A Critical Look at the Regulation of Cybercrime

A Comparative Analysis with Suggestions for Legal Policy

Mohamed CHAWKI *

* LL.B (1998), BA (1998), LL.M (2000), DU (2003). Member of the Council of State (*Conseil d'Etat*). Member of several NGOs. Phd Researcher at the School of Law, University of Lyon III, France.
mohamed_chawki@hotmail.com

"*Instantaneous global communications have given us a window on the world through which can be seen both the wonder of it all and the things that make us wonder about it all*"

John Naisbitt (Global Paradox: 1994)

Abstract:

Cybercrime cut across territorial borders, creating a new realm of illegal human activity and undermining the feasibility--and legitimacy--of applying laws based on geographic boundaries. Territorially-based law-making and law-enforcing authorities find cybercrime deeply threatening. It has subjected the nation-State to unprecedented challenges with regard to its efficacy, sovereignty and functions. However, established territorial authorities may yet learn to defer to the self-regulatory efforts of Cyberspace participants who care most deeply about this new digital trade in ideas, information, and services. Separated from doctrine tied to territorial jurisdictions, new legislations will emerge, in a variety of online spaces, to deal with a wide range of new phenomena that have no clear parallel in the real world.

Accordingly, this article seeks to address and analyse the following issues: Firstly, it examines how cybercrime is being addressed at the national and international levels.
Secondly, it reviews the state of the existing legislative and regulatory framework and their efficiency in combating this form of cross-border organised crime, taking the European Union as a case study. Finally, the article will conclude by discussing the steps nations should take in their battle against this crime.

Table of Contents

Introduction:

Cybercrime is a major concern for the global community.[1] The introduction, growth, and utilisation of information and communication technologies have been accompanied by an increase in criminal activities.[2] With respect to cyberspace,[3] the Internet is increasingly used as a tool and medium by transnational organised crime.[4] Cybercrime is an obvious form of international crime that has been affected by the global revolution in ICTs.[5] As a resent study noted, cybercrimes differ from terrestrial crimes in four ways: "They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal." [6] On such a basis, the new forms of cybercrime present new challenges to lawmakers, law enforcement agencies, and international institutions.[7] This necessitates the existence of an effective supra-national as well as domestic mechanisms that monitor the utilisation of ICTs for criminal activities in cyberspace.[8]

---

[1] This concern is shared by many international organizations, including the United Nations, the G-8, the European Union and the Council of Europe.

[2] See D. PARKER, *Fighting Computer Crime: For Protecting Information* (U.S.A, John Wiley), [1998] p. 10.

[3] In fact, the dictionary defines cyberspace as 'the online world of computer networks.' *Merriam-Webster's Collegiate Dictionary* [1997]. For the purposes of this article, the term 'cyberspace' denotes the multifaceted global network of computerized information exchange made possible by ICTs.

[4] In fact, the involvement of organised crime groups in the field of computer fraud was illustrated when a Russian group attacked one of the best known US banks in New York via data networks in 1994. Operating from St. Petersburg, the group succeeded in causing the American bank to transfer over US$ 10 million to foreign accounts. Monitoring and following the "money trail" of the manipulations, some of the perpetrators finally could be arrested. The responsible security officer of the bank told the author that the arrested perpetrators possessed false Greek and Israeli passports which were forged in a quality which could be produced in Russia only by members of the former Russian secret service KGB. *See* M. LYMAN and G. POTTER, *Organized Crime* (New Jersey, Prenhall); U. SIEBER, *Legal Aspects of Computer Related Crime* (European Commission), [1998] p. 25.

[5] D. PARKER, *op. cit.*

[6] Mcconnell International, *Cybercrime...and Punishment? Archaic Laws Threaten Global Information* [Dec., 2000].

[7] Many of the legal challenges facing prosecutors in their pursuit of cybercriminals can be illustrated by the destructive career of the 'Love Bug Virus'. The virus which destroyed files and stole passwords. The virus which also affected NASA and the CIA and raced around the world in two hours, three times faster than its Melissa predecessor. As to the damage it inflected, estimates varied from $ 2 billion to $ 10 billion, since it is always difficult to assess estimate the harm inflicted by cybercrime. On these points see D. HOPPER, *Destructive ILOVEYOU Computer Virus Strikes WorldWide* , available at <http://archives.cnn.com/2000/TECH/computing/05/04/iloveyou/>(visited 25/03/2005), J. LEYDEN, *LoveBug Threatens Email Servers* [5 May 2000], <http://www.vnunet.com/news/1100661> (visited 25/03/2005), P. FESTA and J. WILCOX, *Experts Estimate Damages in the Billions for Bug* [5 May 2000], at: <http://news.com.com/2100-1001-240112.html?legacy=cnet> (visited 25/05/2005).

[8] In fact, the difficulty comes in defining the laws that need to be in place to allow the apprehension and prosecution of cybercriminals. While this might be a straightforward task, it actually raises some difficult issues. One is the scope of cyber-offences a country needs to define. Another is the extent to which these laws should be cybercrime specific. Thus, it is necessary for a country to add a 'computer fraud' offence if it has already outlawed fraud. On this point see M. D. GOODMAN and S. BRENNER, *The Emerging Consensus on Criminal*

I. The Rise of Crime in Cyberspace

The term "cyberspace" was coined by the science fiction author William Gibson in his 1984 novel *Nuromancer*, to describe the environment within which computer hackers operate.[9] In this novel, the activity of hacking- securing unauthorized access to the contents of computer systems- is couched in very physical terms. [10] The image is of the hacker overcoming physical security barriers to penetrate into the heart of computer systems and make changes to the physical structure thereby modifying the operation of the system.[11] When departing, the hacker might even remove and take away elements of the system. [12]

Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location.[13] The rise of the global computer network is destroying the link between geographical location and: (1) the *power* of local governments to assert control over online behaviour; (2) the *effects* of online behaviour on individuals or things; (3) the *legitimacy* of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give *notice* of which sets of rules apply.[14]

Faced with their inability to control the flow of electrons across physical borders,[15] some legislators strive to inject their boundaries into electronic mediums through filtering

Conduct in Cyberspace (Oxford, International Journal of Law and Information Technology), [200] Vol. 10, n. 2 p. 3.

[9] In fact, the term cyberspace literally means 'navigable space' and is derived from the Greek word *kyber* (to navigate). In William Gibson's 1984 novel, the original source of the term, cyberspace refers to, a navigable, digital space of networked computers accessible from computer consoles, a visual, colourful, electronic, Cartesian datascape known as 'The Matrix' where companies and individuals interact with, and trade in, information. Since the publication of this novel, the term cyberspace has been reappropriated, adapted and used in a variety of ways, by many different constituencies, all of which refer in some way to emerging computer-mediated communication and virtual reality technologies. Here, we refocus the definition back to the envisaged by Gibson, so that cyberspace refers to the *conceptual space* within ICTs, rather than the technology itself. *See* W. GIBSON, *Neuromancer* (New York, Grafton), [1984]; M. DODGE, *Mapping Cyberspace* (N.Y, Routeldge), [2001] p. 1.

[10] C. REED, *Computer Law* (U.K, John Angel), [2004] p. 242.

[11] *Id.*

[12] *Id*.

[13] However, the blurring of real and virtual extends beyond the imaginable. Analysts have recently started to argue that our geographic environments are becoming virtualised as computers are used increasingly to manage information concerning places. As such, city structure is becoming composed of and controlled by computers, and a recursive relationship is evolving so that as the city becomes composed of computers, the computer network is the city. Here, the virtual spaces of city data and management and the real spaces of buildings and streets become entwined. On this point see M. DODGE, *op. cit.* p. 22.

[14] D. JOHNSON and D. POST, *Law and Borders: The Rise of Law in Cyberspace* (Stanford, Stanford Law Review), [1996] n° 1378.

[15] On the conflict of laws in cyberspace see A. MEFFORD, *Lex Informatica: Foundations of the Law on the Internet* (IJGLS), [1997], 5(1) p.212.

mechanisms and the establishment of electronic barriers. [16] Others have been quick to assert the right to regulate all online trade insofar as it might adversely impact local citizens. For example The Attorney General of Minnesota, has asserted the right to regulate gambling that occurs on a foreign web page that was accessed and 'brought into' the state by a local resident. [17] Also, the New Jersey securities regulatory agency has similarly asserted the right to shut down any offending Web page accessible from within the state.[18]

On such a basis this section examines the distinct phenomenon of "cybercrime". Compare it with traditional crime and review the reports that have been conducted on its incidence and the damage it inflicts.

1.1 A Study of the Phenomenon

1.1.1 Understanding the Concept of Cybercrime

Generally speaking, computers play four roles in crimes: They serve as objects, subjects, tools, and symbols.[19] Computers are the objects of crime when they are sabotaged or stolen. There are numerous cases of computers being shot, blown up, burned, beaten with blunt instruments, kicked, crushed and contaminated.[20] The damage may be international, as in the case of an irate taxpayer who shot a computer four times through the window of the local tax office. [21] Or unintentional, as in the case of a couple who engaged in sexual intercourse while sitting on computer sabotage destroys information, or at least makes it unavailable.[22] Computers play the role of subjects when they are the environment in which technologies commit crimes. Computer virus attacks fall into this category. When automated crimes take place, computers will be the subjects of attacks. The third role of computers in crime is as tools-enabling criminals to produce false information or plan and control crimes.[23] Finally,

[16] *See* Karen Kaplan, *Germany Forces Online Service to Censor Internet*, L.A. Times, [Dec. 29, 1995] , at A1; *Why Free-Wheeling Internet Puts Teutonic Wall over Porn*, Christian Sci. Monitor, [Jan 4, 1996] , at 1; *Cyberporn Debate Goes International; Germany Pulls the Shade On CompuServe, Internet,* Wash. Post, [Jan. 1, 1996] , at F13 *in Id.*

[17] *See* The Minnesota Attorney General's Office distributed a Warning to All Internet Users and Providers, *available at* <http://www.state.mn.us/cbranch/ag/memo/txt> (visited 30/03/2005).

