED ARAB EMIRATES FEDERAL LAW NO. (1) OF THE ELECTRONIC TRANSACTIONS AND COMMERCE, 2006[22]

In order to meet the changes and developments that have been taking place at international level in the field of electronic commerce and to implement UNCITRAL Model Law on Electronic Commerce and other related documents, the United Arab Emirates Federal Government has enacted Law No. (1) of the Electronic Transactions and Commerce, 2006. This law shall apply to electronic records, documents and signatures pertaining to the electronic transactions and commerce.

The objectives of the this Code are to protect the rights of electronic dealers, facilitate electronic transactions, remove the obstacles in conducting of e-commerce, facilitate the correspondence between the Government and non-government bodies, minimize the falsification of the electronic correspondence and to establish unified principles to the rules, regulations and standards in respect of the authentication and safety of the electronic correspondence. The Code also aims to support the development of the electronic commerce in the local and international arenas, by way of using electronic signature.

The UAE Code on Electronic Transactions and Commerce contains Ten Chapters; definitions part, validity of law and its objects24, requirements of electronic transactions, Electronic Transactions, Protected Electronic Records and Signatures, Provisions in connection with the certificates of electronic approval and the approval services, recognition of the certificates of the electronic approval and the foreign electronic signatures, Governmental use of the electronic records and signatures, Sentences, and final provisions.

4.10.1. Validity of Electronic Correspondence

The electronic message shall not lose its legal effect or its capability of being executed due to the fact that it is in an electronic form.

[22] Federal Law No. (1) 2006: (2009)

4.10.2. Keeping documents, record or information

The condition of keeping of a documents, record or information may be fulfilled if document or record or information is kept in the form of an electronic record by following the conditions laid down in the code.

4.10.3. Equal to a document in writing and signed on document

If the law provides that any statement or document or record or dealing or evidence shall be in writing or provides that certain results shall ensure for not writing any matter, the electronic document or record shall fulfill such condition if the stipulations laid down in the code have been complied.

The reliance can be placed on electronic signature and the certificates of the electronic approval issued according to the provisions of law.

4.10.4. Admission and Evidentiary value of the Electronic Evidence

1. None of the following shall be inconsistent with the admission of the electronic signature as evidence:

(a) That the message or signature is in an electronic form.
(b) That the message or signature is not original or in its original form whenever such electronic message or signature is the best evidence which is reasonably contemplated to be obtained by the person relying upon it as evidence.

2. Regarding the evaluation of the evidential value of the electronic information, the following ingredients shall be taken into consideration:

(a) The extent of the possibility of the reliance in the manner by which one or more of the operations of the insertion of the information or its making or preparation or storing or submission or sending.

(b) The extent of the possibility of reliance upon the manner used in the preservation of the safety of the information.

(c) The extent of the possibility of relying upon the origin of the information if such source is known.

(d) The extent of the possibility of relying upon the manner by which the identity of the creator is confirmed.

(e) Any other ingredient pertaining to the subject.

3. Unless the contrary is proved, it is presumed that the protected electronic signature:

(a) Can be relied upon
(b) It is the signature of the concerned person
(c) It is affixed by that person with the intention of signing and approving the electronic message whose issuance is attributed to such person.

4. Unless the contrary is proved, it is presumed that the protected electronic record:

(a) Did not change since it was made.

(b) Shall be relied on.

4.10.5. Validity of Electronic Transactions

1. The contract shall not lose its validity or the possibility of its execution due the fact that it is made by one or more electronic correspondence.

2. A contract may be made between automated electronic media, comprising two electronic information systems. It means conclusion of a contract without personal or direct intervention of natural person.

3. The electronic message shall be deemed to be issued by the creator if the latter issues such message himself/herself/itself.

4.10. FEDERAL LAW NO (1) OF THE YEAR 2006 IN RESPECT OF THE ELECTRONIC TRANSACTIONS AND COMMERCE OF UNITED ARABS EMIRATES. ARTICLE (10) PROVIDES AS UNDER:

4.10.1. ADMISSION AND EVIDENTIAL VALUE OF THE ELECTRONIC EVIDENCE

1. None of the following shall be inconsistent with the admission of the electronic signature as evidence:

   A. That the message or signature is in an electronic form.
   B. That the message or signature is not original or in its original form whenever such electronic message or signature is the best evidence which is reasonably contemplated to be obtained by the person relying upon it as evidence.

2. Regarding the evaluation of the evidential value of the electronic information, the following ingredients shall be taken into consideration:

   A. The extent of the possibility of the reliance in the manner by which one or more of the operations of the insertion of the information or its making or preparation or storing or submission or sending.

   B. The extent of the possibility of reliance upon the manner used in the preservation of the safety of the information.

   C. The extent of the possibility of relying upon the origin of the information if such source is known.

   D. The extent of the possibility of relying upon the manner by which the identity of the creator is confirmed.

   E. Any other ingredient pertaining to the subject.

3. Unless the contrary is proved, it is presumed that the protected electronic signature:

   A. Can be relied upon.

   B. It is the signature of the concerned person.

   C. It is affixed by that person with the intention of signing and approving the electronic message whose issuance is attributed to such person.

4. Unless the contrary is proved, it is presumed that the protected electronic record:

   A. Did not change since it was made.

   B. Shall be relied on.

CHAPTER – 5

CONCLUSION AND RECOMMENDATIONS

5.1 Limitation & Hurdles:

There are both practical and legal hurdles in the way to fight against electronic fraud, which are discussed as follows:

5.1.1 Practical Issues:

The practical issues, which impose limitations and create hurdles, are summarized as under.

5.1.2. Globalization of Economic System:

The globalization of economic system and the technologies supporting it have generally made it easier for offenders to commit electronic frauds without fear of being apprehended. It usually involves compel, lengthy and expensive investigations. It demands a great care and diligence because the evidence obtained must meet a high standard to ensure successful proceedings and consequent freezing and forfeiture capture of the culprit and their successful trial culminating in conviction.

5.1.3. Multi-National Nature of Offence:

The offence of electronic fraud being a multi-national nature of offence, the time consumed by mutual legal assistance requests is a major problem for investigators, particularly in cases where trail of evidence must be traced through a series of jurisdictions and legal proceedings which must be completed and requirements which must be met before the case can then pass to the next jurisdiction, where the process must be repeated. The offenders understand these sophistications and structure their activities to make advantage of it.

5.1.4. Heavy Costs:

Heavy costs that may incur and the scarcity of resources may pose a serious obstacle particularly for countries already impoverished by such like offences. The financial cost of assembling an effective team of investigators to trace the offenders and the sufficient number of people with necessary expertise may not be available. In some cases law firms, investigators and other may be willing to work on the basis of fees which are contingent on a successful investigation and ultimate recovery of assets derived through electronic frauds but practically it is impracticable when some jurisdictions prohibit such practices and it may give rise to conflict of interests which may jeopardize the successful legal proceedings.

5.1.5. Lack of Seriousness:

It is mandatory for financial institutions, doing their business in the developing countries like Pakistan, to have and effective system of due diligence in their organization. This obviously needs a big amount to be spent on this activity, which ultimately reduces the business / profitability of these financial institutions. It has been observed that, usually, proper attention is not given by these finical institutions to tackle the problem of electronic frauds.

5.1.6. Scarcity of Resources (Financial, Human & Technical):

We know that enforcement of any policy requires financial, human and technical recourses. The third world countries do not have surplus funds to be spent to combat electronic frauds.

Furthermore, skilled human resource is also a major obstacle for these countries in the way of handling computer frauds. The available human resource is also not technically equipped according to our culture, environment and requirements to effectively overcome the situation.

5.1.7. Transfer of Evidence & its Admissibility:

The practical problem also arise from the need to transfer evidence from one jurisdiction to another in a manner which ensures that it will be admissible and credible where it is to be used in the court. Electronic fraud cases often straddle of the boundary between civil and criminal proceedings or may be considered civil in one jurisdiction and criminal in another. Many jurisdictions impose higher standards for criminal evidence, which may make civil recovery easier where it is feasible, but may make evidence gathered for civil proceedings insufficient to meet the standards for criminal ones. To establish authenticity, witnesses such as bank officials, computer forensic experts or investigators must often have to travel to foreign jurisdiction to give personal testimony, which generates costs and demands on their employers. Recent developments may make such testimony by video conference possible but this also raise legal and technical issues, and in some cases the evidence thus given may not be as effective as required.

