«Combating Criminal Activities Threatening Electronic Commerce»

Dr. Rizgar Mohammed Kadir
Associate Professor
College of Law & Politics
Salahaddin University - Iraq

I. INTRODUCTION

One of the major phenomenons of the today's information era is what is commonly known as the electronic commerce which is described by some specialists as a *revolution* in the realm of the business.(1) People are now becoming more and more depending on the electronic commerce. The rapid growth of the internet has resulted in a rapid growth of the electronic commerce.(2) There are many evidences indicating that electronic commerce will continue in occupying and dominating new fields in the realm of the commerce. An author, in this context, has written "[e]-commerce has completely altered the manner in which many companies reach customers, the cost to do so, the information available to both buyers and sellers, the way in which customers buy and from where they buy. For these reasons, it is the most significant development in business in decades, and, even in its current deflated state, has a significant role in the world of commerce today and in the future".(3)

(1) CRAIG STANDING, INTERNET COMMERCE DEVELOPMENT, ARTECH HOUSE, 4 (2000) ("[t]he growth in electronic commerce is proving to be a business revolution. It is a revolution because electronic commerce, particularly over the Internet, is so profoundly different from traditional business in so many ways").

(2) Michael Edmund O'Neill, Old Crimes in New Bottles: Sanctioning Cybercrime, 9 Geo. Mason L. Rev, 237 (2000), at 252.

(3) S. K. BLACK, TELECOMMUNICATIONS LAW IN THE INTERNET AGE, MORGAN KAUFMANN, USA, 390 (2002).

The electronic commerce has raised many complex legal issues which are linked to different branches of the law such as commercial law, civil law, private international law and criminal law. The said issues are usually related to new concepts emerged, as a result of the rapid developments in the field of communication and the electronic commerce itself such as electronic contracts, digital signature, Internet sites and domains, electronic documents and certifications, online payments, stock market transactions, taxation and customs and others.

For example the issue of the jurisdiction over the electronic commerce is one of the main complex legal issues that legal scholars, courts and legislators have faced and forced to find solutions for in the field of the electronic commerce.(4) The same is true in terms of other legal issues we have just mentioned above.

However, the most crucial question which is still widely debated is the question of the legislative protection and avenues of recourse that are necessary to protect this electronic commerce, because of the increasing number of criminal activities threatening this important kind of commerce.(5)

The reason behind this reality is simply that statistics concerning high-technology or computer-related crime show that the range of criminal activities appear to be expanding as technologies create new criminal opportunities and offenders find new ways to exploit them. It is clear that the rapid expansion of electronic commerce is accompanied by subsequent increases in economic computer-related crimes such as fraud, the manipulation of financial markets and money-laundering.(6)

Historical facts show that the commerce, represented in the exchange of goods and services, has existed among individuals and nations since antiquities. The main characteristic of the commerce throughout the history, and still, is the speed which is absolutely depends upon trust and

(4) *See* Ellen S. Podgor, International Computer Fraud: A Paradigm for Limiting National Jurisdiction, 35 U.C. Davis L. Rev. 267 (2002), at 279-80.

(5) Julie A. Tower, Hacking Vermont's Computer Crimes Statute, 25 Vt. L. Rev. 945 (2001), at 949.

(6) *See* Marc D. Goodman & Susan W. Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, 10 Int'l J.L. & Info. Tech., 39 (2002), at 147.

confidence between those involved in the commercial activities; in most cases the exchange is made before any assurances that the goods or services will satisfy the client.

Since the recent developments in the field of telecommunications have brought us face-to-face with electronic commerce including digital transactions over thousands of miles to different cultures and peoples through unfriendly territories, it means that conducting successful electronic commerce is in need of specific mechanisms that might safeguard this commerce and preserve the traditional trust and confidence.(7)

This Article is devoted to find, discuss and analyze strategies that might be adopted for combating criminal activities threatening electronic commerce. For achieving this purpose, this Article is going to explore both national and international experiences. In the next Section of the Article we will study the general aspects relating to the electronic commerce including its definitions, features and advantages. In Section III we are going to shed lights on the different criminal activities targeting electronic commerce. Section IV will be devoted for discussing the strategies that might be adopted for combating criminal activities threatening this new kind of commerce.

II. ELECTRONIC COMMERCE – AN OVERVIEW

In this Section we are going to shed lights on three important general questions relating to the electronic commerce; the definition of the electronic commerce and its main categories, features and characteristics of the electronic commerce, and finally the advantages of the electronic commerce. Each question will be separately dealt with within three separate subsections.

(7) JOSEPH MIGGA KIZZA, ETHICAL AND SOCIAL ISSUES IN THE INFORMATION AGE, SPRINGER-VERLAG LONDON LIMITED 11 308-9 (2007).

A. Defining the Electronic Commerce

The electronic commerce which is also commonly called as 'e-commerce', 'cyber-commerce', 'Internet commerce' and 'dot-com companies' is a term that refers to all modern terms providing ease of use for shoppers and, initially, instant wealth for owners.(8) It simply is "buying and selling goods and services over the Internet"(9), or "the online exchange of goods, services, and money within firms and between firms and their customers".(10)

The term, generally, refers to contracts and payments made using computers and other electronic equipment.(11) It encompasses contracts concluded through the exchange of email, purchases that are made at the Internet websites, money transfers made by electronic means, and other similar activities. The term further includes both business-to-business and business-to-consumer transactions.(12) It also includes other business action such as an inquiry about a product feature, a purchase order, or an invoice delivery about a product feature.(13)

These definitions emphasize that electronic commerce could encompass trading carried out by any means of communication that can be labeled 'electronic'. They, however, emphasize computer to computer transactions and the concern here is basically email and web-based communication, which are sufficiently different from the more traditional means of communication.(14)

---

(8) S. K. BLACK, *supra* note 3, at 390.

(9) HOSSEIN BIDGOLI, ELECTRONIC COMMERCE, PRINCIPLES AND PRACTICE, ACADEMIC PRESS, 45 (2002).

(10) CRAIG STANDING, *supra* note 1, at 4.

(11) Gregory E. Maggs, Regulating Electronic Commerce, 50 Am. J. Comp. L. 665 (2001), at 665.

(12) *Id*.

(13) SYED MAHBUBUR RAHMAN, ELECTRONIC COMMERCE: OPPORTUNITY AND CHALLENGES, IGI PUBLISHING 3 (2000).

(14) DIANE ROWLAND & ELIZABETH MACDONALD, INFORMATION TECHNOLOGY LAW, CAVENDISH PUBLISHING LIMITED, LONDON, 6 251 (2000).

Combating Criminal Activities Threatening Electronic Commerce

It is necessary to mention that electronic commerce was not created by the Internet; it had existed even before the emergence of the Internet.(15) The telephone, the fax machine, the television, electronic payment and money transfer systems, and Electronic Data Interchange (EDI) all make it possible to do business in one or more respects electronically.(16) This reality imposes questioning the reason standing behind attaching electronic commerce to the use of the Internet, particularly, in the business.

Some scholars argue that technologies such as fax and telex are used in the business world, they, however, are not considered electronic commerce because they include the use of paper as an output, which hinders the interaction of electronic media and thus prevents data exchange on an electronic basis.(17) This argument is giving an important explanation to the subject matter; however, we think it does not provide a crucial answer to aforementioned question simply due to the reality that even the use of the Internet includes the use of paper as an output in many occasions.

The reason, in fact, is that the notion of electronic commerce did not become understandable to the public only after the emergence of the Internet. As entire transactions can take place via the Internet, individuals could all of a sudden conduct business without knowing either their client. Moreover, the Internet is a more convenient tool than the other electronic tools as it offers a more efficient and cheaper way to conduct business, extending benefits to both potential merchants and consumers. The existence of the Internet offers more choices for consumers and it is the main instrument for the evolving electronic commerce.(18)

(15) The idea of the Internet is traced back to the mid-1960s. It began as a research project by the US Defense Department which established a called Advanced Research Project Agency Network (ARPANET). It was an experimental network designed specifically to withstand various forms of attack on the communications lines. *See* CRAIG STANDING, *supra* note 1, at 2.