[18] *See* D. JOHNSON and D. POST, *op. cit.*

[19] *Id.* p. 16.

[20] In one such case in San Francisco, an electrical transformer in the basement of a building exploded, causing a poisonous liquid coolant to be released. The computers in the building continued to operate, but the fire department would not allow anybody to enter the building to tend to them, which rendered the information unavailable.

[21] *Id.*

[22] *Id.*

[23] In fact criminals may use computers, graphics software, and colour printers to forge documents. Criminals who create automated crime software and those who purchase and use the software will be using their computers as tools to commit crimes.

computers are also used as symbols to deceive victims. In a $ 50 million securities-investment fraud case in Florida, a stock broken deceived his victims by falsely claiming that he possessed a giant computer and secret software to engage in high-profit arbitrage. In reality, the man had only a desktop computer that he used to print false investment statements. He deceived new investors by paying false profits to early investors with money invested by the new ones. [24]

In the United States, police departments are establishing computer crimes units, and cybercrime makes up a large proportion of the offences investigated by these units. The National Cybercrime training Partnership (NCTP) encompasses local, state, and federal law enforcement agencies in the United States.[25] The International Association of Chiefs of Police (IACP) hosts an annual Law Enforcement Information Management training conference that focuses on IT security and cybercrime. [26] The European Union has created a body called the forum on Cybercrime, and a number of European states have signed the Council of Europe's Convention on Cybercrime treaty, which seeks to standardize European laws concerning cybercrime. From this perspective, each organization and the authors of each piece of legislation have their own ideas of what cybercrime is-and isn't. These definitions may vary a little or a lot. To effectively discuss cybercrime in this part, however, we need a working definition. Toward that end, we start with a board, general definition and then define specific one.

When speaking about cybercrime, we usually speak about two major categories of offences: In one, a computer connected to a network is the target of the offence; this is the case of attacks on network confidentiality, integrity and/ or availability.[27] The other category consists of traditional offences- such as theft, fraud, and forgery- which are committed with the assistance of/or by means of computers connected to a network, computer networks and related information and communications technology.[28] Cybercrime ranges from computer fraud, theft and forgery- to infringements of privacy, the propagation of harmful content, the

[24] *See* D. PAKER, *op. cit.* p. 16.
[25] <http://www.nctp.org>.
[26] <http://www.theiacp.org/>.
[27] The main goal of Internet security is to keep proprietary information confidential, to preserve its integrity, and to maintain its availability for those authorized to view that information. When information is accessed and examined by unauthorized individuals, it is no longer confidential. By connecting to the Internet organizations have made their information assets far more vulnerable to unauthorized access and breaches of confidentiality. If data are tampered with, modified, or corrupted by intruders there is a loss of information integrity. Some times this can happen inadvertently, but most often it is the intentional act of a hacker or a disgruntled employee seeking revenge. Finally, if information is deleted or becomes inaccessible to authorized users, there is a loss of availability. *See* R. SPINELLO, *Regulating Cyberspace: The Policies and Technologies of Control* (U.S.A, Spinello), [2002] p. 207.
[28] *See* M. D. GOODMAN and S. BRENNER, *op. cit.*

falsification of prostitution, and organized crime. [29] In many instances, specific pieces of legislation contain definitions of terms. However legislators don't always do a good job of defining terms. [30] Sometimes they don't define them at all, leaving it up to law enforcement agencies to guess, until the courts ultimately make a decision. [31] One of the biggest criticisms to the definition of computer crime conducted by the U.S Department of Justice (DOJ) is of its overly broad concept. The (DOJ) defines computer crime as 'any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution'. [32] Under this definition, virtually any crime could be classified as a computer crime, simply because a detective searched a computer data base as part of conducting an investigation.

One of the factors that make a hard-and-fast definition of cybercrime difficult is the jurisdictional dilemma.[33] Laws in different jurisdictions define terms differently, and it is important for law enforcement officers who investigate crimes, as well as network administrators who want to become involved in prosecuting cybercrime that are committed against networks, to become familiar with the applicable laws. [34]

Also, one of the major problems with adequately defining cybercrime is the lack of concrete statistical data on these offences. In fact, reporting crimes is voluntary.[35] This means that the figures are almost certainly much lower than the actual occurrence of networked-related crime. [36]

In many cases, crimes that legislators would call cybercrimes are just the 'same old stuff', except that a computer network is somehow involved. The computer network gives criminals a new way to commit the same old crimes.[37] Existing statutes that prohibit these

---

[29] *Id.*
[30] D. SHINDER, *Scene of the Cybercrime* (U.S.A, Syngress), [2002] p. 6.
[31] *Id.*
[32] <http://www.findarticles.com/p/articles/mi_m2194/is_8_70/ai_78413303> (visited 29/03/2005).
[33] D. SHINDER, *op. cit.* p. 6.
[34] *Id.*
[35] Daved GARLAND argues that ' today's world of crime control and criminal justice was not brought into being by rising crime rates or by a loss of faith in penal-welfarism, or at least not by these alone. These were proximate causes rather than the fundamental processes at work. It was created instead by a series of adaptive responses to the cultural and criminological conditions of late modernity- conditions which included new problems of crime and insecurity, and new attitudes towards the welfare State. But these responses did not occur outside of the political process, or in a political and cultural vacuum. On the contrary. They were deeply marked by the cultural formation that he describes as ' crime complex' ; by the reactionary politics that have dominated Britain and America during the last twenty years; and by the new social relations that have grown up around the changing structures of work, welfare and market exchange in these two late modern societies. On this point see D. GARLAND, *The Culture of Control: Crime and Social Order in Contemporary Society* (David Garland, University of Chicago), [2001].
[36] D. SHINDER, *op. cit.* p. 6.
[37] For example, the Internet is a non-secure network with more than one hundred million users around the world. One of the Internet's greatest strengths-its open anonymous nature-is also its greatest weakness, making it ripe

acts can be applied to people who use a computer to commit them as well as to those who commit them without the use of a computer or network.[38]

In other cases, the crime is unique and came into existence with the advent of the network. Hacking into computer systems is an example; while it might be linked to breaking and entering a home or business building, the elements that comprise unauthorized computer access and physical breaking and entering are different.

Most U.S states have pertaining to computer crime. These statutes are generally enforced by state and local police and might contain their own definitions of terms. Texas Penal Code's Computer Crime section, defines only one offence - Breach of Computer Security- as '(a) A person commits an offence if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner'.[39]

California Penal Code, on the other hand, defines a list of eight acts that constitute computer crime, including altering, damaging, deleting, or otherwise using computer data to execute a scheme to defraud, deceiving, extorting, or wrongfully controlling or obtaining money, property, or data using computer services without permission, disrupting computer services, assisting another in unlawfully accessing a computer, or introducing contaminates into a system or network. [40] Thus, the definition of cybercrime under state law differs, depending on the state. Perhaps we should look to international organizations to provide a standard definition of cybercrime.

At the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders, in a workshop devoted to the issues of crimes related to computer networks, cybercrime was broken into two categories and defined thus: [41]

'(a) Cybercrime in a narrow sense: Any illegal behaviour directed by means of electronic operations that targets the security of computers systems and the data processed by them.

(b) Cybercrime in a border sense: Any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or disturbing information by means of a computer system or network'.

---

for abuse and attracting attention from an array of unsavoury individuals and advocacy groups including terrorists, neo-Nazis, pornographers, and paedophiles. Fraudsters of every stripe engage in securities boiler room operations, illegal gambling, Ponzi pyramid schemes, credit card fraud, and a variety of other illicit activities. On this point see D. PARKER, *op. cit.* p. 114.

[38] *Id.*

[39] *See* Texas Penal Code, available at: <http://www.capitol.state.tx.us/statutes/docs/PE/content/word/pe.007.00.000033.00.doc > (visited 29/03/2005).

[40] Section 502.

[41] *See* Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders, Vienna, and April 2000. Available at <http://www.uncjin.org/Documents/congr10/4r3e.pdf> (visited 29/03/2005).

These definitions, although not completely definitive, do give us a good starting point-on that has some international recognition and agreement – for determining just what we mean by term *cybercrime*. Cybercrime, by these definitions, involves computers and networks. In cybercrime, the "cyber" component usually refers to perpetrating qualitatively new offences enabled by information technology or integrating cyberspace into more traditional activities.[42] Having defined the concept of cybercrime, it becomes necessary to compare it with traditional crime. This involves examination of its characteristics, what makes it vulnerable to being manipulates and reviews the reports that have been conducted on its incidence and the damage it inflicts.