5.1.8. Disposition of Recovered Assets & Competing Crime:

In the final stage practical problem may also arise over the ultimate disposition of the assets recovered from the offenders. There may be competing claims form countries other than victim country and competing claims from compensation from various individuals and companies, which may have suffered losses within the victim country. There may also be competition between proposals to use the assets to compensate individuals and proposals to use them for projects to rebuild political, economic and legal institutions, the reduction of external debt or various public works.

5.1.9. Culture:

Cultural values also have their impact upon the efforts to electronic frauds. In Pakistan, where people do not feel that fraudulent activities are crime and they without any hesitation get involved in different businesses which ultimately lead to electronic frauds at small or large scale. The evil practices like tax evasion drug dealing, smuggling and human trafficking are common on our people. In their estimation it is not a foul play, so they consider it as permissive and quite correct, which promotes the evil of electronic frauds.

5.1.10. General Awareness of Public:

People in the countries like Pakistan are generally unaware of the fact that cyber crime not only slaughtering our economic and social fiber but also damaging our image and fame in the eyes of the world. A big chunk of population has no concern with national interests, as they are so much busy in meeting, through whatever means, the finical needs of their families that they have no time to even talk or think over issues like it.

5.1.11. Legal Issues:

There are certain legal issues which impose limitations and create hurdles in the flight against cyber crime. There are discussed in some detail as under:-

5.1.12. Absence of Legislation:

Cyber Crime is a burning issue for almost last 15 years, but unfortunately most of the third world countries are very slow and lethargic to enact the legislations to effectively and rationally combat this problem.

In Pakistan recently an Ordinance has been promulgated with the nomenclature as PECO-2009 but the same is still be presented in Parliament for satisfaction.

5.1.13. Discrepancies in Procedural Law:

A major concern in all cases of a multinational nature is the reconciliation of differences or discrepancies in the relevant substantive and procedural laws of the countries involved. The issue of this nature commonly arise more seriously in cases involving civil law and common law jurisdictions, both having involved fundamental legal differences and asymmetries which can cause difficulties even between relatively similar legal cultures, particularly with respect to the exact definition of criminal offences and areas such as the liability of corporations or legal persons.

5.1.14. Discrepancies Relating to Fundamental Legal Principles:

Another significant area of discrepancy between legal systems relates to fundamental principles governing protection of civil liberties, privacy, disclosure of prosecution information and evidence to the defense in criminal cases and other substantive or procedural safeguards. While the substance of many of the principles may be similar in many countries, the manner in which each country's laws enunciate such principles and the ways in which their courts apply them may be quite different. Thus, even through evidence was properly obtained by means of lawful search and seizure in one country, for example, this may be difficult to establish in the courts of another. Conflicting legal rules may impede the cooperation and coordination operating under the laws of different countries.

5.1.15. Application of Civil/Criminal Proceedings for Electronic Actions:

There are also discrepancies between the approaches taken by different jurisdictions to the use of civil, as opposed to criminal, proceeding regarding the electronic frauds. Generally, criminal actions allow for more effective remedies, but their penal nature establishes a higher burden of proof and more stringent procedural safeguards, which must be met before they can be applied. This higher burden is commonly cited as a major obstacle to the ability of investigators to locate evidence and trace transactions held / made through nominees, s heel corporations, foundations, lawyers who are barred from disclosing their client's identities and institutional secrecy on the part of bank and financial institutions in jurisdictions where it is established. Civil proceedings on the other hand, offer more realistic burdens of proof, but in many jurisdictions legislation and the courts do not regard such proceedings as adequate to overcome secrecy provisions. In some cases the best approach appears to be a combination of the two, in which criminal proceedings are used to obtain access to necessary information (the equivalent of civil discovery), and then civil proceedings brought as a more expeditious way to seek actual freezing and recovery of the illegally derived assets through cyber frauds. The approach is possible in some civil law countries, but very hard in common law jurisdictions.

5.1.16. Discrepancies between Evidentiary Procedures of Rules:

As already noted, discrepancies between the evidentiary procedures or rules ion different jurisdictions are also frequently encountered. Evidence gathered by regular means in one jurisdiction may not meet he standards for admissibility in other, particularly if both civil and criminal proceedings are involved. Other rule also limits admissibility. Evidence furnished to one country under mutual legal assistance agreements may not be used in a third country or for proceedings other than those for which it was originally obtained.

5.1.17. Implications of Transferring Witnesses between the Jurisdictions:

The Practical problem associated with transferring witnesses from one jurisdiction to another any also has legal implications. Assuming that resources can be found to transfer the witness, the questions of whether he or she can be transferred and compelled to testify against his or her will and potential criminal liability for refusal to give evidence or perjury must sometimes be dealt with. In some cases, the question of whether a foreign witness can seek immunity from prosecution for related or unrelated offences and if so, extent of such immunity may also arise.

5.1.18. Competing judgment regarding Cyber Frauds:

The practical problem arises when there are conflicting claims regarding the recovered assets because their recovery is sought by other countries or individuals claiming criminal victimization or criminal damages, may compounded by additional legal problems. Proceedings brought in more than more than one jurisdiction may result in completing judgments claiming the assets, which have to be reconciled before the courts of the country where the assets are located, for example. Civil/Criminal law claims which confiscate assets for the benefit of the state or which would be used to compensate criminal victims.

5.2. RECOMMENDATIONS & SUGGESTIONS – FUTURE STRATEGY:

It is recognized at every level that the problem of Cyber Crime has become such a global threat to the integrity, reliability and stability of the financial and trade systems and even moral fabric structures as to require strict and effective counter measures by the international community in order to deny safe heavens to criminals. We know that "bad money" earned through cyber frauds should not become part of the economy as it should have bad effects on the economic system and cause damage to smooth growth of its development.

It is needed to make special efforts against the Cyber Crimes linked to different financial & social activities.

On the basis of this study, below mentioned recommendations are suggested for Government, Financial Institutions and Law Enforcing Agencies.

5.3. RECOMMENDATION & SUGGESTIONS FOR GOVERNMENT:

The following recommendations are suggested for the government.

5.3.1. Introduction of Legislation:

Cyber Crime is a burning issue for almost last 10 years, but unfortunately in Pakistan no law was finalized and promulgated until recently, exclusively to combat this problem. Hence a comprehensive legislation must be promptly enforced after getting passed the same from the Parliament and should not sufficed to introducing Ordinances.

5.3.2. Allocations of reasonable budget:

Reasonable budget must be allocated effectively fight against this problem so that an up to date system may be introduced / run in order to control the complex cyber fraud transactions.

5.3.3. Adoption of Broad Based and Multi dimensional Strategy:

Fight against cyber crime is an ongoing process. The government should adopt strategies that make the anti cyber crime operations as fool proof. We need to identify the parallels between effective international capabilities to investigate and prosecutes all types of cyber crimes.

5.3.4. Introduction of Crime Control Strategy:

Government must introduce a crime control strategy to get the following objectives.

- Combat cyber crime by denying criminals access to financial institutions and by strengthening enforcement efforts to reduce the threats.
- Seize the illegally derived assets of criminals through aggressive use of forfeiture laws.

- Enhance bilateral and multilateral cooperation against all types of cyber crimes by working with foreign governments to establish or update enforcement tools and to implement multilateral cyber frauds strategies.
- Target offshore centers for international cyber fraud, counterfeiting, electronic access device schemes and other financial crimes.

5.3.5. Mutual Interaction:

The authorities must focus establishing international standards, obtaining agreements to exchange information, establishing linkages for cooperative investigations and overcoming political resistance in various key jurisdictions to ensure cooperation among them.

Holistic efforts are required to fight the menace of Cyber Crime with effective cooperation among various departments and agencies working in this sector with in the country. So, there must be an independent body, which plays an effective role as central unit for all organizations (i.e law enforcing agencies, capital market, financial institutions and business community) dealing with cyber fraud problem. So that these may share their knowledge and experiences in order to strengthen each other.

5.3.6. Establishment of a Strong and Reliable Data Base:

Government is required to increase the jurisdiction of NR3C, so it has all relevant information about an individual, which not only provide his personal data but also its financial background.