(16) M. BACHETTA, ET AL, ELECTRONIC COMMERCE AND THE ROLE OF THE WTO, 5 (1998).

(17) SYED MAHBUBUR RAHMAN, *supra* note 13, at 3.

(18) YUN ZHAO, DISPUTE RESOLUTION IN ELECTRONIC COMMERCE, MARTINUS NIJHOFF PUBLISHERS, 14 (2005).

Electronic commerce are classified into several categories based on the nature of the transactions, including business-to-consumer (B2C), business-to-business (B2B), consumer-to-consumer (C2C), consumer-to-business (C2B). In business-to-consumer electronic commerce, businesses sell directly to consumers. Amazon.com, is well known example of this category. Business-to-business refers to electronic transactions among and between businesses. The consumer-to-consumer category involves business transactions among individuals using the Internet and web technologies. Using C2C, consumers sell directly to other consumers. For example, through classified ads or by advertising, individuals sell services or products on the Web or through auction sites. Finally, Consumer-to-business electronic commerce involves individuals selling to businesses including any service or product that a consumer is willing to sell.(19)

B. Features and Characteristics of Electronic Commerce

The distinctive characteristic of the electronic commerce is the subject matter of electronic contracts concluded via computers linked together by the internet or other electronic equipments.

Contracts that are concluded in such modern ways may simply be concerned with traditional goods or services which finally to be delivered in the traditional way. However, electronic commerce does not simply provide a new means of making contracts. In some situations, it also provides a new method of performance such as software, video, books, music and even newspapers and magazines.(20)

Since the electronic commerce depends essentially upon the Internet, its second characteristic is, then, its global nature. Electronic commerce is not

(19) SYED MAHBUBUR RAHMAN, *supra* note 13, at 50-2.

(20) DIANE ROWLAND & ELIZABETH MACDONALD, *supra* note 14, at 252 (citing Chissick, M. and Kelman, A., *Electronic Commerce: Law and Practice*, 2nd ed., 2000, London: Sweet & Maxwell, para 3.07, "[c]ertain products, such as software, video, books, music and even newspapers and magazines no longer have to be physically delivered in hard copy format to the purchaser. Suppliers can instead send the products in digital form over the internet, providing both time and cost saving").

restricted by geographical or political boundaries in the same way as more traditional business forms. Obviously, contracts are always concluded between parties in different jurisdictions.(21) In the age of the Internet the whole world has become smaller. Using the Internet people around the world can easily and instantaneously interact with each other. National borders between countries in the world has lost considerable parts of their meaning they had in past.

Internet-based electronic commerce has the potential to change the nature of trade. Employees can work from home, cooperate in virtual teams, and be part of decentralized organizations.(22)

With the help of the Internet the electronic commerce is not limited to certain parts of the globe; it can be exercised between people regardless of the distance which separates them physically.

C. Advantages of Electronic Commerce

Electronic commerce presents many advantages, below we will shed lights on the majors of them:

1- More effective marketing:

The adoption of the electronic commerce by trade companies and their marketing on the Internet, allow them to display their products and services in various parts of the world giving them a greater access to more customers around the world.

Business over the Internet can be conducted around the clock without interruption twenty-four hours a day, seven days a week, and 365 days a year. Customers in any part of the world are able, with an Internet connection, to log onto the electronic commerce site and order a product or service. Holidays, weekends, after hours, and differences in time zones do not pose any problem.(23)

2- More profits:

(21) *Id*.

(22) CRAIG STANDING, *supra* note 1, at 4.

(23) HOSSEIN BIDGOLI, *supra* note 9, at 54.

Electronic commerce gives the commercial companies greater opportunity to reap the profits. This is evidenced by many facts; one of them is what we have just mentioned above i.e. the greater circle of customers.

Another reason is the reduction of corporate expenses: the process of preparation and maintenance of the electronic commerce sites on the web more economical to build the retail market. Companies are no in need to spend heavily on promotional matters, or the installation of expensive equipment used in customer service. They are even not in need to employ a large number of staff to conduct the inventory and business management as there are databases maintained on the Internet sales in the company, which is possible for a single person to explore the information in the database to check the dates of sales easily.

3- Facile commercial activities:

The electronic commerce made it easy, in many ways, to customer to involve in commercial activities.

For example, suppose that a consumer needs to purchase a book over the internet, he or she visits the seller's website, browses through the titles for sale, selects a book by clicking on some part of the computer screen, and then inputs a credit card number. If all goes as planned, the seller will ship the book, and charge the consumer's credit card. The issuer of the credit card, most likely through an intermediary bank, will pay the seller, and then bill the consumer. At the end of the month, the consumer will pay the credit card[24]. The customer does not need to leave his or her home or office and commute to purchase an item. The customer does not need to look for parking in a shopping mall during holidays, nor leaving his or her small children or elderly relatives for even a short period. Shopping tasks can be done from the privacy of the home with a few clicks of mouse.[25]

(24) Gregory E. Maggs, *supra* note 11, at 665-6.

(25) HOSSEIN BIDGOLI, *supra* note 9, at 57.

III. CRIMINAL ACTIVITIES THREATNING ELECTRONIC COMMERCE

It is apparent that the computer and the Internet have changed the life style of the individuals, commercial entities and the governmental institutions. They are both playing a very decisive role in facilitating the daily activities due to the cheaply, speedily and easily performing of many different tasks that were, in past, in need of a great deal of efforts, time, and resources as they were performing manually.

However, the same features making computer and internet the most popular instrument in the world such as their wide storage capacity, speed and accessibility of well arranged information, have collectively contributed in making computers targets for crime,(26) creating new environment for criminals and providing new and easy opportunities to them.(27)

The electronic commerce is one of results of the spread of the computer and Internet; hence the efficiency and speed of the network create new opportunities for criminals while simultaneously positing serious criminal threats to the electronic commerce.(28) The criminal activities that represent a real challenge and threat to the electronic commerce are varied and might take so many forms. They, however, can be classified into two main categories; the criminal activities targeting Internet and computer, and the criminal activities targeting the electronic commerce particularly. We are going to discuss in the following subsections.

A. The Criminal Activities Targeting Electronic Commerce Devices

This category includes all criminal activities targeting the Internet and the computer as the two indispensable devices of the electronic commerce. Although these criminal activities are not targeting the electronic

(26) Carla Ottaviano, Computer Crime, 26 IDEA 163 (1985-1986), at 163.

(27) The realities on the ground indicate that computer misuses have occurred short after its spreading inside industrialized countries. *See* generally Swanson & Territo, Computer Crime: Dimensions, Types, and Investigation, 8 J. of Police Sci. and Ad. 304 (1980).

(28) Marc D. Goodman & Susan W. Brenner, *supra* note 6, 147.

commerce directly, the experience indicates their great negative impact on it. The main criminal activities falling into this category include:

1. Hacking

The term 'computer hacking' is traditionally used to describe the penetration of computer systems(29), this is because of that computer hacking in its simplest form means illegal entry into a computer system(30), it is, accordingly, defined as the act of gaining unauthorized access to a computer system(31), it occurs whenever an actor achieves entry into a target's files or programs without having permission to do so(32), and usually, involves using technology for the purpose of gaining unauthorized access to a computer system, program, or data.(33)

Some commentators are considering hacking as being analogous to physical trespass arguing that the offender, in both cases, gains access to an area -a physical location in trespass and a virtual location in hacking- to which he or she does not have legal authority to access.(34)

The techniques of traditional forms of hacking in computer networks were developed during the 1980s(35). It is still the most dangerous threat to

(29) Ulrick Sieber, Legal Aspects of Computer-Related Crime in the Information Society, COMCRIME Study prepared for the European Commission 19 (Jan. 1998), at 42. available at:

http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc (Jan. 27, 2009).

(30) John T. Soma et al, Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed? 34 Harv. J. on Legis. 317 (1997), at 346.

(31) *See* Michael Edmund O'Neill, *supra* note 2, at 246; Susan W. Brenner, Toward a Criminal Law for Cyberspace: Distributed Security, 10 B.U. J. Sci. & Tech. L. 1 (2004) at 73.

(32) Neal Kumar Katyal, Criminal Law in Cyberspace, 149 U. Pa. L. Rev. 1003 (2001), at 1021.