1.1.2 Terrestrial Crime versus Cybercrime

The act of defining crime is often, but not always, a step toward controlling it. That is, the ostensible purpose of defining illegal behaviours as criminals is to make them liable to public prosecution and punishment.[43] Historically, 'crime' was addressed at the local, community level of government. [44] Crime was a small-scale, consisting of illegal acts committed by some persons that were directed against one victim. The 'crimes', which were consistent across societies; fell into routinized, clearly-defined categories that reflected the basic categories of anti-social motivations: Crime was a murder, it was robbery, crime was rape. [45]

Crime was also personal, if the victim and the offender did not know each other; they were likely to share community ties that put offences into a manageable, knowable context.[46] This principle did not only facilitate the process of apprehending offenders – who stood a good chance of being identified by the victim or by reputation – but also gave citizens at least the illusion of security, the conceit that they could avoid being victimized if they avoided some activities or certain associations.[47] Law enforcement officers, dealt with this type of crime because its parochial character meant investigations were limited in scope and because the incidence of crime stood in relatively modest proportion the size of the local populace. Lax enforcement's effectiveness in this regard contributed to a popular perception that social order was being maintained and that crime did not go unpunished. [48]

[42] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 145.
[43] *See* R. CRUTCHFIELD, *Crime: Readings* (California, Pine Forge Press), [2000], p. 7.
[44] *See* P. HITCHENS, *A Brief History of Crime* (Atlantic, London), [2003].
[45] *See* for example W. BALCKSTONE, *Commentaries on the Laws of England* (Chicago, The University of Chicago), [1979].
[46] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 151.
[47] *Id.*
[48] *Id.*

The development in ICTs in urbanization and in geographical mobility under minded this model to some extent. However, it persisted functioned effectively for the most part. Legislators quickly adapted to the fact that ICTs could be used to commit fraud and to harass others. Because, they modified their substantive criminal law to encompass these activities, the old model still functions effectively for traditional real world crime.

Unlike this traditional crime, cybercrime is global crime. [49] As a European Report explains:

'*[c]omputer-related crimes are committed across cyber space and don't stop at the conventional state-borders. They can be perpetrated from anywhere and against any computer user in the world*.'

Some cybercrimes- stalking, say-tend, so far, at least, to be small-scale, single-offender/ single victim crimes, but the world's experience with cybercrime is still in its infancy and yet large-scale offences targeting multiple, geographically dispersed victims are already being committed.[50]

In order to understand the sea change ICTs introduces into criminal activity, it is important to consider a hypothetical: One can analogize a denial of service attack to using the telephone to shut down a supermarket business, by calling the business' telephone number repeatedly, persistently without remorse. Thereby preventing any other callers from getting through to place their orders. On such a base, the vector of cyberspace lets someone carry out an attack such as this easily and with very little risk of apprehension, so easy, in fact, that a 13 year-old hacker used a denial of service attack to shut down a computer company. [51] In addition to the increased scale of criminal activity the cybercrime offers, it also has a tendency to evade traditional offence categories. While some of its categories consists of using ICTs to commit traditional crimes, it also manifests itself as new varieties of activity that cannot be prosecuted using traditional offence categories. [52]

The dissemination of the "Love Bug" virus illustrates this. Virus experts quickly traced this virus to the Philippines. Using Information supplied by an Internet service provider, agents from the Philippines' National Bureau of Investigation and from the FBI identified individuals suspected of creating and disseminating the 'Love Bug'.[53] However, they ran into

[49] *See* e.g LoveBug.

[50] A notorious example of this is in the February, 2000 denial of service attacks that targeted eBay, Yahoo and CNN, among others, that effectively shut down their web sites for hours and were estimated to have caused $ 1.2 billion in damage. *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p.

[51] *See* S. GIBSON, *The Strange Tale of the Denial of Service*, available at <http://grc.com/dos/grcdos.htm> (visited 29/03/2005).

[52] *See* C. BICKNELL, *Sex.Com : It Wasn't Stolen* [25/08/2000], available at : <http://www.mediaesq.com/new31857.php> (visited 29/03/2005).

[53] *See* D. SCHWEITZER, *op. cit.*

problems with their investigation: The Philippines had no ICTs laws, so creating and disseminating a virus was not a crime.[54] Therefore, the law enforcement officers had no hard time convincing a magistrate to issue a warrant to search the suspects' apartment.[55] Later on the suspected author of the virus could not be prosecuted under the repertoire of offences defined by the Philippines criminal code. [56]

On such a basis cybercrime's ability to morph into new and different forms of antisocial activity that evade the reach of existing penal law creates challenges for legislations around the world. [57] Criminals[58] have the ability of exploiting gaps in their won country's penal law in order to victimize their fellow citizens with impunity. [59] Also, cybercriminals can exploit gaps in penal laws of other countries in order to victimize the citizens of those, and other, nations; as the 'Love Bug' episode demonstrated, cybercrime is global crime.[60]

1.2 The Scope of the Phenomenon

Knowing how much crime is committed might help us decide on how much to spend on security. Estimates by security experts of annual losses from computer crime range from $ 555 million to more than $ 13 billion,[61] but there are actually no valid statistics on the losses from this type of crime, because no one knows how many cases go unreported.[62] Even when the victims of computer crimes are aware of the crimes, they are usually relocated to report their losses- especially if those losses can be easily hidden.[63] Victims can lose more from reporting crimes than they lose from the crimes themselves. Embarrassment, key staff diverted to prepare evidence and testify, legal fees, increased insurance premiums, and exposure of vulnerabilities and security failures can all result from reporting computer crime incidents. [64]

---

[54] J. LEYDEN, *Love Bug Suspect Released* (vnunet.com), [May 2000], available at: <http://www.vnunet.com/news/1101024> (visited 29/03/2005).
[55] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 153.
[56] *Id.*
[57] *Id.*
[58] Studies of cybercriminals reveals seven significant profiles. Unfortunately, however, no criminal fits exclusively in any one profile. Instead, the profiles overlap one another in fuzzy relationships. (A) Pranksters; (b) Hackers; (c) Malicious hackers; (d) Personal problem solvers; (e) career criminals; (f) extreme advocates; (g) malcontents, addicts, and irrational and incompetent people.
[59] *See 1999 Report on Cybertalking* (US Department of Justice), [1999] available at: <http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm> (visited 29/03/2005).
[60] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 154.
[61] D. PARKER, *op. cit.* p. 10.
[62] *See* Mcconnell International E-Lert, *Combating Cybercrime : A Proactive Approach* [Feb. 2001], available at: <http://www.mcconnellinternational.com/pressroom/elert.cfm> (visited 29/03/2005).
[63] *See* UNESCO, *Les Dimensions Internationales du Droit du Cyberespace* (Paris, Economica), [2000].
[64] D. PARKER, *op. cit.* p. 10.

However, the results of national surveys bear out the picture that cybercrime is consistently and dramatically on the increase.[65] One of the famous cited national surveys for the United States is the 'Computer Crime and Security Survey' conducted by the Computer Security Institute [66] with the participation of the San Francisco branch of the Federal Bureau of Investigation's Computer Intrusion Squad. [67] The CSI/FBI survey which has been conducted in 2004 – reports the results questionnaire administrated to 494 computer security practitioners in U.S corporations government agencies, financial institutions, medical institutions and universities. One area the survey explores is security breaches; the questionnaire asks the respondents if they have experienced breaches of information security in the last year. [68] The percentage of the respondents answering that their organization experienced unauthorized use of computer systems in the last 12 month declined to 53 percent, the smallest percentage since this question first appeared in the survey in 1999. Moreover, the percentage of respondents answering that there was no unauthorized use of their organization's computer systems increased to 35 percent as the respondents not knowing if such unauthorized use occurred dropped to a low of 11 percent.

The year 2004 showed the lowest percentage (12 percent) of respondents estimating that organization experienced more than ten computer security incidents during the past year. The survey provides a visual demonstration that attacks of computer systems or misuse of these systems has been slowly, but fairly steadily decreasing over many years in nearly all categories. In fact, there has been a dramatic drop in reports of system penetrations, insider abuse and theft of proprietary information.

Data from other countries reveal similar trends. According to a November 2000 report from the United Kingdom:[69]

'Cybercrime accounted for half of all fraud committed in the UK in the first six months of this year, according to a legal expert. Steven Philippsohn, senior litigation partner at law firm Philippsohn, Crawfords, Berwald, said

[65] In fact, some surveys don't focus on the incidence of cybercrime, but on the extent to which the public is concerned about cybercrime. May be on the theory that public opinion is an important driver of national policy. In a February 2001 survey of Americans, two contradictory views emerged: The first is that many Americans do not trust their government and its agencies very much. Yet the second strong strain of opinion is that Americans are quite willing to grant to law enforcement agencies and the FBI the right to intercept the email of criminal suspects, perhaps because Americans are concerned about crime, especially new ways to perpetrate crime using the Internet. While a majority of Americans approve of email interception to fight crime, only 21% of all Americans have heard about Carnivore, the FBI's digital surveillance tool. On this point see Pew Internet and American Life Project, available at <http://www.pewinternet.org/pdfs/PIP_Fear_of_crime.pdf>(visited 29/03/2005).

[66] <http://www.gocsi.com/>. (visited 29/03/2005).

[67] <http://www.emergency.com/fbi-nccs.htm>. (visited 29/03/2005).