5.3.7. Provision of Training and Technical Assistance:

Government must take imitative that law enforcing and regulatory agencies should be provided training on cyber fraud countermeasures and financial investigations. The members of law enforcing agencies and financial regulatory bodies must be sent to renowned international institutions for training courses. These courses must give financial investigators, bank regulators, and prosecutors the necessary tools to recognize, investigate and prosecute cyber crime, financial crimes and related criminal activity. These courses must be arranged in every part of the country.

5.3.8. Promoting Public Awareness:

We know that there is a strong link between poverty and illegal activities. Therefore, it is needed to create culture of obeying laws, change of behaviour and conviction to effectively fight against cyber crime.

Computer frauds cannot be checked through legislation alone therefore there is need to strengthen national social and political institutions, promoting rule of law, tacking corruption, improving economic status of people and raising their standard of living.

Awareness and guidance must be provided to general public through seminar s, publication and radio / TV programmes so that they may become morally aware of the repercussions of electronic offences.

5.4. RECOMMENDATION & SUGGESTIONS FOR LAW ENFORCING AGENCIES:

Computer frauds being a complex nature of crime, the law enforcing agencies will have to be equipped with ability and courage to fight against this evil. In this regard, there are following recommendations and suggestions for law enforcing agencies.

a) The law enforcing agencies in Pakistan are shy of trading on the difficult terrain of cyber investigations that are both complex and time-consuming. The fundamental reason seems to be, apart from constraints of other pressing professional demands, lack of expertise o n the part of investigation officers. Hence there is urgent need to run basic and advance courses designed by experts for the trainers as well as field officers of all the concerned law enforcing agencies. Such courses could be managed jointly at the regional level with coordination of UNDP and other international agencies for improving the professional skills of the intelligence, investigative and prosecution personnel of the law enforcing agencies.

b) In order Anti Cyber Crime operations get adequate priority and required resources, there is need to establish separate dedicated wings within various law enforcing agencies like Police, ANF, NAB and FIA etc. These wings should be well equipped with modern technical and logistics facilities and other resources.

c) A national fund for eradication of cyber crimes may be set up which may receive fixed percentage for all forfeited assets from all concerned agencies. This fund should be utilized for:-

   i) Setting IP of an efficient communication network between the law enforcing agencies.

   ii) Development of a well established intelligence data regarding the activities of cyber criminals; and

   iii) Arranging training programmes for the personals of the law enforcing agencies.

d) Regular exchange of intelligence reports / data on transnational computer crime gangs, their network and modus operandi should be ensured between the different national law enforcing agencies as well as international agencies. In that regard it should also be ensured that a practical and efficient mechanism is established and developed.

e) There is need to educate and sensitize the concerned government agencies to the ill-effects of Cyber Crimes and the need to combat it by adoption of stringent counter measures through domestic policy as well as offering meaningful co-operation and assistance to international bodies and law enforcing agencies.

5.5. CONCLUSION

The international community recognizes the cyber crime as a serious challenge and a threat not only to the soundness of the financial institutions but also to the integrity, reliability and stability of the government structures around the world. No doubt many strong global and regional initiatives have been taken to overcome the problem but there is an ardent need of more co-operations at global level to fight against this menace.

Computer crime with boundary-less chain transactions becomes an intricate and sophisticated process. Criminals are continuously adopting new routes and channels for their activities. Such complexities are compounded by corollary factors such as gaps in domestic legislation, perceived defects in the legitimacy of process initiated to establish facts and determine culpability and last but not the least, the deficiencies in international co-operation. In any case the complexities of the issues are to be addressed on the national, regional and global level. Notwithstanding the difficulties or complexities, the dimensions of the problem demand joint and conclusive action by the international community. For this action to be effective, the international community must embark upon sustained efforts to forge consensus. Such consensus needs to be based on a common perception and appreciation of its foul impacts on the social, political and financial stability and finally agreement on the international aspects of the problem that require genuine and meaningful co-operation. The UN can play an important role to overcome this problem. It has already emphasized the need of international co-operation and working together in finding solutions to this colossal problem, which will make it possible to give fruitful results.

Since the word "Cyber" was hitherto unknown and stranger in Pakistan till the early 90s and soon became a cause of concern to the financial institutions as well as to the law enforcement agencies. Pakistan being a member of international community had to take steps to incorporate legal provisions regarding the cyber activities by way of different legislations. However it could become possible for Pakistan to introduce a formal law in 2002 in the shape of Electronic Transaction Ordinance 2002. Through this legislation Electronic transactions were given legal recognition and acceptability viz-a-viz the documentary transactions. Under this law a certification and legal recognition was given to Electronic forms of documents, electronic signatures and advance electronic signatures. A certification council was established to grant and renew accreditation certificates, monitor compliance with the provisions of Ordinance, establish and manage the repository, encourage the uniformity of standards and practices and to make recommendations to the appropriate authority in relation to the matters covered under this Ordinance.

Under the above law the illegal activities like provision of false information, issue of false certificates, violation of privacy of information and damage to information system etc. were made penal offences inviting different punishments with imprisonments and fines.

In 2007 Electronic Fund Transfer Act has been promulgated to supervise and regulate the payment system and to provide standards for protection of the consumer and to determine respective rights and liabilities of the financial institutions and other service providers, their consumers and participants. In short the Act addresses issues like operation of payment system including the clearing and settlement obligations of the parties involved, supervisory role of SBP, documentation requirements by the participants, liabilities of parties in payment systems and legal proceedings in case of any conflict, finality and irrevocability of settled transactions etc. The act has also given legal coverage to PRISM (this is Pakistan's RTGS system).

The above Act also provides punishments for willfully giving false information, violations effecting electronic commerce and cheating by use of electronic device.

Very recently President of Pakistan has promulgated Prevention of Electronic Crime Ordinance 2009 which specifies different criminal acts relating to cyber crime and provides different punishments therefore, including criminal data access, data damage, system damage, electronic fraud, electronic forgery, misuse of electronic system or a device, unauthorized access to code, misuse of encryption, malicious code, cyber stalking, spamming, spoofing, unauthorized interception and cyber terrorism etc.

A detailed procedure of prosecution and trial of the offences has been given under this law. There is provision to establish a specialized investigation and prosecution cell within FIA to investigate and prosecute the offences under this ordinance. There is a special chapter of International cooperation regarding information/evidence and the investigation and trial proceedings.

The government has established National Response Center for cyber crime (NR3C) in FIA.

Since 9/11 cyber crime has substantially received more attention. After these attack Pakistan and the whole region surrounding it is in direct focus of the world. The government of Pakistan has started to develop the concept of coordinative fight against terrorism and terrorist financing which now is mostly being done through cyber activities. The evidence shows that the terrorist groups which for their activities arrange finance through money laundering practices mostly prefer to utilize electronic fund transfers. They avoid hard cash transactions which are considered unsafe and prone to be detected easily. Strict vigilance on the borders of the countries also forestalls hard cash movement across the borders. In such circumstances electronic fund transfer is considered safer by the terrorists.

APPENDIX-I

Top 10 Cyber Attacks of All Time[23]

Case # 1

Probably the most notorious hacker of all times, **Kevin Mitnick**, was not a programming genius, but he was responsible for some of the most hyped cyber attacks in history. He started by tricking the Los Angeles bus punch card equipment to get free rides, continued with phone phreaking and then went serious during an almost 2.5 year long hacking spree, when he broke into numerous computers coast to coast stealing corporate data, scrambling phone networks and even breaking into the national defense warning system. He was eventually busted by the FBI and convicted to five years in prison for trespassing into Digital Equipment Corporation's (DEC) network and stealing proprietary software. Although Mitnick did succeed in various cyber attacks, including major ones, he admitted that the most powerful weapon he used was "social engineering", which proves that technological vulnerabilities are not always the weakest link, while attention to detail and healthy suspiciousness can do more than the most advanced security systems out there.