(33) Brian C. Lewis, Prevention of Computer Crime Amidst International Anarchy, 41 Am. Crim. L. Rev. 1353 (2004) at 1355.

(34) Susan W. Brenner, Is There Such a Thing as "Virtual Crime?" 4 Cal. Crim. L. Rev. 1 (2001), at ¶ 80. *See* also Michael Edmund O'Neill, *supra* note 2, at 246; Catherine T. Clarke, From CrimINet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet, 75 Or. L. Rev. 191 (1996) at 204.

(35) Ulrick Sieber, *supra* note 29, at 42.

both computer and Internet industries(36). If the remote hacking was in past requiring a considerable degree of programming knowledge, hackers nowadays can freely obtain step-by-step hacking instructions on the Internet, and then launch them against online targets. A high degree of skill in computer science is no longer required.(37)

Computer hacking is not carried out with the purposes of manipulation, sabotage or espionage, but for just the pleasure of overcoming the technical security measures in many cases.(38) Individuals who engage in hacking are known as 'hackers', they carry out computer trespass as a mere hobby. Some hackers, however, intend to engage in criminal activity and are known as 'crackers'.(39)

2. Computer sabotage and vandalism

As the individuals, governmental agencies and private companies are all using computer and related devices in their daily various activities using them particularly for storing huge amount of data and information, computer sabotage and extortion represent another danger threatening all activities based on or using computer technologies.

Computer sabotage might be targeting the tangible computer facilities as well as the intangible data containing computer programs and other valuable information. During the 1970s, the most frequently followed methods of causing physical damage were igniting or bombing a building. These techniques were typically applied by 'outsiders' not employed or otherwise related with the owners of the facilities damaged. Today, the most popular method of causing logical damage is through the use of crash programs which can erase large volumes of data within a short period.(40)

(36) ATTORNEY GENERAL OF NEW JERSEY, COMPUTER CRIME - A JOINT REPORT, 48 (2000).

(37) John T. Soma et al, *supra* note 30, at 347; Michael Edmund O'Neill, *supra* note 2, at 246.

(38) Ulrick Sieber, *supra* note 29, at 42.

(39) Jo-Ann M. Adams, Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet, 12 Santa Clara Computer & High Tech. L.J. 403 (1996), at 409.

(40) Ulrick Sieber, *supra* note 29, at 48.

Such destructive programs, collectively known as 'rogue programs'[41], include viruses, worms, Trojan horses and logic bombs[42].

Computer virus is "a program that infects a computer by inserting a copy of itself into the computer and harms the computer in some manner, generally without the computer user's awareness".[43] Viruses are either benign or malicious. Benign viruses are designed to infect a computer without doing any actual damage to the computer or data. Malicious viruses attack computer systems in various ways, often disguising the damage caused until it is extensive.[44] The worm is similar to computer virus, but it multiplies without any human interaction finding its way through a network system without the need to be attached to a file[45]. Trojan horse is a program that appears to be useful or entertaining, but it in fact will attack the computer when the program is run[46] performing an unauthorized function concurrent with its normal function.[47] The logic bomb is a program that performs the unauthorized act once a pre-programmed condition arises, often overriding the normal functioning of the computer.[48] For example, a logic bomb can be instructed to cause an unauthorized event upon a specific date and time.[49]

---

(41) *See* John T. Soma et al, *supra* note 30, at 355.

(42) Daniel J. Kluth, The Computer Virus Threat: A Survey of Current Criminal Statutes, 13 Hamline L. Rev. 297 (1990), at 279.

(43) Eric J. Sinrod & William P. Reilly, Cyber-Crimes, A Practical Approach to the Application of Federal Computer Crime Laws, 16 Santa Clara Com. & High Tech. L. J. 177 (2000), at 216.

(44) Camille C. Marion, Note, Computer Viruses and the Law, 93 Dick. L. Rev. 625 (1989), at 627.

(45) Eric J. Sinrod & William P. Reilly, *supra* note 43, at 223.

(46) Carol C. McCall, Computer Crime Statutes: Are They Bringing the Gap between Law and Technology, 11 Criminal Justice Journal 203 (1988-1989), at 207 n.43.

(47) U.N. CENTER FOR SOCIAL DEV. & HUMANITARIAN AFF., UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME, INT'L REV. CRIM. POL'Y (Nos. 43, 44), at no.64 (1994).

(48) Carol C. McCall, *supra* note 46, at 207 n. 44.

(49) *Id*.

Today, the rouge programs are regarded the main threat in the realm of computer and Internet causing millions of loss every year in all countries around the world.

B. The Criminal Activities Targeting Electronic Commerce Itself

This category includes criminal activities that are targeting the electronic commerce itself directly. The main criminal activities falling into this category include:

1. Fraud, manipulations and theft

Legal scholars, computer technologists and law enforcement authorities are referring into two kinds of fraud and theft perpetrated in the field of computers and Internet; the insider fraud and theft and outsider fraud and theft. The insider is "anyone who has the same or similar access rights into a network, system, or application. Therefore, a trusted insider can be a current or former employee, a contractor, consultant, service provider, software vendor, and so on".(50)

In the earlier days of the emergence of computer misuses, the commercial companies had been facing just the insider fraud and theft. The connections of computers to international telecommunication networks soon provided opportunities commit these computer manipulations from outside the victimized companies. First cases of online manipulations appeared in the United Stated during the 1970s. Today most big companies are connected to the Internet, consequently the Internet is increasingly used to commit online fraud.(51)

This category of criminal activities represents probably the largest category of cybercrime as the Internet has created what has become known as cybercrime - borderless fraud.(52)

(50) KENNETH C. BRANCIK. INSIDER COMPUTER FRAUD AN IN-DEPTH FRAMEWORK FOR DETECTING AND DEFENDING AGAINST INSIDER IT ATTACKS, AUERBACH PUBLICATIONS, 1, 4 (2008).

(51) Ulrich Sieber, *supra* note 29, at 52.

(52) Marc D. Goodman & Susan W. Brenner, *supra* note 6, at 146-7.

Fraud is well known traditional offense in almost all comparative criminal laws; it is "the crime of deliberate deception in order to unjustly obtain property or services".(53) Computer fraud, according to the British Law Commission, is any "conduct which involves the manipulation of a computer, by whatever method, in order to dishonestly obtain money, property or some other advantage of value or to cause loss"(54)

Computer fraud and theft might take several forms; the most common one is what is called online auction fraud.(55) The United States FBI has a special office called Internet Fraud Complaint Center ("IFCC") for investigating computer crimes. Only through one calendar year the said office reported over 16,000 complaints of fraud to law enforcement agencies with the majority of complaints involving Internet auction fraud.(56) Reports indicate that online fraud has resulted in an estimated $2.6 billion in the United States in 2004, $700 million more than in 2003 and more than the prior fraud loss record of $2.1 billion in 2002.(57) In Japan and in December 2006, over 990 cases of fraud were reported totaling losses of 88 million JPY (about $725,100).(58)

Another criminal activity included in this category is the invoice manipulations concerning the payment of bills and salaries of industrial companies as well as the manipulations of account balances and balance sheets at banks were and still are the predominant offences.(59)

(53) UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD), INFORMATION ECONOMY REPORT 201 (2005) [hereinafter UN Information Report].

(54) THE LAW COMMISSION, WORKING PAPER NO. 186, CRIMINAL LAW-COMPUTER MISUSE 9 (1989)

(55) Marc D. Goodman & Susan W. Brenner, *supra* note 6, at 147 (quoting Criminal Threats to E-Commerce 54, INTERPOL, Jan. 2001).

(56) *See* Robert Ditzion, Elizabeth Geddes & Mary Rhodes Computer Crimes, 40 Am. Crim. L. Rev. 285 (2003), at 317

(57) UN Information Report, *supra* note 53, at 201.

(58) Masao Kobayashi & and Takayuki Ito, A Transactional Relationship Visualization System in Internet Auctions (in MAKOTO YOKOO ET AL (EDS), ELECTRONIC COMMERCE - THEORY AND PRACTICE, SPRINGER, 87 (2008).

(59) Ulrich Sieber, *supra* note 29, at 51.