[68] <http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf> (visited 29/03/2005).

[69] *See Cybercrime Soars in the UK*, available at <http://www.vnunet.com/news/1113497> (visited 29/03/2005).

this figure would rise as it becomes easier for criminals to break online security. Speaking at the Compsec computer security conference in London last week, he said: The internet is a criminal's charter. There is an increasing number of targets and despite what people say, buying online is not the same as giving your credit card to someone in a restaurant. In that scenario, maybe 10 people will see your credit card details. The minute you put those details on to a website and that site is hacked, the information can be accessed by millions if not billions around the world. Philippsohn said it is cheap for fraudsters to set up an online scam. They don't need premises, and they can set up a website claiming anything they like and give a very good impression of what can be an absolute scam. He said there has been a 56 per cent increase in hacking in the UK over the past 12 months, with most hackers seeking financial gain, for example by using their hack to demand money, or for political reasons such as posting messages for a certain cause on a company's website'.

In Japan and china, studies showed high increases in cybercrime.[70] From its part, the Australian version of the CSI/FBI survey 2004 found that: 'more respondants organizations experienced electronic attacks that harmed the confidentiality integrity or availability of network data or systems (49% in 2004 compared to 42% in 2003)'.[71] It also remarked that: 'Most of these attacks were again sourced externally (88%) compared to internally (only 36%) , but fewer respondents experienced external attacks compared to 2003 (91%)' . [72] The survey showed that: 'Infections from viruses, worms or Trojans were the most common form of electronic attack reported by respondants for the third consecutive year. They were the greatest cause of financial losses and accounted for 45% of total losses for 2004. [73] In fact, the value of these surveys is perhaps more anecdotal than scientific.[74] As almost everyone concedes, it is difficult to gather accurate cybercrime statistics. [75] On such a basis PARKER states: "*In reality, we have no valid statistics on cybercrime frequency or size of loss. Even if there were valid statistics on cybercrime, beyond helping with actuarial insurance rate structures and legislation, they would be of little use to a particular organization for its own risk assement. Each organization's circumstances differ significantly from the average incident represented in the statistics. Unfortunately, the limited surveys that are conducted on cybercrime are often conducted by individuals who are unfamiliar with cybercrime. Each survey respondent has a different definition of cybercrime and may be unaware of what*

[70] *See* M. KABAY, *Studies and Surveys of Computer Crime* (Norwich), [20001], available at: <http://www.securitystats.com/reports/Studies_and_Surveys_of_Computer_Crime.pdf#search='studies%20and%20surveys%20of%20computer%20crime'> (visited 30/03/2005).
[71] *See* Deloitte and Victoria Police Computer Crime Survey [2004], p. 3.
[72] *Id.*
[73] In 1999, the Australian survey found that the attacks perpetuated appear to be random, 'spur of the moment' attacks, with no discernible pattern detected in more than 70% of the cases. According to respondents, the most likely motivation for an attack was curiosity (71%). The attacker was most likely to be a disgruntled employee or an independent hacker. On this point see M. D. GOODMAN and S. BRENNER, *op. cit.* p. 156.
[74] *Id.*
[75] *Id.*

actually happened, how it happened, or what the actual losses were. In addition, many victims do everything they can to avoid revealing their actual losses.[76]

Confirming this, KABAY states that's 'a commonly-held view within the information security community is that only one-tenth or so of all the crimes committed against and using computer systems are detected'. [77] He also declares that:

> [E]ven if attacks are detected, it seems that few are reported in a way that allows systematic data collection. This belief is based in part on the unquantified experience of information security professionals who have conducted interviews of their clients; it turns out that only about ten percent of the attacks against computer systems revealed in such interviews were ever reported to any kind of authority or to the public. The Department of Defence studies mentioned above were consistent with this belief; of the few penetrations detected, only a fraction of one percent were reported to appropriate authorities.[78]

Most experts believe that common forms of computer related crime are significantly underreported because 'victims may not realize that they have been victimized, may not realize that the conduct involved in a crime, or may decide not to complain for reasons of embarrassment or corporate credibility'.[79] Other reasons for the under-reporting of cybercrime are that 'Further problems arise with the mass victimization caused by offences such as virus propagation, because the number of victims are simply too large to identify and count, and because such programs can continue creating new victims long after the offenders have been caught and punished'. [80] Finally, a factor complicating the gathering and comparison of national crime statistics will be the fact that transnational computer related crimes are, by definition committed in or have effects in at least two States risking multiple reporting or no reporting at all. [81] Thus, much of the information we have on cybercrimes is the product of studies and surveys addressed to individuals working in information security. [82] On such a basis the obvious problem that survey results include only the respondents of people who agreed to participate.[83] Before basing critical decisions on survey information, it is important to find out what the response rate was; although there are no absolutes, in general we aim to trust survey results more when the response rate is high.[84] However, response rates for telephone surveys are often less than 10%; response rates for mail and e-mail surveys can be

[76] *See* D. PARKER, *op. cit.* p. 74.
[77] *See* M. KABAY, *op. cit.*
[78] *Id.*
[79] *See* U.N Commission on Crime Prevention and Criminal Justice, 10 th session, Item 4 at 10, *Conclusion of the Study on Effective Measures to Prevent and Control High-Technology and Computer Related Crime* [2001] p. 10. Available at: <http://www.unodc.org/pdf/crime/10_commission/4e.pdf> (visited 30/03/2005).
[80] *Id.*
[81] *Id.*
[82] *See CSI/FBI 2004Computer Crime and Security Survey, op. cit.*
[83] *See* M. KABAY, *op. cit.*
[84] *Id.*

less than 1%.[85] It is not easy to make any case for random sampling under such circumstances, and all results from such low-response-rate surveys should be viewed as indicating the range of problems or experiences of the respondents rather than as indicators of population statistics. [86]

As to the problems noted above, a research firm estimated in 2001 that 'Cybercrime today is focused on corporate espionage and financial gain. There are no guns or violence and the perpetrator is nowhere near the scene: in fact, most of the time they aren't even in the same country! Gartner Group is already predicting that the financial damage caused by cybercrime will increase by between 1000 and 10,000 per cent by 2004'.[87] Also, at a Berlin conference of 100 Internet experts from the G8 group of industrialized nations in October 2000, J. FISCHER German Foreign Minister declared that cybercrime losses have reached 100 billion German marks for the eight major countries including the U.S. [88]

As to the effects of cybercrime, it is, at the very least, safe to agree with the position the European Commission took in launching a cybercrime initiative: [89] While conceding that ' there is a little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society'. [90] The Commission states 'it is necessary that substantive law in the area of high tech crime is approximated'. [91] European leaders called during the special EU-summit in Tampere (1999) for common definitions, incriminations and sanctions in the area of high tech crime'.

1.3 Cyberspace Misuse and Abuse

As the surveys above had demonstrated, cybercrimes are complex and sometimes elusive phenomena; there is no comprehensive, globally accepted definition that separates the sensational from the sensible and scientific. Thus, the following scenarios – all of which are quit real and take place frequently illustrate the range of activities that can be considered cybercrimes:

[85] *Id.*
[86] *Id.*
[87] *See* A. MILES, *Bug Watch: The Fight Against Cybercrime* [20 April 2001]. Available at: <http://www.pcw.co.uk/print/it/1120814> (visited 31/03/2005).
[88] For a full study, see F. CILLUFFO and al., *Cyber Threats and Information Security* (CSIS), [May 2001].
[89] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 160.
[90] *See* J. BURREN, *European Commission Wants to Tackle Cyberime* [10/01/2001]. Available at: <http://www.heise.de/tp/r4/artikel/4/4658/1.html>(visited 31/03/2005).
[91] *Id.*

1.3.1 Hacking and Related Activities

To some extent, the definition of hacking depends on what we ask.[92] Generally speaking, a 'hack' used to be a clever solution to a restriction.[93] A hack was an ingenious, but temporary, fix or 'make-do' rather than an attack on a computer system. [94] However, in 1960s malicious hacking started with compromising telephone systems and stealing telephone services.[95] It soon spread to computers and networks. When we extend this term to the individuals who practice the art of hacking, however, the definitions become murkier. The Oxford English Dictionary (1998) defines hacker as "a person who or thing that hacks or cuts roughly" or "a person whose uses computers for a hobby, esp. to gain unauthorized access to data".

In his book *The Hacker Crackdown* Brice STERLING takes a rather positive view of the activity, explaining that the term *hack* 'can signify the free-wheeling intellectual exploration of the highest and deepest potential of computer systems.[96] 'Hacking can involve the heartfelt conviction that beauty be found in computers, that the fine aesthetic in a perfect program can liberate the mind and spirit'. [97] This is hacking as it was defined in Steven LEVY's much praised history of the pioneer computer milieu, *Hackers* published in 1994.