Case # 2

Kevin Poulsen, a.k.a Dark Dante, is another hacking idol. He started his "career" at 17, when he gained access to the Internet's predecessor, ARPANET. The network was still being developed and he exploited an existing loophole to temporarily gain complete control over the nationwide network. However, he became a real celebrity after his famous trick with LA's KIIS FM radio, which brought him a brand-new Porsche, among other valuable items, and the fame of a "phone wiz". The station was running a contest at that time and would give a posh sport ride to the 102th caller. Poulsen successfully hacked into the city's phone system, seized control of all the lines, blocked all incoming calls and eventually made sure he was the lucky number 102. Indeed, almost all of his hacking coups have been carried out using regular telephone lines. Shortly after the Porsche trick, he reactivated old Yellow Page escort phone numbers for an acquaintance of his who ran a virtual agency. Despite his luck and conspiracy skills, Poulsen was arrested in a supermarket after a nation-wide raid and did five long years in prison to later become a senior editor for Wired News writing about IT security.

[23] Top-10-cyber-attacks-of-all-time: (2009)

Case # 3

Robert Tappan Morris was the person behind the first computer worm known as the "Morris worm" - a self-replicating program that quickly spread over the vast spans of the global network and caused substantial damage to thousands of computer systems. Although the hacker allegedly intended to use the worm to probe the real size of the Internet, his creation brought over 6000 computers worldwide to their knees, making them completely unusable. Morris became the first person to be prosecuted under the 1986 Computer Fraud and Abuse Act and was sentenced to three years of probation, 400 hours of community service and a fine of $10,500.

Case # 4

Adrian Lamo's hacking into the networks of high-profile organizations like Microsoft and the New York Times made him one of the most renowned hackers in history. He breached the security barriers of major companies and anonymously pointed them at existing vulnerabilities. Although he did not have any malicious intent, his intrusions were not authorized and therefore considered cyber crimes. He never used his home line for any of his provocative attacks, preferring public access points, such as Kinko's, cafes and libraries - and that's what earned him the nickname of "homeless hacker". Always on the move, he successfully hacked companies we all know very well: Yahoo!, Bank of America, Cingular and Citigroup. For a certain period of time, he managed to get away with his vigilante acts, but he made a big mistake after he broke into The New York Times intranet and LexisNexis account containing confidential data about employees, contributors and partners. Although Lamo informed the company about this vulnerability and offered assistance in fixing it, charges were shortly filed against him and the hacker's desire to help was punished by an ample fine, half a year of home confinement and two years of probation.

Case # 5

The coolest kid on the hackers' block, **Jonathan James** became the first underage offender who was sentenced to a half a year of in-house arrest with probation (although he eventually did this time in prison for violation of parole). His targets included the most respectable an high-profile organizations, such as NASA and DTRA

(Defense Threat Reduction Agency), a special agency within the Department of Defense responsible for reducing the threat to the United States and its allies from weapons of different types, including nuclear, chemical and biological. The software he installed on DTRA's servers allowed him to intercept personal emails and capture access details of a large number of top-level officials within the agency. In NASA's case, he simply stole the software that controlled the Space Station's environment parameters, such as temperature and humidity. NASA estimated the aggregated losses at over 1.7 million dollars, although James remained extremely skeptical about the quality of the space agency's code and its real value.

Case # 6

Russian hacker **Vladimir Levin** became the first person in history to rob a bank without a hockey mask, a shotgun and a diamond drill. In 1995, he penetrated Citibank's security systems and stole 10 million dollars that he later transferred to multiple accounts in Europe in the US. Although this was an elegant job, he was shortly arrested in the UK.

Case # 7

In 1996, an American hacker by the name of **Timothy Lloyd** managed to inject just six lines of malicious code into the network of Omega Engineering, one of the key suppliers for NASA and the US Navy. Under certain conditions, the "bomb" exploded and completely destroyed the software used in Omega Engineering's production processes. This time, things got really serious, as the company estimated its losses at a staggering $10 mln.

Case # 8

The Melissa virus became one of the largest Internet pandemics in history. It was written by **David Smith** from New Jersey with no direct intent to harm other computers, but soon proved to be very efficient in replicating itself, which quickly resulted in clogged communication lines and mail servers going down around the globe. The concept behind this macro virus was very simple. Melissa spread through Microsoft documents (Word and Excel) and mass-mailed itself when infected attachments were downloaded and opened. Third-party variations of Melissa were much more dangerous and targeted critical system files and users' data. The unfortunate author of the original version, David Smith, was sentenced to 20 months in a federal prison and a fine of 5000 dollars.

Case # 9

Michael Calce, known on the Internet as MafiaBoy, is another prodigy who "joined the dark side" at just 15 and caused one of the most notorious DDoS attacks in history against such companies as Yahoo!, Amazon.com, Dell, Inc., E*TRADE, eBay, and CNN between February 6 and Valentine's Day in 2000. He secured access to 75 computers in 52 networks and launched a massive packet bombardment of these sites. The estimated amount of global economic damages from these attacks reached 1.2 billion, according to industry experts. Due to the hacker's age, he was only sentenced to 8 months of "open custody", a year of probation, restricted use of the Internet and a minor fine.

Case # 10

A hacker group called **MOD** (Masters of Deception) was the ultimate example of how dangerous hackers can be when they act together. From 80s to 90s, this NY-based cybersquad successfully controlled all major telephone and X.25 networks, as well as backbones of the Internet that was gaining popularity at that time. MOD members reached unparalleled mastery in anonymous access to various systems using alternate handles, social engineering, discovery and exploitation of system vulnerabilities and loopholes, misdirection, backdoors and trojan horses. Although the group gained access to a huge array of confidential and secret information, none of it has ever leaked outside the group thanks to MOD's philosophy and nearly religious principles. As a result of a large-scale operation by FBI and the secret service task force, 5 members of the group were arrested in 1992 and pleaded guilty in court.

The examples above are just the tip of the iceberg. Many more hackers have left their trace in history and demonstrated that knowledge and ingenuity combined with good social skills can lead to tragic outcomes. Since then, computer security has evolved into a separate industry, thousands of products have been released and countless IT security books have been published. However, just as in case with planes, tragedies mostly occur due to human factors - negligence, excessive trust and lack of proper attention to the design of isolated networks containing information that should not go public. Hacking a real and hackers can punish you for not assigning the right priority to IT security in your company or home. When online, trust only your intuition, experience and reliable security tools — and never let strangers cross the line of your online comfort zone.

APPENDIX-II

CYBER CRIME YEAR-WISE DATA (NR3C FIA)[24]

Year	No of cases reported	No. of cases registered (FIRs Registered)	Sent up cases (disposed off)	Under Trial in Court (Challan Submitted)	Convicted	Acquitted	Details of major Cases (4-6 lines each)
2007	62	18	34	13	01	Nil	**(1)** SDPI complaint to NR3C Cyber Crime Unit Rawalpindi about illegal access to their email servers. Technical team of NR3C forensically analyzed email server of SDPI and trace back unauthorized by Mr. Arsalan (ex-employee of SDPI) the court of law convicted Mr. Arsalan with Rupees fifteen thousand fine and twenty days imprisonment. **(2)** On the complaint of Bank Alfalah, NR3C Cyber Crime Unit Lahore registered a case FIR under ETO- 2002 and recovered amount of Rs.200,000.00 from accused Shahid Majeed & Razzaq Ahmed on account of defrauding Branch through ATM Card. **(3)** On the complaint of Bank Alfalah, NR3C Cyber Crime Unit Lahore registered a case FIR under ETO and recovered amount of Rs. 93,585.00 from accused Malik Mansoor Ahmed etc. on account of defrauding Branch through Credit Card. **(4)** On the complaint of UBL, NR3C Cyber Crime Unit Lahore registered a case FIR under ETO and recovered amount of Rs. 450,000.00 from accused Sheikh Hamza Tariq on account of defrauding Branch.
2008	287	50	60	34	02	01	**(1)** On the complaint of Hong Kong Bank, NR3C Rawalpindi registered a case FIR 01/08 against the accused and recovered amount of Rs.157000 from the culprit on account of recharging credit card. **(2)** On the complaint of National Bank of Pakistan NR3C Cyber Crime Unit Rawalpindi registered a case FIR 06/08 against the accused and recovered amount of Rs.10,00,000 from the culprits on account of illegally accessing ATM system of NBP. Case is under process.