Credit card fraud or theft is also another form of computer fraud and theft. It is regarded as "the classic example and continues to grow with the development of e-commerce activities".(60) It occurs when "a perpetrator illegally obtains the victim's personal information by hacking' into a website where the victim maintains an account or makes purchases".(61) The Internet is especially vulnerable to credit card fraud, this has particularly become apparent since 1990s. For example Kevin Mitnick, who was arrested by FBI in February 1995, was able to steal thousands of credit card numbers from an Internet service provider. Ivy James Lay, an MCI employee in North Carolina, programmed a microcomputer to capture more than 50,000 credit card numbers. Selling the numbers to a network of dealers, he has caused more than $50 million in fraudulent charges.(62) In another case, a nineteen year old Russian student using the name 'Maxim' could steal 300,000 credit card numbers from the computer server of CD Universe. He extorted CD Universe by agreeing to destroy the customer data he had stolen in return of $100,000 cash. CD Universe did not pay the thief quickly enough for his liking, and Maxim published the credit card and customer data of 25,000 victims online.(63)

2. Commercial Espionage

In the age of the computer, almost every piece of information generated by a modern company or other organization eventually finds its way onto a computer somewhere. Information is either recorded on a computer to formalize it or actually created in a computer environment. Nowadays, most executives type their own messages and daily correspondence

(60) UN Information Report, *supra* note 53, at 201.

(61) Shannon L. Hopkin, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, J. of High Tech. L,.101 (2003) at 102.

(62) REBECCA HEROLD (ED.) THE PRIVACY PAPERS - MANAGING TECHNOLOGY, CONSUMER, EMPLOYEE, AND LEGISLATIVE ACTIONS, AUERBACH PUBLICATIONS, 260 (2002) (quoting Cortese, Warding Off the Cyberspace Invaders, *Business Week* , March 13, 1995, p. 92).

(63) Marc D. Goodman & Susan W. Brenner, *supra* note 6, at 147-8 (quoting Criminal Threats to E-Commerce 57, INTERPOL, Jan. 2001).

directly into computers. Computers are used for spreadsheets, databases, project design, and editing, sending receiving tons and tons of e-mail.(64)

Due to the fact that in computer systems, huge quantities of data are stored in an extremely narrow space, and the data can be copied quickly and easily with the help of modern technology, also via data telecommunication, Computer espionage constitutes a special danger compared with traditional economic espionage.(65)

This criminal activity might target several objects including, in particular, computer programs, data of research and defense, data of commercial accounting as well as addresses of clients.(66) In the world of business trade secrets are valuable targets of commercial espionage. According to the United States Supreme Court, trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives one an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers.(67)

3. Intellectual property piracy

As an author has written, "with the advent of digital technology and the capacity of the Internet to move audio, video, text and numeric data from point to point in a short amount of time. As digital technology develops further, cinema fans will access movies at any hour, music fans may sample or download tunes from an historic catalog, art lovers may cyber-

(64) IRA WINKLER, SPIES AMONG US - HOW TO STOP THE SPIES,TERRORISTS, HACKERS, AND CRIMINALSYOU DON'T EVEN KNOW YOU ENCOUNTER EVERY DAY, WILEY PUBLISHING, INC. 22 (2005).

(65) Ulrich Sieber, *supra* note 29, at 44.

(66) *Id.*

(67) MIKE GODWIN, CYBER RIGHTS - DEFENDING FREE SPEECH IN THE DIGITAL AGE, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 216 (2003) (quoting *Kewanee Oil Co. v. Bicron Corp* (1974).

tour any great museum in the world, and e-book purchasers may replace visits to libraries and bookstores with convenient downloads".(68)

However, the same technology also presents a danger for content producers. As copying material to a computer hard drive can be the first step in making content available for unauthorized distribution to any computer on the planet. Illegally distributed copies then may reasonably be expected to substitute for legal purchases, and to harm producer incentives in the process.(69)

It is well known fact that the intellectual property piracy existed many decades ago even before the emergence of computers and the Internet. They have, however, made the piracy and theft of intellectual property easier to be performed in one side and coast much more of losses in another.

If someone in 1980 wanted to pirate an album, he had to buy a legitimate copy, buy expensive recording equipment to copy the album to tape or audiocassette, and also reproduce the album cover and other accompanying material. With very poor quality, he might only able to copy the album about twenty-five times per day. The next problem was then selling illegal copies on the street which is highly visible; the police might see the operation and shut it down. In the computer age even copies of copies are now almost perfect, copying costs are nil; you can simply download the album once to your computer and post the material once on the internet. Within minutes, your album could be distributed across the world. You can sell online without being known by your customers, even if law enforcement infiltrated your site, they would not necessarily know your true identity(70)

Copyright piracy is now representing a great threat and challenge to the electronic commerce. According to The Business Software Alliance which is a software industry trade group, international software piracy costs U.S.

(68) MICHAEL A. EINHORN, MEDIA, TECHNOLOGY AND COPYRIGHT – INTEGRATING LAW AND ECONOMICS, EDWARD ELGAR PUBLISHING, 6 (2004).

(69) *Id.*

(70) Neal Kumar Katyal, *supra* note 32, at 1031-32

software makers $12 billion dollars annually.(71) Music piracy causes an estimated $300 million annual loss to the recording industry(72). Software piracy costs the United States some 109,000 jobs and $991 million in tax revenue.(73)

IV. THE COMBATING STRATEGIES

Crimes and criminal activities had been existed throughout the history of mankind. The crime had been, and stills, the major threat to the lives of people and their different kinds of their interests everywhere in the world. Societies have always been trying to fight crimes and criminal activities by all available means and ways. The history of crime control indicates that crimes can not be prevented hundred per cent, their rates, however, can be reduced to a considerable levels.

The history is also telling us that every new technology invented to serve humanity has brought new types of criminal activities. In some cases the new technology itself has been a target of crimes, in other cases it has provided criminal with new tools that facilitate the perpetration of the crime. For this reason, with the emergence of new types of criminal activities attached to a new technology, the question of the possible ways and useful strategies has always been the subject of debates.

The mentioned reality is also true in the case of the electronic commerce. The rapid development of this kind of commerce in the world in one side, and the rapid increase of the rate of criminal activities threatening it in another side, have made the strategies of combating such

(71) Adam G. Ciongoli et al, Ninth Survey of White Collar Crime – Computer-Related Crimes, 31 Am. Crim. L. Rev. 425 (1994), at 447 (citing This Lobby Speaks Software and Carries a Big Stick, BUSINESS WEEK, March 22, 1993, at 88).

(72) Michael Edmund O'Neill, *supra* note 2, at 262-3 (citing UNITED STATES DEPARTMENT OF JUSTICE, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET 7 (2000).

(73) *Id*, at 273 (citing Joel Smith, Software Piracy Cost Business Billions, USA TODAY, July 3, 2000).

criminal activities to be one of the major legal question in the field of the electronic commerce.

Combating criminal activities threatening electronic commerce is a great challenge to all countries all over the world. It is a hard task and in need of adopting, simultaneously, more than one strategy. In the following subsections, we are going to discuss the main of these strategies.

A. Legislative Confrontation

When the computer misuse activities begun to emerge on a wide scale in 1970s legal scholars and computer experts have sharply differed over the best way of confronting such activities. (74)

The axis of the dispute was specifically about the question whether new legislation were necessary to be enacted for combating the new activities that have emerged with the rapid spread of computer uses or the existing legislation were enough to address the problem. Some legal scholars had taken the position that new legislation were completely unnecessary because the existing legislation were quite sufficient to successfully prosecute any type of computer abuses.(75) In contrast to this, other legal scholars had seen that existing legal rules which had been enacted long before the invention of computer and the Internet were not suitable for the digital age.

Later, the experience proved the reality of the second view. It has become clear that all types of computer misuses could not be treated by existing penal provisions designed for traditional offences(76); some of these misuses were beyond the reach of such provisions.(77) As a result, many of countries in the world have taken various legislative steps.

There is now a common believe in the world that the main and necessary step for combating criminal activities attached to the computer

(74) Amalia M. Wagner, The Challenge of Computer – Crime legislation: How Should New York Respond, 33 Buff. L. Rev. 777 (1984), at 795.