Hacking or gaining unauthorized access to computer system, programs, or data, open a broad playing filed for inflicting damage. [98] The *New Hackers Dictionary* [99] offers six definitions for hacking and hacker:

(a) A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to many users, who prefer to learn only the minimum necessary; (b) A person who enjoys the intellectual challenge of overcoming or circumventing limitations; (c) A person good at programming quickly; (d) An expert in a particular

[92] Recent studies of actual hacker crimes reveal that there are many misconceptions about hackers? In one instance, members of the U.S military, testifying before the U.S Armed Services Committee in Congress in 1994, described a 'master spy' that posted a major threat to U.S security. The military chiefs feared that an East European spy ring had successfully hacked into American Ai Defence systems and learned some of its most well-guarded intelligence secrets. A 13-month investigation however, revealed that a 16-year-old British music student was responsible for the break-ins. The culprit, known as the Datastream Cowboy, had downloaded dozens of military files, including details of ballistic missile research and development, and had used a company's network in California for more than 200 logged security breaches-all using a $ 1,200 computer and modem. He was tried and convicted in 1997, and fined $ 1,915 by a London court. After his conviction, the media offered the musical hacker considerable sums for the book and film rights to his story, but he declined, preferring to continue his musical studies and concentrate on wining a place in a leading London orchestra. On these points see D. PAKER, *op. cit.* p. 164.

[93] *See* D. PAKER, *op. cit.* p. 158.

[94] *Id.*

[95] On the history of hacking see J. CHIRILLO, *Hack Attacks Encyclopaedia: A Complete History of Hacks, Cracks, Phreaks and Spies* (Canada, John Wiley), [2001] p. 1.

[96] *See* B. STERLING, *The Hacker Crackdown* (Batman Books) pp. 50 -51.

[97] *Id.*

[98] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 146.

[99] *See* E. RAYMOND, *The New Hackers Dictionary* (U.S.A, MIT Press).

language; (e) A person who programs enthusiastically; (f) A malicious meddler who tries to discover sensitive information by poking around.[100] On such a base hacking can manifest itself in many ugly forms including "cyber murders". A British hacker hacked into a Liverpool hospital in 1994 and changed the medical prescriptions for the patients.[101] A nine-year-old patient who was 'prescribed' a highly toxic mixture survived only because a nurse decided to re-check his prescription.[102] The hacker's motive - he wanted to know 'what kind of chaos could be caused by penetrating the hospital computer'! Others have not been so lucky. An underworld don who was only injured in a shoot out was killed by an overdose of penicillin after a hacker broke into the hospital computers and altered his prescription.[103]

Hacking is facilitated by many technologies, the major ones being packet sniffing,[104] tempest attack, [105] password cracking, [106] and buffer overflow. [107] Due to recent developments

[100] Some information has distinct monetary value. This is a unique kind of information that requires great security. Indeed, the threats to monetary information encompass the full spectrum of crime: Fraud, larceny, extortion, sabotage, forgery, and espionage focus on it. In the cyberspace, for example, we encounter real, negotiable money in bank account balances or as *e-cash* or *cybercash*. Each amount of money consists of optionally the name of a country and its currency symbol, numeric characters, and a decimal point. An ordered set of these symbols and characters represents an amount of monetary credit in an account. When you spend some of this money electronically, the balance in the computer account or smart card is debited by the appropriate amount, and the balance in the merchant's account in another computer is credited with that amount. Owners may require different degrees of security for monetary information, depending on differences in its values, representations, and media. Thus, we need to consider the information's value to various individuals to identify where and how to apply security. The choices of security controls may depend on the means of converting from one representation or medium to another. *See* D. PARKER, *op. cit.* p.40.

[101] A. NAGPAL, *Cyberterrorism in the Context of Globalisation* (India, UGC sponsored National Seminar on Globalization and Human Rights), [September 2001].

[102] *Id.*

[103] *Id.*

[104] In fact, when information is sent over computer networks, it gets converted into hex and broken into lots of packets. Each packet is identified by a header, which contains the source, destination, size of packet, total number of packets, serial number of that packet, etc. If a hacker wants to see this information, he uses Packet Sniffing technology that reconverts the data from hex to the original. This technology is like putting the equivalent of a phone tap on a computer. Sniffing can be committed when a packet leaves the source or just before it reaches the destination. For this, the hacker would need to know only the IP Address (the unique number that identifies each computer on a network). A packet sniffer can log all the files coming from a computer. It can also be programmed to give only a certain type of information - e.g. only passwords. On this point see *Id.*

[105] TEMPEST (Transient Electromagnetic Pulse Emanation Standard) technology allows someone not in the vicinity to capture the electromagnetic emissions from a computer and thus view whatever is on the monitor. A properly equipped car can park near the target area and pick up everything shown on the screen. There are some fonts that remove the high-frequency emissions, and thus severely reduce the ability to view the text on the screen from a remote location. This attack can be avoided by shielding computer equipment and cabling. *See Id.*

[106] A password is a type of secret authentication word or phrase used to gain access. Passwords have been used since Roman times. Internal to the computer, passwords have to be checked constantly. So, all computers try to "cache" passwords in memory so that each time a password is needed the user does not need to be asked. If someone hacks into the memory of a computer, he can sift the memory or page files for passwords. Password crackers are utilities that try to 'guess' passwords. One way, the dictionary attack, involves trying out all the words contained in a predefined dictionary of words. Ready-made dictionaries of millions of commonly used passwords can be freely downloaded from the Internet. Another form of password cracking attack is 'brute force' attack. In this attack, all possible combinations of letters, numbers and symbols are tried out one by one till the password is found out. *See Id.*

in the field of telephone and telecommunications technology (such as ISDN), hacking does not only affect classic computer systems but also increasingly telephone lines, *answerphones* and voice-mail-systems.[108] "Telephone hackers" dial themselves into the telephone company's local phone exchanges and are thus able to eavesdrop on the digitally led conversations in a respective part of town. In the US, besides other confidential information, especially the numbers of telephone access cards (so-called calling cards) are eavesdropped on, which are then resold.[109]

1.3.2 Viruses and Malicious Codes

As we mentioned before, computers are the subjects of crime in computer virus distribution, Trojan horse attacks, logic bombs use, and *data diddling* – the term used by Donn Parker to refer to the act of putting false data into computers.[110] Malicious code is any software program designed to move from computer to computer and network to network, in order to intentionally modify computer systems without the consent of the owner or operator. [111] It includes viruses, Trojan horses, worms, script attacks and rogue Internet code.[112] Computer viruses have been around for almost as long as computers. [113] The term *computer virus* was formally defined by Fred COHEN 1984, while he was performing academic experiments on a Digital Equipment Corporation VAX computer system.[114] Fred Cohen is the best known as the inventor of computer viruses and virus defence techniques. [115]

Actually, a computer virus is a specific type of malicious code that replicates itself and inserts copies or new versions of itself in other programmes, when it is executed with the infected program. [116] It replaces an instruction in the target program with an instruction to transfer control to the virus which is stored in the memory.[117] Whenever the program transfer

---

[107] Also known as buffer overrun, input overflow and unchecked buffer overflow, this is probably the simplest way of hacking a computer. It involves input of excessive data into a computer. The excess data "overflows" into other areas of the computer's memory. This allows the hacker to insert executable code along with the input, thus enabling the hacker to break into the computer. *See Id.*

[108] *See* U. SIEBER, *op. cit.* p. 43.

[109] *Id.*

[110] *See* D. PAKER, *op. cit.* p. 82.

[111] *See* R. GRIMES, *Malicious Mobile Code, Virus Protection for Windows* (O'Reilly), [August 2001] p. 2.

[112] *Id.*

[113] *See* D. SCHWEITZER, *op. cit.* p. 44.

[114] On this point see experiments with computer virus. Available at <http://all.net/books/virus/part5.html> (visited 25/03/2005).

[115] *See* D. SCHWEITZER, *op. cit.* p. 44.

[116] *See* E. SKOUDIS, *Malware, Fighting Malicious Code* (Prentice), [2003] p. 25.

[117] Although viruses cannot be activated in data files because these files are not executed as programs, viruses can be activated through execution of imbedded or attached macro programs that accompany data file documents. When a user executes a word processor program (e.g Microsoft Word) to open a file for viewing, the embedded to attached macro programs are automatically executed to format the data contents. Macros can be

instruction is executed, it dutifully transfers control to the virus program, which then executes the replaced instructions and performs its work of inserting itself in other programs. [118] There are presently more than 10, 000 identified viruses affect the PC and Apple operating systems. In addition, a few viruses affect other operating systems such as UNIX. There are, however, no known viruses that attack the large-scale mainframe computer operating systems.[119] There are, however, no known viruses that attack the large-scale mainframe computer operating systems. This probably because the virus makers have easy access to the desk top and laptop computing environments, and because of the proliferation and casual exchange of software for these environments. [120]

On such a basis, a calamitous virus may delete files or permanently damage systems. A Trojan horse masquerading as a utility or animation may copy users IDs and passwords, erase files, or release viruses.[121] The program may also be used for blackmail, with activation of a virus or detonation of a digital bomb threatened unless demands are met.[122] A virus might cause a minor annoyance, or tremendous losses in money and productivity, or human lives, if it changes or destroys such crucial data as medical records at a hospital. [123] In some cases, the original software which was issued by the producing company was already infected with a virus. While viruses only spread in "host programs", worm programs attack other computer systems independently.[124] An illustrative example for the possible dangers is the American "Internet worm"-case. In this case a young computer scientist created an extremely complex virus which consisted of several programs. The virus was injected into a Department of Defence research computer system. Due to a design error it replicated wildly in a similar manner as a worm, ultimately jamming more than 6,000 computers. Although the virus caused no actual damage to any files, it cost many thousands of employee hours to locate and erase this virus. [125] The most famous viruses over years are Melissa,[126] ExploreZip, [127]

infected with *macro viruses* that also execute when the user opens a file. This type of virus (most notably, *Microsoft Word Concept*) is becoming increasingly common. The bizarre *Maddog* virus, for example, changes the letter *a* to *e* throughout infected documents tat happen to be in use at 8 PM on any day. *See* D. PARKER, *op. cit.* p. 84.