[24] Year-wise data. (2009)

							(3) On the complaint of Wendel Jakson Jamican NR3C Cyber Crime Unit Rawalpindi registered case FIR No. 9/08 under Prevention of Electronic Crimes Ordinance-2007, against the accused Mr. Xavier William who created website www.north-starco.com for the purpose of online fraud. Accused was arrested and amount US $12500 were recovered from accused. **(4)** On the complaint of Mezan Bank, NR3C Cyber Crime Unit Lahore registered a case FIR 15/08 under PECO-2007, against the culprits involved in online banking fraud and recovered amount of Rs.28.2 million along with five vehicles and paper of plots purchased by the culprits through defrauded. **(5)** Discovered the last of Rs 760 million to national exchequer through illegal international gateway exchange in Faisalabad. **(6)** On the request of NAB, NR3C cyber crime unit Lahore recovered the amount of Rs. 35 million in the company's Foreign Accounts involved in illegal business activities. **(7)** On the complaint of PIA, NR3C cyber crime unit, Lahore arrested the culprit involved illegal access to online reservation system of PIA and booking of online tickets. **(8)** NR3C Cyber Crime Unit Lahore recovered the amount of Rs 7.4 million from shopkeeper involved in fraudulently withdrawing amount using ATM Debit card of Allied Bank of Pakistan. **(6)** On the complaint of Bank Alfalah, NR3C Cyber Crime Unit Lahore registered a case FIR under ETO- 2002 & PECO-2007 and recovered amount of Rs.113,141.00 from accused Ali Pervaiz & Khuram Pervaiz on account of defrauding Branch using Credit Card. **(9)** On the complaint of UBL, NR3C Cyber Crime Unit Lahore registered a case FIR under ETO-2002 & PECO-2007, and recovered amount of Rs. 33,758.00 from accused Hassan Shah on account of defrauding Branch through online fraud. **(10)** On the complaint of Bank Alfalah, NR3C Cyber Crime Unit Lahore registered a case FIR under ETO- 2002 & PECO -2007 and recovered amount of Rs. 92,200.00 from accused Azhar Abbas on account of defrauding Branch through Credit Card.

							(11) On the complaint of Wall Street Exchange Company, NR3C Cyber Crime Unit Lahore branch registered a case FIR under ETO & PECO and recovered amount of Rs. 146,112.00 from accused involved in defrauding company. **(12)** On the complaint of Bank Alfalah, NR3C Lahore branch registered a case FIR under ETO & PECO and recovered amount of Rs. 4,058,000.00 from accused Faisal Jamil on account of defrauding Branch. **(13)** On the complaint of Bank Alfalah, NR3C Lahore branch registered a case FIR under ETO & PECO and recovered amount of Rs. 1,679,000.00 from accused Ali Shehzad Saleem & Faisal Jamil on account of defrauding Branch. **(14)** On the complaint of Bank Alfalah, NR3C Lahore branch registered a case FIR under ETO & PECO and recovered amount of Rs. 83,183.00 from accused Sajid Javaid S/O Javaid Iqbal on account of defrauding Branch. **(15)** On the complaint of FDI Telecom Pvt Ltd. NR3C Lahore branch registered a case FIR under ETO & PECO and recovered amount of Rs. 161,634.00 from accused on account of defrauding Company. **(16)** NR3C assisted the crime wing in investigation of Khanani & Kalia and determined that total amount transferred by K & K through illegal Hundi & Hawala. The forensic analysis of computers of K & K transpired that total amount of Rs. 103849 millions was transmitted through hawala in Karachi from Year 2005 to 2008. **(17)** Hacker Muhammad Khan was convicted by court for maximum of thirty eight years (38) for illegal access to banking systems and making of fake credit cards.
2009	63	15	04	Nil	Nil	Nil	**(1)** On 7th April, 2009, NR3C Cyber Crime Unit Rawalpindi arrested the accused who sent threatening email of Bomb in GEO office. FIR has been registered under Prevention of Electronic Ordinances and accused is on Judicial custody. **(2)** On the complaint of Pakistan Telecommunication Authority NR3C cyber crime unit Karachi arrested a culprits involved in operating of illegal internet based Gateway exchange to terminate international calls. Per annum losses

							amount to approximately Rs. 30 million due to illegal voice calls termination. **(3)** On 21st Feb, 2009, NR3C cyber crime Lahore raided the M/S Zarco Exchange Lahore, forensic analysis of their systems determined that total amount Rs.47 billions was sent/ received illegally through inward/outward transactions during year 2008. Total amount of 131 millions (in different foreign currencies) was transferred illegally from Pakistan from Jun, 2008 to 1st Nov, 2008.
Total	412	83	98	47	03	01	Total amount of Rs. 61 million has been recovered by NR3C Cyber Crime Units during investigation of different cases related to cyber/ electronic crime.

APPENDIX-III

2008 INTERNET CRIME REPORT

INTERNET CRIME COMPLAINT CENTER [25]

General IC3 Filing Information

Internet crime complaints are primarily submitted to IC3 online at www.ic3.gov. Complainants without Internet access can submit information via telephone. After a complaint is filed with IC3, the information is reviewed, categorized, and referred to the appropriate law enforcement or regulatory agency.

From January 1, 2008 - December 31, 2008, there were 275,284 complaints filed online with IC3. This is a 33.1% increase compared to 2007 when 206,884 complaints were received (See Chart 1). The number of complaints filed per month, last year, averaged 22,940 (See Chart 2). Dollar loss of referred complaints was at an all time high in 2008, $264.59 million, compared to previous years (See Chart 3).

The number of referred complaints has decreased from 90,008 in 2007 to 72,940 in 2008 (See Chart 4). The 129,349 complaints that were not directly referred to law enforcement are accessible to law enforcement, used in trend analysis, and also help provide a basis for future outreach events and educational awareness programs.

Chart 1

From January 1, 2008 – December 31, 2008, there were 275,284 complaints filed online with IC3. This is a 33.1% increase compared to 2007 when 206,884 complaints were received. Tracking of this data began in 2000, when there were 16,838 complaints. Since then, complaints doubled each year to 2004, when they hit 207,449. From 2004 through 2007 they remained around the same threshold. In 2008, there was again a spike of approximately 75,000 complaints that took it to the 275,284 total.

Chart 2

From January 1, 2008 – December 31, 2008 the number of complaints filed per month, last year, averaged 22,940. This is a dramatic increase since the year 2000, when IC3 averaged just over 1,400 compliant a month.

Chart 3

Dollar loss of referred complaints was at an all time high in 2008, $264.59 million, exceeding last year's record breaking dollar loss of $239.09 million. On average, men lost more money than women.

Chart 4

The number of referred complaints has decreased from 90,008 in 2007 to 72,940 in 2008. The 129,349 complaints that were not directly referred to law enforcement in 2008 are accessible to law enforcement, used in trend analysis, and also help provide a basis for future outreach events and educational awareness programs.

[25] *Internet Crime Report 2008*. (2009)

The results contained in this report were based on information that was provided to IC3 through the complaint forms submitted online at ***www.ic3.gov*** by the public; however, the data represents a sub-sample comprised of those complaints that have been referred to law enforcement. While IC3's primary mission is to serve as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime, those complaints involving more traditional methods of contact (e.g., telephone and mail) were also referred. Using information provided by the complainant, the vast majority of all complaints were related to the Internet or online service. Criminal complaints were referred to law enforcement and/or regulatory agencies based on the residence of the perpetrator(s) and victims(s).

Complaint Characteristics

During 2008, non-delivery of merchandise and/or payment was by far the most reported offense, comprising 32.9% of referred crime complaints. This represents a 32.1% increase from the 2007 levels of non-delivery of merchandise and/or payment reported to IC3. In addition, during 2008, auction fraud represented 25.5% of complaints (down 28.6% from 2007), and credit and debit card fraud made up an additional 9.0% of complaints. Confidence fraud such as Ponzi schemes, computer fraud, and check fraud complaints represented 19.5% of all referred complaints. Other complaint categories such as Nigerian letter fraud, identity theft, financial institutions fraud, and threat complaints together represented less than 9.7% of all complaints (See Chart 5).

Statistics contained within the complaint category must be viewed as a snapshot which may produce a misleading picture due to the perception of consumers and how they characterize their particular victimization within a broad range of complaint categories. It is also important to realize IC3 has actively sought support from many key Internet E-Commerce stake holders. As part of these efforts, many of these companies, such as eBay, have provided their customers links to the IC3 website. As a direct result, an increase in referrals depicted as auction fraud has emerged.