(75) Carla Ottaviano, *supra* note 26, at 167.

(76) Elizabeth A. Glynn, Computer Abuse: The Emerging Crime and the Need for Legislation, 12 Fordham Urb. L.J. 73 (1984), at 100.

(77) DONN B. PARKER, FIGHTING COMPUTER CRIME, Ch. 8 (1983), at 239.

and the Internet is representing in new criminal legislation punishing all kinds of such activities. The circle of the countries that legislatively responded to the problem is constantly expanding.

Of course, the leading industrialized countries in the world have preceded the developing countries in this believe. They have witnessed several waves of legislation addressing different issues related to computer and the Internet during the period between 1970s and the mid of 1990s.(78)

In resent years the Middle East countries witnessed considerable legislative movement against the illegal activities targeting computer, Internet and the electronic commerce. In 2006, the United Arab Emirates enacted its "Law on Combating Information Technology Crimes", the law no.2 of the year 2006. The law with its twenty-nine articles provides, *inter alia*, a strong legislative protection to the electronic commerce components.

For a comprehensive legislative protection of the electronic commerce, it is necessary for the legislator to enact specific criminal legislation to address different criminal activities which experience indicates their negative impacts on the mentioned kind of the commerce. In this context, special focus should be made on the following aspects:

1- General criminal protection of the computer and Internet:

This can be achieved by enacting new criminal provisions either by inserting them to the existing criminal laws or in new and separate legislation. The main idea governing this legislative step, which has become the common idea after a long period of debates, is that the new specific computer crime legislation is needed to cover only those crimes that are unique to computers themselves not crimes that are facilitated or

(78) *See* Ulrick Sieber, *supra* note 29, at Sec. I.B.2, The Main Waves of Computer Crime Legislation (classifying the these waves as to their subject matters into six categories, privacy protection - in the 1970s and 1980s, computer-related economic crimes - at the beginning of the 1980s, computer related intellectual property rights - in the course of 1980s, illegal and harmful contents - in 1980s and mid-1990s, criminal procedural law – in 1980s, and the creation of requirements for and prohibitions of security measures - in 1990s).

furthered through the use of a computer.(79) According to the United Nations, there are four basic substantive computer offenses which should be criminalized by the legislator; unauthorized access, unauthorized access with intention to commit a further offense, intentional unauthorized modification offense, and misuse of devices: "[t]he computer integrity activities addressed in the international instruments can be broadly classified into four categories: offences concerning access to data and systems; offences relating to interference with data and systems; offences concerning the interception of data in the course of their transmission; offences concerning the use of tools or "devices" to carry out any of the above acts."(80)

2- Criminal protection of digital rights:

The intellectual property rights have been protected on both national and international levels. This has given authors and other innovators strong incentives to develop and distribute thousands of exciting new products.

As we saw previously, in the digital age copyright piracy represented in the online theft of creative property is forming one of the most significant problem and challenge to the electronic commerce. Thousands of copies of copyrighted computer programs, electronic books, music, movies and other kind of digital products are stolen by pirates every day.

Although the experience indicates that the piracy of intellectual property rights can not be eradicated, some measures by governments could diminish its range to a considerable level. One of these measures is to enact new legislation, proper to the information era, providing stronger protection the digital products.

New interference by the legislator represented in adopting new legislation determining legal protection to what is called multimedia products has been one of the major legal issues dealt with by legal scholars. It is clear that the traditional criminal laws protect different types of intellectual property rights; however the wording of such criminal laws

(79) *See* e.g., Steve Shackelford, Computer-Related Crime: An International Problem in Need of an International Solution, 27 Tex. Int'l L.J. 479 (1992), at 500; Stephen P. Heymann, Legislating Computer Crime, 34 Harv. J. on Legis. 373 (1997), at 380.

(80) UN Information Report, *supra* note 53, at 235.

do not encompass violations targeting new types of intellectual property emerged in the age of the computer. (81) Courts in the western countries had been facing a real challenge in submitting such violations, like copying a computer program, to the traditional criminal provisions such as the provisions related to theft, extortion or larceny. (82) Taking all these facts together alongside the great deal of multimedia products that have been the subject of the electronic commerce nowadays, it is very important that the legislator provide real legal protection to such products. (83)

3- Direct criminal protection of the electronic commerce:

We mean by this criminal protection those punitive provisions that determine proper punishments for criminal activities targeting particularly the means and methods of the electronic commerce such as the electronic signature and electronic documents.

As related to the legislative technique which might be followed by the legislation in terms of the best place in which the suggested punitive provisions are put, reference can be made into four options; they can be stipulated in the electronic commerce regulation legislation, inserted to the already existing criminal laws, inserted to the statutes which are laid down specifically of the computer crimes, or included in separate legislation.

Whatever option is chosen by the legislator, considerable attention should be paid to the criminal protection of some decisive devices and tools that are regarded as the cornerstones of the electronic commerce. These include the electronic signature and electronic documents.

(81) *See* Ulrick Sieber, *supra* note 29, at sec. I.B., The Concept of Computer-Related Criminal Law, and for details about the differences between multimedia products and existing copyright works, *see* IRINI A. STAMATOUDI, COPYRIGHT AND MULTIMEDIA PRODUCTS - A COMPARATIVE ANALYSIS, CAMBRIDGE UNIVERSITY PRESS, 23-41 (2002).

(82) *See* Carla Ottaviano, *supra* note 26, at 163; Stephen P. Heymann, *supra* note 79, at 381.

(83) For more details about the justifications for protecting multimedia works, *see* TANYA APLIN, COPYRIGHT LAW IN THE DIGITAL SOCIETY, HART PUBLISHING, 2, 16-35 (2005).

The electronic signature, also called 'digital signature', and 'e-signature', is defined as a "form of encryption that allows online users to sign documents, pay bills, bank, and shop online with an electronic or digital signature unique to only them."(84)

Since a digital signature is created when a sender uses his or her private key to encrypt a message, it is, therefore, an integral part of the encryption process. As such, encryption prevents confusion and fraud in the Internet Age and provides the security required by persons doing business in a non–face-to-face manner. In light of this reality, digital signature is an increasingly important technology in the new Internet Age. It provides the means for any intended recipient to receive a highly secure, identifiable private message that cannot be altered or decrypted by others. Without this digital verification, e-commerce and advanced uses of communication could not proceed to its fullest potential.(85)

B. Self Protection

Another line of defense against criminal activities threatening the electronic commerce is for individuals to employ the technology to protect themselves. Industry-developed and supplied encryption technologies and firewalls, for example, provide individuals with substantial tools to guard against unwarranted intrusions.(86) This argument is supported by, and might be originated from, a common feeling that the criminal activities, generally, can not be abolished by the law alone.(87) It has been said in this concern that "[i]n the final analysis, laws will not make computer networks more secure. The problem of computer crime will be solved only when makers of computer technology build more secure systems and when owners, operators and users of computer systems operate their systems in

(84) J. A. HITCHCOCK, NET CRIMES & MISDEMEANORS: OUTMANEUVERING WEB SPAMMERS, STALKERS, AND CON ARTISTS, SECOND EDITION, 327 (2006).

(85) SHARON K. BLACK, TELECOMMUNICATIONS LAW IN THE INTERNET AGE, ACADEMIC PRESS, 347 (2002).

(86) PETE LOSHIN & JOHN VACCA, ELECTRONIC COMMERCE, CHARLES RIVER MEDIA, 2 (2004)

(87) Carla Ottaviano, *supra* note 26, at 169.

more secure manner. By and large, this is an area in which the private sector must lead. It is not the government's role to dictate standards or control technology design. Governments do need, however, to secure their own computer systems with proper security practices".(88)

The experience shows that private protection is not less effective than the law in decreasing the rate of criminal activities in the society. Some experts are regarding such private protection even as "the first and best line of defense".(89) Others have asserted that strategies focusing solely on increasing the effectiveness of prosecution will inevitably fail.(90)

The technology has provided electronic commerce with many security measures by which a strong capacity of defense might be realized against the different types of activities threatening it. These security measures include various security software and hardware designed to protect computers and computer networks anti- viruses and anti- spies and other techniques.