[118] *Id* p. 83.

[119] *Id.*

[120] *Id.*

[121] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 146.

[122] *Id.*

[123] *Id.*

[124] *See* U. SIEBER, *Legal Aspects of Computer Related Crime*, *op. cit* p. 49.

[125] *Id.*

[126] This virus, when it was first noticed on 26th March 1999 was the fastest spreading virus the world over. The virus by itself was quite harmless. It merely inserted some text into a document at a specified time of the day. What caused the maximum harm was that the virus would send itself to all the email addresses in the victim's address book. This generated enormous volume of traffic making servers all over the world crash.

Chernobyl, [128] I Love You virus, Pakistani Brain, Stoned-Marijuana, [129] Cascade, [130] and Michelangelo. [131]

1.3.3 Online Fraud

All stages of computer operations are susceptible to criminal activity, either as the target of the fraud, the instrument of the fraud, or both.[132] Input operations, data processing, output operations and communications have all been utilized for illicit purposes.[133] The more common types of computer fraud are: [134]

(A)Fraud by Computer Manipulation

Intangible assets that are represented in data format, such as money-on-deposit, or hours of work, are the most common targets of computer related fraud. Modern business is replacing cash with deposits transacted on computer systems, creating an enamours potential for computer fraud. The organized criminal community has targeted credit card information, as well as personal and financial information about clients. The sale of this information to counterfeiters of credit cards and travel documents has proven to be extremely lucrative.[135]

---

[127] In its activities it was similar to Melissa, but there was one major difference. ExploreZip, first discovered in June 1999, was not a virus but a Trojan. This means that it was incapable of replicating itself. Thus, the Melissa virus had more far reaching presence. Also, ExploreZip was more active. It not only hijacked Microsoft Outlook but also selected certain files and made their file size zero - reduced their data to nothing. Those files were then of no use to the user and they could not be recovered.

[128] The Chernobyl, or PE CIH, virus activates every year on the 26th of April - on the anniversary of the Chernobyl, Ukraine, nuclear power plant tragedy. The virus wipes out the first megabyte of data from the hard disk of a personal computer thus making the rest of the files of no use. Also, it also deletes the data on the computer's Basic Input-Output System (BIOS) chip so that the computer cannot function till a new chip is fitted or the data on the old one is restored. Fortunately only those BIOSes, which can be changed or updated, face a threat from this virus.

[129] This virus was originally written in New Zealand and would regularly display a message, which said, 'Your PC is stoned. Legalize Marijuana'.

[130] This virus is also called 'Falling Letters' or '1701'. It initially appeared as a Trojan horse in the form of a program designed to turn off the Num-Lock light on the user's keyboard. In fact, what it did was to make the characters on the screen drop in a heap to the bottom of the screen.

[131] This virus is titled after famous Italian Renaissance artist Michelangelo Buonarroti. It gets activated every year on the artist's birthday - 6th March.

[132] It is difficult to determine when the first crime involving a computer actually occurred. The computer has been around in some from since the abacus. It is known to have existed in 3500 B.C. In 1801 profit motives encouraged Joseph Jacquard, a textile manufacturer in France, to design the forerunner of the computer card. This device allowed the repetition of a series of steps in the weaving of special fabrics. So concerned where Jacquard's employees with the threat to their traditional employment and livelihood that acts of sabotage were committed to discourage M. Jacquard from further use of new technology. A computer crime had been committed. On this point see J. WELLS, *The Computer and Internet Fraud Manual* (Austin, Texas), [2002] p. 3.

[133] Investigations show that online auction complaints represent the largest category for internet fraud statistics. On this point see <http://www.fraud.org/internet/lt00totstats.htm> (visited 26/03/2005). At the same time it is argued that the amount of internet fraud is tiny compared with the number of transactions which take place. *See* M. BICHLER, *The Future of E-Markets: Multidimensional Mechanisms* (CUP), [2000] p. 131.

[134] *Id* p. 8.

[135] *Id.*

On such a base, improved remote access to databases allows the cybercriminals to commit several types of fraud such as: (a) Input manipulation; (b) Program manipulation; (c) Output manipulation. [136]

(B) Computer Forgery and Desktop Counterfeiting

When a criminal alters data stored in a computer system, the crime committed may be forgery.[137] In this case computer systems are the target of criminal activity. However, computers can also be used as tools with which to commit forgery. A new generation of fraudulent alteration emerged when computerized colour laser copies became available. [138] These copies are capable of high resolution copying-modifying of documents, and even the creation of false documents without benefit of an original. [139] Moreover, they produce documents whose quality is indistinguishable from that of authentic documents except by an expert.[140]

(C) Modifications of Data or Programmes [141]

This category of criminal activity involves either direct or covert unauthorized access to a computer system by the introduction of malicious software.[142] The unauthorized modification of computer data or functions, with the intent to hinder normal functioning of the system, is clearly criminal activity and is commonly referred to as computer sabotage.[143] It can be the tool for gaining economic advantage over a competitor. For promoting the illegal activities of

[136] *Id.*
[137] Although data and information are synonymous according to most dictionaries, some people like to think of data as "raw" information or as collections of symbols that are not structured and labelled for people to use. Data security is usually synonymous with information security. Some organizations, however, use *data security* to mean the administration of computer security. Such as password assignment to users, and *information security* to mean the management of information security, such as establishing security policies and control standards.
[138] Some years ago, the U.S. Secret Service (the department responsible for the odd combination of protecting the President and tracking down counterfeiters) determined the new colour laser printers as being a significant threat, what with their ability to produce almost perfect copies of paper money. Based on this, the Secret Service paid a little visit to colour laser printer manufacturers across the the globe and convinced them to add a special little circuit to pretty much every laser printer that leaves the dock. Using a pattern of dots nearly invisible to the naked eye and distributed at random points on the page, it encodes the printer's serial number or various other identifying characteristics in the printer's output. Using seized counterfeit bills, law enforcement agencies can determine exactly which printer made the bills and, working with the printer manufacturer's sales records, determine whom the printer was sold to.
[139] *Id.*
[140] *Id.*
[141] For the *modi operandi*, one can be differentiate between methods causing physical damage and those causing logical damage. During the 1970s, the most frequently practised 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.
[142] *See* J. WELLS, *The Computer and Internet Fraud Manual* (Austin, Texas), [2002] pp. 9-10.
[143] *Id.*

ideologically motivated terrorists or for stealing data or programmes for extortion purposes.[144] In on case,[145] a computer operations supervisor at a bank in New Jersey used a utility program to increase the balances of several friends' accounts. The friends withdraw the money as it arrived, and the supervisor destroyed the withdrawal slips. His plan was to stop the thefts before the end of the current audit period to avoid detection. His friends, however, were too greedy to stop and forced him to proceed further. When the auditors found the logged fraudulent transactions in the balance computer system (which the supervisor did not know about), they investigated to see who had the ability to cause the discrepancies. The supervisor was the only one to fit the bill. [146]

(D) Online Auction Fraud

Many Internet marketplaces conduct transactions by using methods of auctions or exchanges in order to make potential buyers and sellers meet and conclude a deal. [147] However, one of the most types of cyberfraud is online 'auction' fraud. [148] The vendor may be describing the products in a false or misleading manner, or may take orders and money, but fail to deliver the goods.[149] Or he may supply counterfeit goods instead of legitimate ones.[150] One of the most famous types of fraud is investment fraud.[151] Thousands of online investment e-mails have appeared on the Internet in recent years. Many offer investors seemingly unbiased information

[144] *Id.*
[145] *See* D. PAKER, *op. cit.* p. 52.
[146] In another case in Germany, a complex invoice manipulation was committed as early as 1974 by a programmer who carried out salary manipulations worth over DM 193,000 through changes of the salary data as well as the book-keeping and balance sheet programs of his company. Using a program written especially for this purpose, he entered the information on the salaries of fictitious people into the data memories containing company salary information and entered his own account as the account to which the fictitious salaries should be transferred. These salary manipulations would have been discovered by the company because normally, the computer prepared wage-slips, checklists, account summaries, and balances sheets which were carefully checked. In order to prevent discovery by these control printouts, the offender first made adjustments in the salary payments program to ensure that no pay-slips were printed for payments to the fictitious employees so that the payment did not appear in the checklists produced by the computer. By further manipulation of the program which produced the company's accounting summaries and balance sheets, the perpetrator finally succeeded in having the embezzled amounts deducted from the income tax to be paid to the tax office. Thus, the sums did not appear as deficient amounts in the company's accounting summaries and balance sheet. Cited by U. SIEBER, *Legal Aspects of Computer Related Crime, op. cit* p. 52.
[147] *See* C. RAMBERG, *Internet Market Places, The Law of Auctions and Exchanges Online* (Oxford, Oxford University Press), [2002] p. 36.
[148] Normally when thinking about the term, the English auction comes to mind. This is an auction initiated by a seller where higher and higher bids are made orally by bidders. When no further bids are heard the auctioneer lets the hammer fall and the highest acquires the item offered As we see nowadays in the cyberspace, there are many types of transactions that in different ways resemble this English auction. There are actually many examples of Internet marketplaces which may be operated by an independent intermediary or be set up by the party taking the initiative in the transaction. Example of interesting change sites are eBay, Bidlet, Goindustry.com, Metalsite, and Autodaq.
[149] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 147.
[150] *Id.*
[151] *Id.*

free of charge about featured companies or recommending 'stock picks of the month.' While legitimate online e-mails can help investors gather valuable information, some e-mails are tools for fraud. [152] In fact, some companies pay the persons who send online e-mails cash or securities to 'tout' or recommend their stocks. While this is against the law, the federal securities laws require the e-mails to disclose who paid them, the amount, and the type of this payment.[153] However, many fraudsters fail to do so. Instead, they'll lie about the payments they received, their independence, their so-called research, and their track records.[154] The e-mails masquerade as sources of unbiased information, when they stand to profit handsomely if they convince investors to buy or sell particular goods. [155]