Through its relationships with law enforcement and regulatory agencies, IC3 continues to refer complaints to the appropriate agencies. Complaints received by IC3 included confidence fraud, investment fraud, business fraud, and other unspecified frauds. Identity theft complaints are referred to the Federal Trade Commission (FTC) in addition to other agencies. Also, Nigerian (west African, 419, advance loan) letter fraud or 419 scams are referred to the United States Secret Service and child sexual exploitation complaints are referred to the National Center for Missing and Exploited Children. Compared to 2007, there were slightly higher reporting levels of all complaint types, except for auction

Chart 5

During 2008, non-delivered merchandise and/or payment was, by far, the most reported offense, comprising 32.9% of referred complaints. Internet auction fraud accounted for 25.5% of referred complaints. Credit/debit card fraud made up 9.0% of referred complaints. Confidence fraud, computer fraud, check fraud, and Nigerian letter fraud round out the top seven categories of complaints referred to law enforcement during the year.

Fraud, in 2008: For a more detailed explanation of complaint categories used by IC3, refer to Appendix Explanation of Complaint Categories at the end of this report.

A key area of interest regarding Internet fraud is the average monetary loss incurred by complainants contacting IC3 (See Chart 6). Such information is valuable because it provides a foundation for estimating average Internet fraud losses in the general population. To present information on average losses, two forms of averages are offered: the mean and the median. The mean represents a form of averaging that is familiar to the general public: the total dollar amount divided by the total number of complaints. Because the mean can be sensitive to a small number of extremely high or extremely low loss complaints, the median is also provided. The median represents the 50th percentile, or midpoint, of all loss amounts for all referred complaints. The median is less susceptible to extreme cases, whether high or low cost Of the 72,940 fraudulent referrals processed by IC3 during 2008, 63,382 involved a victim who reported a monetary loss. Other complainants who did not file a loss may have reported the incident prior to victimization (e.g., received a fraudulent business investment offer online or in the mail), or may have already recovered money from the incident prior to filing (e.g., zero liability in the case of credit/debit card fraud).

The total dollar loss from all referred cases of fraud in 2008 was $264.6 million. That loss was greater than 2007 which reported a total loss of $239.1 million. Of those complaints with a reported monetary loss, the mean dollar loss was $4,174.50 and the median was $931.00. Nearly fifteen percent (14.8%) of these complaints involved losses of less than $100.00, and (36.5%) reported a loss between $100.00 and $1,000.00. In other words, over half of these cases involved a monetary loss of less than $1,000.00. Nearly a third (33.7%) of the complainants reported

Chart 6

A key area of interest regarding Internet fraud is the average monetary loss incurred by complainants contacting IC3. Of the 72,940 fraudulent referrals processed by IC3 during 2008, 63,382 involved a victim who reported a monetary loss. The total dollar loss from all referred cases of fraud in 2008 was $264.6 million.

Amount Lost by Selected Fraud Type for Individuals Reporting Monetary Loss

Complaint Type	% of Reported Total Loss	Of those who reported a loss the Average (median) $ Loss per Complaint
Check Fraud	7.8%	$3,000.00
Confidence Fraud	14.4%	$2,000.00
Nigerian Letter Fraud	5.2%	$1,650.00
Computer Fraud	3.8%	$1,000.00
Non-delivery (merchandise and payment)	28.6%	$800.00

Auction Fraud	16.3%	$610.00
Credit/Debit Card Fraud	4.7%	$223.00

Table1
The total dollar loss from all referred cases of fraud in 2008 was $264.6 million. That loss was greater than 2007 which reported a total loss of $239.1 million. The highest dollar loss per incident was reported by check fraud (median loss of $3,000). The lowest dollar loss was associated with credit/debit card fraud (median loss of $223.50).

Losses between $1,000.00 and $5,000.00 and only 15.0% indicated a loss greater than $5,000.00. The highest dollar loss per incident was reported by check fraud (median loss of $3,000). Confidence fraud victims (median loss of $2,000.00), and Nigerian letter fraud (median loss of $1,650) were other high-dollar loss categories. The lowest dollar loss was associated with credit/debit card fraud (median loss of $223.50). Table 1 illustrates this.

Perpetrator Characteristics

Equally important to presenting the prevalence and monetary impact of Internet fraud is providing insight into the demographics of fraud perpetrators. In those cases with a reported location, over 75% of the perpetrators were male and over half resided in one of the following states: California, Florida, New York, Texas, District of Columbia, and Washington (see Map 1). These locations are among the most populous in the country. Controlling for population, the District of Columbia, Nevada, Washington, Montana, Florida, and Delaware have the highest per capita rate of perpetrators in the United States (see Table 2). Perpetrators also have been identified as residing in the United Kingdom, Nigeria, Canada, Romania, and Italy (see Map 2). Inter-state and international boundaries are irrelevant to Internet criminals. Jurisdictional issues can enhance their criminal efforts by impeding investigations with multiple victims, multiple states/counties, and varying dollar losses. These statistics highlight the anonymous nature of the Internet. The gender of the perpetrator was reported only 37.3% of the time, and the state of residence for domestic perpetrators was reported only 33.3% of the time.

The vast majority of perpetrators were in contact with the complainant through either e-mail or via websites. (Refer to Appendix III at the end of this report for more information about perpetrator statistics by state). Of these reports 77.4% of perpetrators were male and 22.6% were female.

Top Ten States by Count: Individual Perpetrators

Top Ten States (Perpetrators)

1.	California	15.8%
2.	New York	9.5%
3.	Florida	9.4%
4.	Texas	6.4%
5.	D.C.	5.2%
6.	Washington	3.9%
7.	Illinois	3.3%
8.	Georgia	3.1%

9.	New Jersey	2.8%
10.	Arizona	2.6%

Perpetrators per 100,000 people

Rank	State	Per 100,000 People
1	District of Columbia	81.32
2	Nevada	80.84
3	Washington	55.38
4	Montana	54.47
5	Florida	47.96
6	Delaware	45.75
7	New York	45.47
8	Hawaii	44.55
9	Utah	41.11
10	California	40.09

These locations are among the most populous in the country. Controlling for population, the District of Columbia, Nevada, Washington, Montana, Florida, and Delaware have the highest per capita rate of perpetrators in the United States.

***Map 2** - Top Ten Countries by Count (Perpetrators)*

1.	United States	66.1%
2.	United Kingdom	10.5%
3.	Nigeria	7.5%
4.	Canada	3.1%
5.	China	1.6%
6.	South Africa	0.7%
7.	Ghana	0.6%
8.	Spain	0.6%
9.	Italy	0.5%
10.	Romania	0.5%

Perpetrators also have been identified as residing in the United Kingdom, Nigeria, Canada, Romania, and Italy. Inter-state and international boundaries are irrelevant to Internet criminals. Jurisdictional issues can enhance their criminal efforts by impeding investigations with multiple victims, multiple states/counties, and varying dollar losses.

Complainant Characteristics

The following graphs offer a detailed description of the individuals who filed an Internet fraud complaint through IC3 (see Map 3). The average complainant was male, between 40 and 49 years of age, and a resident of one of the four most populated states: California, Florida, Texas, and New York. Alaska, Colorado, and DC, while having a relatively small number of complaints (ranked 31st, 11th, and 45th respectively), had among the highest per capita rate of complainants in the United States (see Table 3). While most complainants were from the United States, IC3 has also received a number of filings from Canada, the United Kingdom, and Australia (see Map 4).

Table 4 compares differences between the dollar loss per incident and the various complainant demographics. Males reported greater dollar losses than females (ratio of $1.69 dollars to every $1.00 dollar). Individuals 40-

49 years of age reported higher or equal amounts of loss than other age groups.

Top Ten States By Count: Individual Complainants

Map 3 - Top Ten States (Complainant)

1.	California	14.6%
2.	Texas	7.2%
3.	Florida	7.1%
4.	New York	5.4%
5.	Pennsylvania	3.6%
6.	New Jersey	3.5%
7.	Illinois	3.4%
8.	Ohio	3.0%
9.	Virginia	2.9%
10.	Washington	2.9%

The graph offers a detailed description of the individuals who filed an Internet fraud complaint through IC3.