Commercial entities should adopt security measures to ensure the safety of their electronic business.(91) Their concerns should not be related only to the payment systems, but to a range of issues that stem from being connected to the Internet. Developing adequate security measures should be high on the agenda of any Internet commerce development team.(92) The organization should develop a security policy that covers the entire information system. It should outline the general policies in relation to security, the levels of security that should be adopted, the key risks, and the individuals who are responsible for maintaining security.(93)

(88) Global Internet Policy Initiative, Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime (2002), at 2. Available at: http://www.internetpolicy.net/cybercrime/20050900cybercrime.pdf (Jan. 31, 2009).

(89) PETE LOSHIN & JOHN VACCA, *supra* note 86, at ch.2.

(90) Brian C. Lewis, *supra* note 33, at 1353.

(91) Laura J. Nicholson et al, Computer Crimes, 37 Am. Crim. L. Rev. 207 (2000), at 255 ("[b]usinesses want to protect commercial transactions and increase the use of the Internet for commercial purposes").

(92) CRAIG STANDING, *supra* note 1, at 157.

(93) *Id*.

Combating Criminal Activities Threatening Electronic Commerce

The modern technology has created many techniques by which commercial corporate can protect their electronic business. The encryption, firewall and anti viruses, and authentication are the major techniques for attaining security needed for the safety electronic commerce. Below we shed more lights of these techniques.

1- Encryption

Encryption is the use of mathematical and other devices to encode information so that it is intelligible only to users possessing the appropriate key to decipher it.(94) It is also defined as "applying a scrambling function to a given set of data so that only those who possess the right 'key' can restore the encrypted data to its original form".(95) Encryption, in brief, is the use of mathematical algorithms to convert digital information into a different format so it cannot be decoded without a password.(96)

Encryption has been used to secure communications for centuries, and remains a cornerstone of commercial and governmental communications, its technology is not difficult to use. Indeed, with sufficient computing power, just one individual can simply multiply two large prime numbers together to create an encryption code.(97)

The modern encryption technology, taken the either the form of hardware or software, made it possible for trade companies to protect sensitive information included in e-mails, database information and other electronic documents with an electronic locks providing a strong protection against thieves, hackers, and industrial spies.

2- Firewalls and Anti-viruses

The second major technique is represented in what is called the firewall and anti-viruses.

(94) Michael Edmund O'Neill , *supra* note 2, at 268 (citing David Hricik, Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-Mail, 11 GEO. J. LEGAL ETHICS 459, 493 (1998).

(95) Michael Lee et al., Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal, 14 Berkeley Tech. L.J. 839 (1999), at 851.

(96) Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U. Pa. L. Rev., 709 (1995), at 714.

(97) Michael Edmund O'Neill , *supra* note 2, at 268-9.

Firewall is like checkpoints or a tollgate. It requires all traffic passing through, whether in or out, to request permission. Without the proper authorization, the firewall will either block the traffic or channel it to specific designated areas until express authorization is given.(98)

Firewalls are devices that secure one network segment from another; the device can be either a single-purpose computer or a computer with application software loaded. Good firewalls can prevent many attacks from outside an organization, if they are properly configured.(99)

The important feature of the firewall system is that it can be used to protect a network or system from both outside and inside threats. The firewall could be used to separate the intranet from other systems within the organization or outside of the organization.(100)

On the other side, anti-viruses software prevents just about all known virus attacks. It can also help prevent Trojan horses and other destructive programs. As dozens of new viruses appear every week, vendors update the software weekly or sometimes more often for rapidly spreading attacks. In order the process goes easily, all common anti-virus software has a feature that allows for automatic updates.(101)

Adopting strong firewall systems might impose large costs including hardware and software purchases, programmer time, hardware maintenance and software upgrades, administrative setup and training, inconveniences and lost business opportunities resulting from a broken gateway or denial of services, and an inevitable loss in connectivity.(102) The same is true in the case of anti-virus software. There is, however, no other choice for commercial entities rather than affording such costs for protecting the trust and confidence upon which the electronic commerce they exercise is depending.

---

(98) *Id*, at 277-8 (citing WILLIAM R. CHESWICK & STEVEN M. BELLOVIN, FIREWALLS AND INTERNET SECURITY: REPELLING THE WILY HACKER 9 (1994); Neal Kumar Katyal, *supra* note 32, at 1083.

(99) IRA WINKLER, *supra* note 64, at 279.

(100) CRAIG STANDING, *supra* note 1, at 159.

(101) IRA WINKLER, *supra* note 64, at 236.

(102) Neal Kumar Katyal, *supra* note 32, at 1084.

3- Authentication

Authentication "means a function for establishing the validity of a claimed identity of a user, device or another entity in an information or communications system".(103) Authentication deals with proving the identity of a person. It takes many forms; passwords, hardware tokens, smart cards, and biometric properties such as fingerprints or retinal patterns are all forms of authentication. Of course passwords are the most commonly used form of authentication.(104)

C. Governmental Measures

The legal scholars and computer technicians and experts argue that the governments should also take specific measures in terms of combating criminal activities that threaten electronic commerce. In this concern, they are particularly focusing on the question of law enforcement question.

The main idea here is that the modern information technology has brought new criminal activities which have their unique own characteristics, therefore the traditional model of law enforcement is not useful and effective in the field of computer crimes and the law enforcement personnel face real difficulties if they are limited computer literacy.(105) For these reasons governments should adopt new strategies and have to make a comprehensive review of the traditional methods of crime detection in order to successfully deal with computer criminals.(106)

The first step that must be taken by the governments in this concern is to adopt adequate training measures for all individuals involving in prevention, investigation and prosecution of computer and the Internet

(103) David Goldstone & Betty-Ellen Shave, International Dimensions of Crimes in Cyberspace, 22 Fordham Int'l L.J. 1924 (1999) at 1965.

(104) CRAIG STANDING, *supra* note 1, at 161-2.

(105) This was one of the major problems that industrialized countries have faced when they first laid down their computer crime related criminal legislation. *See* Marc D. Goodman, Why the Police Don't Care About Computer Crime, 10 Harv. J. L. & Tech. 465 (1997) at 491-4.

(106) *See* Jessica McCausland, Note, Regulating Computer Crime After Reno v. Aclu: The Myth of Additional Regulation, 49 Fla. L. Rev. 483 (1997), at 503; Ellen S. Podgor, *supra* note 4, at 317.

related criminal activities.(107) They have to be well trained and quite familiar with both technical and legal aspects of the new types of criminal activities.

This kind of the governmental measures is, as more than one commentators indicated, justified by the fact that the electronic crime investigations require specialized training and experience on the part of law enforcement agents and prosecutors.(108)

In addition to this and in the light of the realities that computer technologies evolve at phenomenal rate, and high-tech criminal techniques and capabilities change more rapidly than those in more traditional areas of criminal activity(109), legal scholars argue that the training should be provided to those involving in the investigation and prosecution of high-tech cases.(110)

Some countries in the world have practically taken these suggestions in consideration. For example, in the United States, high-tech prosecutors at the federal level attend a one-week training course every year. The training provided by both government and private sector personnel. Similarly, all federal investigative agencies provide high-tech training to their agents. The government's National Cybercrime Training Partnership is developing high-tech training for federal, state, and local law enforcement personnel.(111)

Another measure which has been suggested by many legal scholars as well as by computer experts is the establishment of special computer-competent police forces which all its officers should attain a minimal level

(107) UN Information Report, *supra* note 53, Ch.6.E.Concluding remarks and policy recommendations.

(108) David Goldstone & Betty-Ellen Shave, *supra* note 103, at 1940.

(109) Michael A. Sussmann, The Critical Challenges from International High-Tech and Computer-Related Crime at The Millennium, 9 Duke J. of Comp. & Int'l L. 451 (1999), at 464.

(110) Scott Charney & Kent Alexander, Computer Crime, 45 Emory L. J. 931 (1996), at 944.