(E) Electronic-Mail Forgery

E-mail spoofing or forgery is the term applied to the counterfeiting and forging of e-mail messages, but the euphemism doesn't fully convey the insidious nature of the crime.[156] The sheer size and anonymity of cyberspace demand the information passing through the Internet be subjected to both authentication and accountability controls. The most effective way to invoke these controls is through the use of independent trusted third parties called *certificate authorities* (CAs), which provide digital signatures and encrypted communication of electronic authentication certificates. CAs authenticates the identities of users by exchanging personal information known only to be the communicating parties.[157] CAs log messages for later audit, and they use investigative software to trace the source of messages. In addition, they initiate criminal and civil litigation for wrongdoing.[158] A famous case of e-mail forgery occurred in California in 1996. [159] The spurned girlfriend of the CEO of a large software firm won a wrongful termination suit against the company and collected a $ 100,000 settlement. Until she was fired, the girlfriend as an executive assistant to a vice president in the company. Among other things, she was responsible for changing her supervisor's passwords, providing him with new codes, and managing his e-mail account. A key piece of evidence in the termination suit was copies of an e-mail message her supervisor, the vice president, allegedly sent to the CEO that said, "I have terminated Adelyn per your request." The CEO denied that

[152] Internet Fraud, *How to Avoid Internet Investment Scams*, available at: <http://www.sec.gov/investor/pubs/cyberfraud.htm> (visited 26/03/2005).
[153] *Id.*
[154] *Id.*
[155] *Id.*
[156] *See* D. PAKER, *op. cit.* p. 123.
[157] *Id.*
[158] *Id.*
[159] *See Id* p. 124.

he had fired the women because she refused to have a relation with him, maintaining that the e-mail message was a spoof. In 1997, the company challenged the veracity of the e-mail messages. The district attorney subsequently indicated, creating false documents, and perjury in a superior court. The company found a computer audit records showing back and forth between the vice president's and another employee's e-mail accounts on the day and time that the questionable e-mail message was sent. The vice president proved that he was driving his car and talking on his cellular phone at the time the e-mail message was sent. Even through investigators were unable to retrieve the last numbers dialled from the woman's home computer, she convicted and sentenced to one year in prison and fined $100,000.

1.3.4 Cyberstalking, Harassment and Hate Speech

The neologism *stalking* [160] has entered the English lexicon, connotating a paranoid tinged world of malicious and instructive activity on the Internet.[161] Meloy and Gothard defined it, or as they prefer to call it obsessional tollowing, as 'an abnormal or long term pattern of threat or harassment directed toward a specific individual'.[162] The pattern of threat or harassment was further clarified as being 'more than one overt act of unwanted pursuit of the victim as being harassing', although more than one may seem generous rendering of a long term pattern. [163] Meloy furthers states that in distinction to legal definitions, was designed to further scientific investigation and clinical understanding.[164]

Cyberstalking, also called online stalking or online victimisation, shares important characteristics with offline stalking.[165] The similarities are that, first, the majority of cases involve stalking by former intimates, although stranger stalking certainly occurs in the real

[160] In fact, the word stalk has the meaning of both the act of following one's prey and walking stealthily. To label someone a staker has been, at least from the sixteenth century, to imply he or she a prowler or a poacher. When the media appropriated the word to describe those who pestered and harassed others they provided a new focus for this ancient indictment. Stalking is now a part of our culture language. It has become a category with which we describe and understand our experiences. If someone is repeatedly followed by a stranger, or is distressed at receiving numerous unwanted letters from an estranged partner the, in today's world, they are likely to describe themselves as being staked. Looking back over their life they may now recall having been stalked in the past. In California, a 50-year-old former guard…used the Internet to solicit the rape of a women who rejected his romantic advances…[He] terrorized his 28-old-victim by impersonating her in various Internet chat rooms and online bulletin boards , where he posted , along with her telephone number and address, messages that she fantasized of being raped. On six occasions, sometimes in the middle of the night men knocked on women's door saying they wanted to rape her.

[161] As US Attorney General Janet Reno noted in the report prepared by the Department of Justice in 1999, many of the attributes of the Internet – low cost, ease of use and anonymous nature- make it an attractive medium for fraudulent scams, child sexual exploitation and cybertalking. She also noted that while some conduct involving annoying menacing behaviour may be a prelude to stalking and violence and should be treated seriously. On this point see J. BOON, *Stalking and Psychosexual Obsession* (UK, John Wiley), [2002] p. 202.

[162] *See* P. MULLEN, *Stalkers and their Victims* (Cambridge, Cambridge University Press), [2000], p. 7.

[163] *Id.*

[164] *Id.*

[165] *See* J. BOON, *op. cit.* p. 202.

world and in cyberspace; second, most victims are women and most stalkers are men.[166] And third, stalkers are believed to be motivated by the desire to control the victim. Major differences include, first, offline stalking requires the stalker and victim to be located in the same geographic area whereas cyberstalkers may be located in the same city or across the country; second, technologies make it easier for a cybertalker to encourage third parties to harass and/or threaten a victim; and third, technologies lower the barriers to harassment and threats, and a cyberstalker does not need to physically confront the victim.[167]

Cyberstaking, harassment, hate and racist speech perpetrated over computer networks may or may not be criminal activities, depending on the jurisdiction. [168]

1.3.5 Cyberterrorism

Cyberterrorism is the convergence of terrorism and cyberspace. It has been defined as 'premeditated, politically, motivated attack against information, computer systems, computer programs, and data which result in violence against non combatant targets by sub national groups or clandestine agents.'[169] Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Cyberspace is constantly under assault.[170] Cyber spies, thieves, saboteurs, and thrill seekers break into computer systems, steal personal data and trade secrets, vandalize Web sites, disrupt service, sabotage data and systems, launch computer viruses and worms, conduct fraudulent transactions, and harass individuals and companies.[171] These attacks are facilitated with increasingly powerful and easy-to-use software tools, which are readily available for free from thousands of Web sites on the Internet.[172]

Many of the attacks are serious and costly. In 1998,[173] Spanish protestors bombarded the Institute for Global Communications (IGC) with thousands of bogus e-mail messages. E-mail was tied up and undeliverable to the ISP's users, and support lines were tied up with people who couldn't get their mail. The protestors also spammed IGC staff and member accounts, clogged their Web page with bogus credit card orders, and threatened to employ the same

[166] *Id.*
[167] *Id.*
[168] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 149.
[169] *Id.*
[170] *See* D. DENNING, *Cyberterrorism* (U.S.A, Special Oversight Panel on Terrorism), [May 2000]
[171] *Id.*
[172] *Id.*
[173] *See* Defining cyberterrorism, available at <http://www.asianlaws.org/cyberlaw/library/cc/def_ct.htm> (visited 28/03/2005).

tactics against organizations using IGC services. [174] In the same year a 12-year-old boy successfully hacked into the controls for the huge Roosevelt Dam on the Salt River in Arizona, USA.[175] He might have released floodwaters that would have inundated Mesa and Tempe, endangering at least 1 million people. [176] And finally in 2002, numerous prominent Indian web sites were defaced.[177] Messages relating to the Kashmir issue were pasted on the home pages of these web sites.[178] The Pakistani Hackers Club, led by "Doctor Neukar" is believed to be behind this attack.