Complainants per 100,000 people

Rank	State	Per 100,000 People
1	Alaska	337.61
2	Colorado	135.46
3	District of Columbia	119.63
4	Nevada	113.07
5	Maryland	111.60
6	Washington	105.95
7	Arizona	101.46
8	Oregon	101.03
9	Florida	95.25
10	California	95.09

The average complainant was male, between 40 and 49 years of age, and a resident of one of the four most populated states: California, Florida, Texas, and New York. Alaska, Colorado, and DC, while having a relatively small number of complaints (ranked 31st, 11th, and 45th respectively), had among the highest per capita rate of complainants in the United States

Top Ten Countries (Complainant)

Map 4 - Top Ten Countries (Complainant)

1.	United States	92.93%
2.	Canada	1.77%
3.	United Kingdom	0.95%
4.	Australia	0.57%
5.	India	0.36%
6.	France	0.15%
7.	South Africa	0.15%
8.	Mexico	0.14%
9.	Denmark	0.13%

10.	Philippines	0.13%

Amount Lost per Referred Complaint by Selected Complainant Demographics

Map 4 - Top Ten Countries (Complainant)

1.	United States	92.93%
2.	Canada	1.77%
3.	United Kingdom	0.95%
4.	Australia	0.57%
5.	India	0.36%
6.	France	0.15%
7.	South Africa	0.15%
8.	Mexico	0.14%
9.	Denmark	0.13%
10.	Philippines	0.13%

While most complainants were from the United States, IC3 has also received a number of filings from Canada, the United Kingdom, and Australia

Amount Lost per Referred Complaint by Selected Complainant Demographics	Average (Median) Loss Per Typical Complaint
Male	$993.76
Female	$860.98
Under 20	$500.00
20-29	$873.58
30-39	$900.00
40-49	$1,010.23
50-59	$1,000.00
60 and older	$1,000.00

Table 4

The difference between the dollar loss per incident and the various complainant demographics is shown above. Males reported greater dollar losses than females (ratio of $1.69 dollars to every $1.00 dollar). Individuals 40- 49 years of age reported higher or equal amounts of loss than other age groups.

Complainant-Perpetrator Dynamics

One of the components of fraud committed via the Internet that makes investigation and prosecution difficult is that the offender and victim may be located anywhere in the world. This is a unique characteristic not found with other types of "traditional" crime. This jurisdictional issue often requires the cooperation of multiple agencies to resolve a given case. Table 5 highlights this truly "borderless" phenomenon. Even in California, where most of the reported fraud cases originated, only 30.6% of all cases involved both a complainant and perpetrator residing in the same state. Other states have an even smaller percentage of complainant-perpetrator similarities in residence. These patterns not only indicate "hot spots" of perpetrators (California for example) that target potential victims from around the world, but also indicate that complainants and perpetrators may not have had a relationship prior to the incident.

Another factor that impedes the investigation and prosecution of Internet crime is the anonymity afforded by the Internet. Although complainants in these cases may report multiple contact methods, few reported interacting face-to-face with the vast majority of perpetrators contact through e-mail (74.0%) or a webpage (28.9%). Others reportedly had phone contact (15.0%) with the perpetrator or corresponded through physical mail (8.3%). Interaction through chat rooms (2.2%) and in-person (1.7%) meetings were rarely reported. The anonymous nature of an e-mail address or a website allows perpetrators to solicit a large number of victims with a keystroke (see Chart 7).

Perpetrators from Same State as Complainant

State	Percent	1	2	3
1. California	30.6	(New York 8.0%)	(Florida 8.0%)	(Texas 5.1%)
2. Florida	24.4	(California 12.6%)	(New York 8.6%)	(D.C. 5.1%)
3. Arizona	22.7	(California 12.6%)	(New York 7.5%)	(Florida 7.3%)
4. New York	21.7	(California 14.0%)	(Florida 9.2%)	(Texas 5.1%)
5. Nevada	20.0	(California 15.8%)	(New York 7.2%)	(Florida 6.2%)
6. Texas	19.5	(California 12.8%)	(New York 8.5%)	(Florida 7.2%)
7. Georgia	18.6	(California 11.5%)	(New York 9.2%)	(Florida 8.7%)
8. Washington	18.1	(California 14.5%)	(Florida 7.7%)	(New York 7.3%)
9. Illinois	15.6	(California 13.0%)	(New York 8.4%)	(Florida 8.0%)
10. D.C	15.6	(California 8.9%)	(Texas 5.5%)	(New York 5.5%)

Table 5 *- Other top three locations in parentheses*

The table above highlights this truly "borderless" phenomenon. Even in California, where most of the reported fraud cases originated, only 30.6% of all cases involved both a complainant and perpetrator residing in the same state. Other states have an even smaller percentage of complainant-perpetrator similarities in residence.

Chart 7

Although complainants in these cases may report multiple contact methods, few reported interacting face-to-face with the vast majority of perpetrators contact through e-mail (74.0%) or a webpage (28.9%). Others reportedly had phone contact (15.0%) with the perpetrator or corresponded through physical mail (8.3%). Interaction through chat rooms (2.2%) and in-person (1.7%) meetings were rarely reported.

A: No. Valuable data could be lost during an orderly shutdown.

Q: How do you perform a disorderly shutdown of a computer?
A: Disconnect the plug on the back of the computer. Do not use the off switch.

Q: How large must the destination drive be when using SafeBack?
A: At least as large as the source disk.

Q: Should you load and run evidence collection and analysis tools from the hard drive that contains the evidence you are collecting?
A: No. Always load and run your tools from another medium, such as a diskette, Jaz Drive, Zip disk, or CD-ROM.

Q: Name other network devices you can collect evidence from besides standard computer systems.
A: Firewalls, routers, switches, e-mail server

Q: What software tool can you use in court to prove that your copy of the file is valid?
A: CRCMD5 from NTI.

Q: What tool would be used to collect a bit-stream backup of a hard drive?
A: SafeBack from NTI.

Q: When using SafeBack, one of the options is local and the other is lpt1. Explain each of these options.
A: Local = Zip Drive or other collection device you have connected directly to the back of the computer that contains the evidence. lpt1 = moving data from the victim computer to another computer.

Q: What does the program ResPart.exe from NTI do?
A: Restores partition table data when it is destroyed.

Q: To start SafeBack, what filename do you type from the diskette?
A: Master.

Q: When using the backup selection on SafeBack, are you making a bit-stream backup?
A: Yes.

Q: What does the restore function do in SafeBack?
A: Restores the bit-stream image to the destination drive.

Q: You have used SafeBack to make your bit-stream backup. What should be the next option you use in SafeBack?
A: Use the "verify" option to ensure that the backup you just made can be properly accessed and read.

Q: If I tell SafeBack to attempt Direct Access, what is the purpose of this and what will it do?
A: Bypass BIOS and go directly to the drive controller.

Q: In SafeBack, what do numbered drives represent?
A: Physical drives.

Q: In SafeBack, what do lettered drives represent?
A: Logical volumes.

Q: What does the phrase "secure the crime scene" mean?
A: Keep people away from the area containing the compromised systems. Do not let the victim machines be touched.

Q: What is the Federal Bureau of Investigation's (FBI's) definition of a computer crime?
A: The computer must be the victim.

Q: What is a Cyber Trail?
A: Digital logs, stored files, Web pages, e-mail, digitized images, digitized audio and video.

Q: When you arrive at a scene, how do you secure the logs and any information you capture to logs from the time you arrived?
A: Spool logs off to a log host machine. No trust relationship.

Q: A ribbon cable has two connectors. What do they connect to?
A: Primary hard drive and primary slave.

Q: What does it tell you if Auto-Answer is lit up on the modem?
A: The modem is configured to receive incoming calls.

Q: What do flashing lights on a modem indicate?
A: The modem is in use.

Legal

Q: Define exculpatory evidence.
A: Evidence that contradicts your findings or hypothesis.

Q: What is case law?
A: How judges and juries have interpreted the law as it is written in the statues.

Q: What is the purpose of the exclusionary rule?
A: To eliminate evidence that was improperly or illegally collected.

Q: In a court of law, what are protective orders?