(111) Michael A. Sussmann, *supra* note 109, no. 49 (citing Martin Kettle & Owen Bowcott, Computer Crime: The Age of the Digital Sleuth, The Guardian, Dec. 12, 1997, at 19).

of competency about the crimes they investigate. In this concern, Marc D. Goodman, a senior sergeant and investigator for the Los Angeles Police Department writes in a note of him in Harvard Journal of Law and Technology: "[f]or the bulk of the police force, the levels of computer literacy necessary to function are relatively low. It is certainly not necessary for every police officer to have a Ph.D. in computer science in order to be effective in the twenty-first century. However, a basic level of computer literacy must be mandated so that officers can ask the basic questions about the crimes they will be investigating. Patrol officers must be trained to recognize a high-technology crime when it occurs. Furthermore, these "first responders" must understand the importance of calling in an expert to deal with such situations. A lack of attention or willingness to call in a computer crime specialist can have negative consequences for police departments attempting to preserve evidence, arrest a perpetrator, or successfully pursue a prosecution in court. If a computer examination is not conducted properly, valuable evidence may be lost, and the police department involved may be liable for any damage caused to the computer".(112)

Again, many countries in the world have taken practical steps in this context establishing specific offices, departments or task force police to deal exclusively with high-tech criminal activities. For instance, the United States Federal Bureau of Investigations has launched several units dedicated to investigating computer crimes. One of these units is called Cyber Action Teams which are small, highly-trained teams of FBI agents, analysts, and computer forensics and malicious code experts who travel the world on a moment's notice to respond to fast-moving cyber threats. Another unit is Connecticut Computer Crimes Task Forces. This unit is responsible of taking calls from an Internet scam victims. The third unit is called Internet Crime Complaint Center which receives cyber crime complaints. The Center works closely with a range of law enforcement

(112) Marc D. Goodman, *supra* note 102, at 492. *See* also Michael A. Sussmann, *supra* note 109, at 363 ("[t]he complex technical and legal issues raised by computer-related crime require that each country have individuals who are dedicated to high-tech crime".

agencies and private sector organizations, and releases annual statistics and performs analysis and research.(113)

Recently, a similar step was taken in the United Kingdom when the government established special cybercrime unit called Police Central e-Crime Unit (PCeU). The Units' purpose is "[t]o create a national centre of excellence to combat e-crime in England, Wales and Northern Ireland. Its mission is "[t]o improve the police response to victims of e-crime by developing the capability of the Police Service across England, Wales and Northern Ireland, co-rdinating the law enforcement approach to all types of e-crime, and by providing a national investigative capability for the most serious e-crime incidents."(114) Another example from developing countries is India. In Mumbai, The Cyber Crime Investigation Cell of Mumbai Police was inaugurated on 18th December 2000.(115)

Besides the continuous training, the successful of such unites depends upon some other decisive conditions. The most important one is providing such unites with the necessary technical equipments including the latest hardware and software.(116)

Another governmental measure against Internet crime is the "improvement of cooperation between national law enforcement agencies. At one level, cooperation will involve mutual assistance in the obtaining and exchange of information, whether as intelligence or evidence."(117) We can add to this the cooperation between the law enforcement agencies and the private sector. Commercial companies exercising electronic commerce could be a great support of the law enforcement agencies in preventing,

(113) *See* FED. BUREAU OF INVESTIGATIONS, CYBER INVESTIGATIONS, available at: http://www.fbi.gov/cyberinvest/cyberhome.htm (Mar. 12, 2009).

(114) See, ETROPOLITAN POLICE, POLICE CENTRAL E-CRIME UNIT, available at: http://www.met.police.uk/pceu/index.htm (Mar. 12, 2009).

(115) *See* CRIME BRANCH, CRIMINAL INVESTIGATION DEPARTMENT, MUMBAI, INDIA, CYBER CRIME INVESTIGATION CELL, available at: http://www.cybercellmumbai.com/ (Mar. 12, 2009).

(116) Michael A. Sussmann, *supra* note 109, at 464; Marc D. Goodman, *supra* note 102, at 485

(117) UN Information Report, *supra* note 53, at 242.

following up and even prosecuting the criminal activities threatening this kind of commerce.

It is, however, necessary to be said that the mentioned cooperation is obviously and negatively affected by reluctance of victims to report computer crimes, the fact approved by the history of computer related criminal activities, which regarded as one of the major factors making the prosecution of computer crimes more difficult.(118) For this reason, the challenge, as one commentator says, is "to educate users and operators on how to prevent computer crime and to convince them of the desirability of reporting such crime."(119)

V. CONCLUSION

The electronic commerce represents a main results of what is called digital age. Since it changed, or at least affected, many concepts, methods, and practices in the realm of the commerce, it deserves to be described as a revolution in the field of the business.

Although the electronic commerce has raised many complex legal issues linked to different branches of the law, the most decisive question is the question of the legislative and non-legislative protection which might provide this important kind of commerce with a strong shield against the increasing criminal activities threatening it.

The criminal activities threatening electronic commerce are varied and might take so many forms. They, however, can be classified into two main categories; the criminal activities targeting Internet and computer crimes, and the criminal activities targeting the electronic commerce particularly. The first category includes hacking and computer sabotage and vandalism, while the second one includes fraud, manipulations and theft, commercial espionage, and intellectual property piracy.

(118) *See* William S. Allred, Criminal Law – Connecticut Adopts Comprehensive Computer Crime Legislation: Public Act 84-206, 7 W. New Eng. L. Rev. 807 (1985), at 820.

(119) *See* Dodd S. Griffith, The Computer Fraud and Abuse Act of 1986: A Measured Response to A Growing Problem, 43 Vand. L. Rev. 453 (1990), at 490.

Combating criminal activities threatening electronic commerce forms a great challenge to all countries all over the world. It is a hard task and requires from nations to adopt, at same time, more than one strategy.

The first strategy is the legislative confrontation. This means enacting specific criminal legislation to address different criminal activities which experience approved their negative impacts on this kind of the commerce. In this regard, three kind of protection should be laid down by the legislators;

- General criminal protection of the computer and Internet: this can be done by enacting new specific computer crime statutes addressing those crimes that are unique to computers themselves. The crimes that are facilitated or furthered through the use of a computer can usually be subjected to the existing traditional criminal laws.

- Criminal protection of what is called digital rights: this can be achieved by enacting new legislation that provides stronger protection to the digital products such as copyrighted computer programs, electronic books, music, movies and other kind of digital products.

- A direct criminal protection of the electronic commerce: this means enacting punitive provisions that determine proper punishments for criminal activities targeting particularly the means and methods of the electronic commerce such as the electronic signature and electronic documents.

After the legislative protection, self protection comes as another indispensable line of defense against criminal activities threatening the electronic commerce. It should be understood that criminal activities, generally, can not be abolished by the law alone. The private protection is not less effective than the law in decreasing the rate of criminal activities in the society. The technology has provided electronic commerce with many security measures by which a strong capacity of defense might be realized against the different types of activities threatening it. These security measures include various security software and hardware designed to protect computers and computer networks anti- viruses and anti- spies and other techniques.

The third strategy which should be adopted is the governmental measures. This includes adopting new strategies and making a

comprehensive review traditional model of law enforcement in order to successfully deal with computer criminals. Adequate training measures should be adopted for all individuals involving in prevention, investigation and prosecution of computer and the Internet related criminal activities. Another measure is the establishment of special computer-competent police forces which all its officers should attain a minimal level of competency about the crimes they investigate. These special units have to be provided with the necessary technical equipments including the latest hardware and software.

REFERENCES

(a) Books:

- ATTORNEY GENERAL OF NEW JERSEY, COMPUTER CRIME - A JOINT REPORT (2000).
- CRAIG STANDING, INTERNET COMMERCE DEVELOPMENT, ARTECH HOUSE (2000).
- DIANE ROWLAND & ELIZABETH MACDONALD, INFORMATION TECHNOLOGY LAW, CAVENDISH PUBLISHING LIMITED, LONDON (2000).
- DONN B. PARKER, FIGHTING COMPUTER CRIME (1983).
- HOSSEIN BIDGOLI, ELECTRONIC COMMERCE, PRINCIPLES AND PRACTICE, ACADEMIC PRESS (2002).
- IRA WINKLER, SPIES AMONG US - HOW TO STOP THE SPIES,TERRORISTS, HACKERS, AND CRIMINALSYOU DON'T EVEN KNOW YOU ENCOUNTER EVERY DAY, WILEY PUBLISHING, INC. (2005).
- IRINI A. STAMATOUDI, COPYRIGHT AND MULTIMEDIA PRODUCTS - A COMPARATIVE ANALYSIS, CAMBRIDGE UNIVERSITY PRESS (2002).
- J. A. HITCHCOCK, NET CRIMES & MISDEMEANORS: OUTMANEUVERING WEB SPAMMERS, STALKERS, AND CON ARTISTS, SECOND EDITION (2006).
- JOSEPH MIGGA KIZZA, ETHICAL AND SOCIAL ISSUES IN THE INFORMATION AGE, SPRINGER-VERLAG LONDON LIMITED (2007).
- KENNETH C. BRANCIK. INSIDER COMPUTER FRAUD AN IN-DEPTH FRAMEWORK FOR DETECTING AND DEFENDING AGAINST INSIDER IT ATTACKS, AUERBACH PUBLICATIONS (2008).
- MAKOTO YOKOO ET AL (EDS), ELECTRONIC COMMERCE - THEORY AND PRACTICE, SPRINGER (2008).

- M. BACHETTA, ET AL, ELECTRONIC COMMERCE AND THE ROLE OF THE WTO (1998).
- MICHAEL A. EINHORN, MEDIA, TECHNOLOGY AND COPYRIGHT – INTEGRATING LAW AND ECONOMICS, EDWARD ELGAR PUBLISHING (2004).
- MIKE GODWIN, CYBER RIGHTS - DEFENDING FREE SPEECH IN THE DIGITAL AGE, MASSACHUSETTS INSTITUTE OF TECHNOLOGY (2003).
- PETE LOSHIN & JOHN VACCA, ELECTRONIC COMMERCE, CHARLES RIVER MEDIA (2004).
- REBECCA HEROLD (ED.) THE PRIVACY PAPERS - MANAGING TECHNOLOGY, CONSUMER, EMPLOYEE, AND LEGISLATIVE ACTIONS, AUERBACH PUBLICATIONS (2002).
- SHARON K. BLACK, TELECOMMUNICATIONS LAW IN THE INTERNET AGE, ACADEMIC PRESS (2002).
- S. K. BLACK, TELECOMMUNICATIONS LAW IN THE INTERNET AGE, MORGAN KAUFMANN, USA (2002).
- SYED MAHBUBUR RAHMAN, ELECTRONIC COMMERCE: OPPORTUNITY AND CHALLENGES, IGI PUBLISHING (2000).
- TANYA APLIN, COPYRIGHT LAW IN THE DIGITAL SOCIETY, HART PUBLISHING (2005).
- THE LAW COMMISSION, WORKING PAPER NO. 186, CRIMINAL LAW- COMPUTER MISUSE (1989)
- U.N. CENTER FOR SOCIAL DEV. & HUMANITARIAN AFF., UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME, INT'L REV. CRIM. POL'Y (Nos. 43, 44).
- UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD), INFORMATION ECONOMY REPORT (2005).
- YUN ZHAO, DISPUTE RESOLUTION IN ELECTRONIC COMMERCE, MARTINUS NIJHOFF PUBLISHERS (2005).

(b) Articles, Notes and Papers:

- Adam G. Ciongoli et al, Ninth Survey of White Collar Crime – Computer-Related Crimes, 31 Am. Crim. L. Rev. 425 (1994).
- Amalia M. Wagner, The Challenge of Computer – Crime legislation: How Should New York Respond, 33 Buff. L. Rev. 777 (1984).
- Brian C. Lewis, Prevention of Computer Crime Amidst International Anarchy, 41 Am. Crim. L. Rev. 1353 (2004).
- Camille C. Marion, Note, Computer Viruses and the Law, 93 Dick. L. Rev. 625 (1989).
- Carla Ottaviano, Computer Crime, 26 IDEA 163 (1985-1986).
- Carol C. McCall, Computer Crime Statutes: Are They Bringing the Gap between Law and Technology, 11 Criminal Justice Journal 203 (1988-1989).
- Catherine T. Clarke, From CrimINet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet, 75 Or. L. Rev. 191 (1996).
- Daniel J. Kluth, The Computer Virus Threat: A Survey of Current Criminal Statutes, 13 Hamline L. Rev. 297 (1990).
- David Goldstone & Betty-Ellen Shave, International Dimensions of Crimes in Cyberspace, 22 Fordham Int'l L.J. 1924 (1999).
- Dodd S. Griffith, The Computer Fraud and Abuse Act of 1986: A Measured Response to A Growing Problem, 43 Vand. L. Rev. 453 (1990).
- Elizabeth A. Glynn, Computer Abuse: The Emerging Crime and the Need for Legislation, 12 Fordham Urb. L.J. 73 (1984).
- Ellen S. Podgor, International Computer Fraud: A Paradigm for Limiting National Jurisdiction, 35 U.C. Davis L. Rev. 267 (2002).
- Eric J. Sinrod & William P. Reilly, Cyber-Crimes, A Practical Approach to the Application of Federal Computer Crime Laws, 16 Santa Clara Com. & High Tech. L. J. 177 (2000).

- Global Internet Policy Initiative, Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime (2002). Available at:

  http://www.internetpolicy.net/cybercrime/20050900cybercrime.pdf
- Gregory E. Maggs, Regulating Electronic Commerce, 50 Am. J. Comp. L. 665 (2001).
- Jessica McCausland, Note, Regulating Computer Crime After Reno v. Aclu: The Myth of Additional Regulation, 49 Fla. L. Rev. 483 (1997).
- Jo-Ann M. Adams, Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet, 12 Santa Clara Computer & High Tech. L.J. 403 (1996).
- Julie A. Tower, Hacking Vermont's Computer Crimes Statute, 25 Vt. L. Rev. 945 (2001).
- Laura J. Nicholson et al, Computer Crimes, 37 Am. Crim. L. Rev. 207 (2000).
- Marc D. Goodman & Susan W. Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, 10 Int'l J.L. & Info. Tech., 39 (2002).
- Marc D. Goodman, Why the Police Don't Care About Computer Crime, 10 Harv. J. L. & Tech. 465 (1997).
- Michael A. Sussmann, The Critical Challenges from International High-Tech and Computer-Related Crime at The Millennium, 9 Duke J. of Comp. & Int'l L. 451 (1999).
- Michael Edmund O'Neill, Old Crimes in New Bottles: Sanctioning Cybercrime, 9 Geo. Mason L. Rev, 237 (2000).
- Michael Froomkin, The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution, 143 U. Pa. L. Rev., 709 (1995).
- Michael Lee et al., Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal, 14 Berkeley Tech. L.J. 839 (1999).
- Neal Kumar Katyal, Criminal Law in Cyberspace, 149 U. Pa. L. Rev. 1003 (2001).

- Robert Ditzion, Elizabeth Geddes & Mary Rhodes Computer Crimes, 40 Am. Crim. L. Rev. 285 (2003).
- Scott Charney & Kent Alexander, Computer Crime, 45 Emory L. J. 931 (1996).
- Shannon L. Hopkin, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, J. of High Tech. L,.101 (2003).
- Stephen P. Heymann, Legislating Computer Crime, 34 Harv. J. on Legis. 373 (1997).
- Steve Shackelford, Computer-Related Crime: An International Problem In Need Of An International Solution, 27 Tex. Int'l L.J. 479 (1992).
- Susan W. Brenner, Is There Such a Thing as "Virtual Crime?" 4 Cal. Crim. L. Rev. 1 (2001).
- Susan W. Brenner, Toward a Criminal Law for Cyberspace: Distributed Security, 10 B.U. J. Sci. & Tech. L. 1 (2004).
- Swanson & Territo, Computer Crime: Dimensions, Types, and Investigation, 8 J. of Police Sci. and Ad. 304 (1980).
- Ulrick Sieber, Legal Aspects of Computer-Related Crime in the Information Society, COMCRIME Study prepared for the European Commission 19 (Jan. 1998), available at: http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc (Jan. 27, 2009).John T. Soma et al, Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed? 34 Harv. J. on Legis. 317 (1997).
- William S. Allred, Criminal Law – Connecticut Adopts Comprehensive Computer Crime Legislation: Public Act 84-206, 7 W. New Eng. L. Rev. 807 (1985).