A: A warrant.

Q: What are the current laws used to prosecute computer crimes in the United States at the federal level?
A: Under Title 18 U.S.C.:

Paragraph 1029: Unauthorized use of access devices
Paragraph 1030: Unauthorized access to computer
Paragraph 1831: Theft of trade secrets by a foreign agent
Paragraph 1832: Theft of trade secrets
Paragraph 2319: Copyright infringement
Paragraph 2320: Trademark infringement
Paragraph 2511: Unauthorized interception of wire communication

Note:

Paragraphs 1029 and 1030 are used most for:
Computer hacking
Telephone phreaking
Computer intrusions
Theft of passwords
Intentional destruction of data

Q: What is the ECPA and to whom does it apply?
A: Electronic Communications Privacy Act. Everyone.

Evidence Analysis

Q: Do I use the NTI FileList program before or after using SB?
A: After.

Q: Must FileList be on a DOS-bootable diskette?
A: Yes.

Q: What program must I use to read the output from FileList?
A: FileCnvt.exe from NTI.

Q: Name three hidden areas on a hard drive that could contain data.
A: Slack Space, unallocated space, Web browser cache.

Q: Name two file types to look at immediately.
A: Configuration and Startup files.

Q: What are the two main DOS startup files?
A: CONFIG.SYS, AUTOEXEC.BAT.

Q: What version of Norton Utilities must be used in CF investigations?
A: <= 4.0 DOS.

Q: What three items do we try to apply to a suspect?
A: Motive = why; means = how; opportunity = when.

Q: A file is never deleted until __________.
A: It is overwritten.

Q: What is it called when a large file is spread over several sectors?
A: Fragmentation.

Q: What are the four main areas of a hard drive?
A: Track, sector, cylinder, and cluster.

Q: What is slack space?
A: Space that a file does not use up inside a cluster.

Q: What is unallocated space?
A: The space taken up by a file when you erase it.

Q: What are the two types of windows swap files?
A: Temporary and permanent.

Q: What tool do you use to look at the Web browser cache?
A: unmozify.

Q: Use ________ to search for keywords in hidden areas of the disk.
A: TextSearch.

Q: What is chaining?
A: Following fragmented files from sector to sector to reconstruct the file.

Q: Can SUN UNIX disks be read in an Intel-based computer?
A: Yes.

Q: Fifteen items can be used in software forensics to determine who wrote the code. Name three of them.
A: Data structures, algorithms, compiler used, expertise level, system calls made, errors made, language selected, formatting methods, comment styles, variable names, spelling and grammar, language features used, execution paths, bugs, comments.

Q: Try to narrow the field of _____________ before using SFA.
A: Potential suspects.

Q: Name a major system log limitation.
A: Easy to modify anonymously without being noticed; easy to tamper with.

Q: Can you depend upon the evidence from one log? Why or why not?
A: No. Other corroborating evidence is needed.

Q: I have run SafeBack, FileList, and FileCnvt. Now I must run Filter_I. What will it do?

A: It is an intelligent filter that removes binary data and any ASCII data that is not a word.

Q: Must Filter_I and FileList be run in the same directory that contains the bitstream backup?
A: Yes.

Q: If the disk is highly fragmented, should GetSlack and GetFree be used or is it better to use some other program?
A: Use GetSlack and GetFree.

Q: Are TextSearch Plus search strings case sensitive?
A: No.

Q: Which tool in Norton Utilities is primarily used to rebuild fragmented files?
A: Disk Editor.

Q: What are two choices of tools for creating a working copy of a diskette?
A: DOS DiskCopy (best) and AnaDisk.

Q: What are three methods for hiding data on a diskette?
A: Disks within disks; write data between tracks; hide data in graphics.

Q: You decide that you want to look at the Web browser cache. What tool would you use?
A: unmozify.

UNIX

Q: What command do you use in UNIX to write RAM to disk, shut down the machine, and restart it?
A: shutdown –r

Q: What UNIX command can be used to reboot the machine and cause it to come up in single user mode?
A: halt -q

Q: You have the UNIX box in single user mode. You have the settings so that it will boot from the CD (compact disk). What command should you now type to cause the UNIX box to boot from the CD?
A: boot

Q: Which log saves commands that were typed on the system (in UNIX)?
A: HISTORY

Q: What files in UNIX keep track of login and logout times?
A: WTMP, BTMP

Q: What ten items should be logged as a minimum?

A: Logins, logouts, privilege changes, account creation, file deletion, su access, failed logins, unused accounts, reboots, and remote access.

Q: Name two versions of UNIX that normally run on an Intel platform.
A: BSD and LINUX.

Q: If you put a UNIX disk in an Intel platform and it will not boot, what should your next step be to make the boot happen?

A: Use a "bare bones" version of the same UNIX version on another disk and boot from this disk. Be sure to set this boot disk as the PMHD (Primary Master Hard Drive).

Q: DOS uses autoexec.bat and config.sys. What are the similar type startup files in UNIX?
A: rc files

Q: To what UNIX files do hackers like to add booby traps?
A: rc files

Q: You have rebooted the UNIX box to single user mode. What are the first files you should look at?
A: rc files

Q: What is the name of the rootkit for Linux?
A: Knark

Q: What UNIX file will save the memory contents if the system crashes?
A: Core file

Q: Name two things that lastlog will show you.
A: Who was on the system and key words such as "crash."

Q: What are the four major UNIX commands to use when analyzing crash dump files?
A: Ps, netstat, nfsstat, and arp.

Q: What type of machine should you use if you are doing crash dump analysis?

A: Same o/s version.
Q: For RedHat Linux, what is the command to verify the integrity of all important system files?

A: rpm -VA
Q: The results of your last command indicate that a user named
Bragger23 logged in earlier in the day and is currently logged into
Solaris5. You want to see all the processes in memory that
Bragger23 is running. What do you type?

A: ps -aux | grep Bragger23

Q: What steps do you follow to remove Bragger23 and collect RAM evidence?

A: To remove Bragger23 from the system, remove all of this user's processes:

```
kill -9 1365
kill -9 3287
kill -9 1087
kill -9 3001
```

To collect RAM evidence:

```
ps -aux > a:\Solaris5RAMproc.txt
```

Hackers

Q: How do crackers usually get caught?

A: Vanity, bragging, behavior patterns, sharing information, and tool signatures.

Q: Explain the TCP (Transmission Control Protocol) three-way handshake.

A: Syn. Syn/Ack. Ack.

Q: What is a SynFlood and what does Fin do?

A: SynFlood will mute a system by flooding it with syn packets. Fin will tear down a connection.

Q: What is an exploit?

A: A program written to break into computer systems.

Q: To hijack a computer system, does a hacker want to complete the three-way handshake?

A: No.

Q: What are crafted packets?

A: Packets maliciously constructed to damage a computer system.

Q: What software program can be used to detect reconnaissance probes to a network?

A: TCPdump.

Q: What procedure should you follow to remove hacker software (four steps)?

A:
1. Kill process.
2. Delete in registry.
3. Delete file.
4. Reboot.

Q: Failing computers can act as though they are being __________.

A: Attacked.

Q: If you suspect a DoS (Denial of Service) attack, what three things should you look for?
A: File deletions, file corruption, and hacker tools.

Q: What are the five steps you should follow on a client's system to recover from a malicious rootkit installation and usage?
A:
1. Client should back up their data (potentially corrupted).
2. You should format the hard drive(s).
3. You should reinstall the operating system from a trusted source.
4. Every password for the system should be changed (as should those for any other system the user may be on).
5. You should run a password cracker on the changed passwords to ensure they are strong passwords.

Q: In one sentence, what is being done here (in general)?

```
mkdir.HiddenHackFiles
mv rootkit.tar.gz.HiddenHackFiles
cd.HiddenHackFiles
tar -zvf rootkit.tar.gz
ls
cd rootkit
./install
exit
```

A: A rootkit is being installed.

Q: When there is very little information to work with, what can you do on an Internet Relay Chat (IRC) line to draw the perpetrator out?
A: Brag about how you are the one who pilfered the system(s).

Q: When determining keywords, keep in mind that hackers' words can look different than normal words yet have the same meaning.
For example, how could a hacker write the letter I? An E?
A: Pipe symbol. 3.