1.3.6 Cybertheft

There are many different types of cybertheft, or ways of using ICTs to steal information, money, or other valuables. The offences include: [179]

- *Embezzlement*, which involves misappropriating money or property for the own use of the perpetrator, that has been entrusted to him by someone else. [180]
- *DNS cache poisoning*, a form of unauthorized interception in which intruders manipulate the contents of a computer's DNS cache to redirect network transmissions to their own servers.
- *Unlawful appropriation*, which differs from the embezzlement in that the criminal was never entrusted with the valuables but gains access from outside to company and transfer funds or modifies documents.
- *Plagiarism*, which is the theft of someone else's original writing with the intent of passing it off as one's won.
- *Piracy*, which is the unauthorized copying of copyrighted software, music, movies, art, books, and so on, resulting in loss of revenue to the legitimate owner of the copyright.[181]

---

[174] *Id.*
[175] *See* A. NAGPAL, *Cyberterrorism in the Context of Globalisation* (India, UGC sponsored National Seminar on Globalization and Human Rights), [September 2001].
[176] *Id.*
[177] *Id.*
[178] *Id.*
[179] On this point see D. SHINDER, *op. cit.* p. 24.
[180] For example an employee who uses his or her legitimate access to the company's computerized payroll system to change the data so that he is paid extra, or who move funds out of company bank accounts into his won personal account.
[181] In fact, the unauthorised copying and use of *computer programs* – often called theft of software or software piracy – at first involved, in accordance with the historic development of computer technology, the copying of individual software which frequently contains important internal company know-how. Therefore software theft overlaps with computer espionage in many cases. For example, the German "*debit collection program case" is an example for the copying of individual software which led to the first decision of the Bundesgerichtshof concerning the possibility of copyright protection: Because of the copying of its central computer program and*

- *Identify theft*, in which the cyberspace is used to obtain a victim's personal information, such as Social Security and driver's numbers, in order to assume that person's identity to commit criminal acts or to obtain money or property or to use credit cards or bank accounts belonging to the victim. [182]

II. Legislative Approaches

The part above established the concept of cybercrime and its different forms. This part examines what should be done about it, in terms of developing penal laws that are clear enough to discourage those who might otherwise engage in cybercrime and to allow expeditious investigation and prosecution of those who are not deterred. Section **(2.1**) reviews what has been done in this regard at the national and regional levels. Section **(2.2**) examines efforts that were taken at the international level to combat this crime. Finally, section (**2.3**) examines additional measures that can de taken to achieve this end.

2.1. National and Regional Strategies

The history of computer crimes begins with the history of computers. [183] The first empirical computer crime studies applying scientific research methods were conducted in the 1970s. [184] These studies verified a limited number of cases and suggested that many more have gone undetected or unreported. [185] In the United States, the Senator Abraham RIBICOFF introduced the first proposed federal computer crime legislation in 1977: Federal Computer Systems Protection Act. [186] The bill was revised and reintroduced two years later. [187] It then died in committee;[188] however it was influential in promoting the subsequent enactment of federal computer crime legislation and in encouraging the adoption of such legislation in Florida and Arizona. [189]

---

the following low-price sales by the perpetrator, the victimised debit collection company got into a situation that threatened its existence". *See* U. SIEBER, *op. cit.* p. 45.

[182] In March 2002, federal agents arrested a Jacksonville, Florida man for identify theft in connection with stealing personnel records of 60,000 Prudential Insurance Company employees from a computer database. The man was a former IT employee for Prudential, and he attempted to sell the database information over the Internet for the purpose of obtaining fraudulent credit cards using the stolen identities. *See Press Release, U.S Department of Justice.*

[183] *See* D. SHINDER, *op. cit.* p. 50.

[184] *See* D. PARKER, *op. cit.* p. 11.

[185] M. D. GOODMAN and S. BRENNER, *op. cit.* p. 161.

[186] *See* <http://www.cybercrimelaw.net/tekster/background.html> (visited 31/03/2005).

[187] M. D. GOODMAN and S. BRENNER, *op. cit.* p. 161.

[188] D. GRIFFITH, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, (43 VAND. L. REV), [1990] 453, 456.

[189] *See* R. HOGGE et al., *Computer Invasion of Privacy Under the Virginia Computers Crime Act* [Jan. 2001].

Since then many new crimoids have emerged. Some crimoids, such as eavesdropping on the radio waves that emanate from computers, have never been proven. [190] Reports of computer codes, including the Michelangelo and fictitious Good Times viruses, have added to the folkore of computer crimoids.[191] The vulnerabilities of information society and the limitations of the existing computer security approaches as well as legislations and law enforcement efforts became apparent and widely and publicized in the 1990s. SIEBER argues that the scope of demonstrated and expected computer crimes today and in the future has also expanded far beyond the economic crime, to recover attacks against national infrastructure and social well being.[192]

In Europe, legal reforms have taken place in many countries since 1970s, reflecting a change in legal paradigm. The criminal codes of most of the countries have focused on the protection of tangible objects. However, the revolution of ICTs, which greatly depends on incorporeal values and information, in the latter part of the twentieth century has predicated the development of new legislations which seeks these incorporeal values. The first step of this development in most European countries addressed the protection of privacy, as a response to emerging vast capabilities for collecting, storing and transmitting data by computer. [193] " Data protection legislations " were enacted and have been constantly revised and updated, protecting the citizens' right of privacy with administrative, civil, and penal regulations in (1973) in Sweden, (1974) in the United States of America, (1977) in the Federal Republic of Germany, (1978) in Austria, Denmark, France and Norway, (1979) and (1982) in Luxembourg, (1981) in Iceland and Israel, (1982) in Australia and Canada, (1984) in the United Kingdom, (1987) in Finland, (1988) in Ireland, Japan and the Netherlands, (1991) in Portugal, (1992) in Belgium, Spain and Switzerland, (1995) in Spain, and (1997) in Italy and Greece.[194] Additional data protection laws can be found in many federalist jurisdictions (e.g.

Available at:
<ww.virginialaborlaw.com/library/e-law/outline-vccacomputerinvasionofprivacy2001-01-24.pdf#search='robin%20Kutz%20, %20computer%20crime%20in%20virginia'> (visited 31/03/2005). *See also* L. BECKER, *Electronic Publishing: First Amendment Issues in the Twenty-First Century* , 13 Fordham Urb. L.J. 801 [1985].

[190] D. PARKER, *op. cit.* p. 11.

[191] *Id.*

[192] M. D. GOODMAN and S. BRENNER, *op. cit.* p. 162.

[193] *See* U. SIEBER, *Legal Aspects of Computer Related Crime* (European Commission), [1998] p. 25.

[194] *Id.* For detailed information see for *Australia*, the Freedom of Information Act of 9 March 1982, as amended and the Privacy Act 1988; for *Austria*, the Federal Data Protection Act of 18 October 1978, amended by laws Nos. 370 of 1986, 605 of 1987 and 632 of 1994; for *Canada*, the Access to Information Act and the Privacy Act of 28 June 1982; for *Belgium*, the law for the Protection of the Private Life with Respect to the Treatment of Personal Data of 8 December 1992; for *Denmark*, the Private Registers Act of 8 June 1978 (Act No. 293), amended on 1 April 1988 and the Public Authorities' Registers Act of 8 June 1978 (Act No. 293), amended on 1 April 1988; for *Finland*, the Personal Data File Act No. 471 of 30 April 1987, Personal Registers Act of

Canada, the Federal Republic of Germany, Switzerland, or the United States of America) as well as in many "sectorial" laws regulating privacy protection in specific areas which today become increasingly important (e.g., in the area of telecommunication, police data or online services). This concern with privacy prompted constitutional amendments in Brazil, the Netherlands, Portugal and Spain. [195]

The second step of involved the repression of computer-related economic crimes at the beginning of the 1980s. [196] It was precipitated by the inadequacy of the existing traditional criminal provisions, which protect visible, tangible, and physical objects against traditional crimes, in the advent of cybercrime.[197] These new legislations addressed the new capabilities of cybercrimes to violate traditional objects through new media, to protect intangible objects such as computer software.[198] Many countries enacted new laws fighting computer-related economic crime (including unauthorized access to computer systems). Legislations against computer-related economic crime were enacted since 1978 in the United States of America (in state legislation) and in Italy, since (1979) in Australia , (1981) in the United Kingdom, (1984) in the United States of America (federal level), (1985) in Canada and Denmark, (1986) in the Federal Republic of Germany and in Sweden, (1987) in Austria, Japan and Norway, (1988) in France and Greece, (1990) in Finland and the United Kingdom, (1992) in the

4 February 1987 and chapter 38 of the Penal Code (as amended 1995); for *France*, the Act on Data Processing, Data Files and Individual Liberties (Act No. 78-17) of 6 January 1978, amended on 11 March 1988; for *Germany*, the Data Protection Act of 20 December 1990 (succeeding the Data Protection Act of 27 January 1977); for *Greece*, Data Protection Act (law 2472/1997), passed in April 1997 by the Greek Parliament; for *Iceland*, the Act Concerning the Systematic Recording of Personal Data (Act No. 39/1985) of 25 May 1981; for *Israel*, the Protection of Privacy Law (Act No. 5741/1981) of 23 February 1981, amended in 1985; for *Ireland*, the Data Protection Act (Act No. 25/1988) of 6 July 1988; for *Italy*, Law No. 675 of 31 December 1996, published in the Gazetta Ufficiale 8 January 1997; for *Japan*, the Personal Information Protection Act No. 95 of 16 December 1988; for *Luxembourg*, The Act Organising the Identification on Physical and Legal Persons by Number of 31 March 1979, the Act Regulating the Use of Nominal Data in Electronic Data Processing of 31 March 1979 and the Act concerning the Protection of Privacy of 11 August 1982; for *the Netherlands*, the Law on the Protection of Privacy in Connection with Personal Registration of 28 December 1988; for *New Zealand*, the Privacy Act 1993, amended by the Privacy Amendment Act 1993 and the Privacy Amendment Act 1994; for *Norway*, the Law on Personal Data Registers of 9 June 1978 (Act No. 48) amended by Law No. 55 of 12 June 1987, Law No. 66 of 20 July 1991 and Law No. 78 of 11 June 1993; for *Portugal*, Law 10/91 of 29 April 1991 on the Protection of Personal Data with Respect to Informatics, amended by Law 28/94 of 29 August 1994; for *Spain*, Art. 18 para. 4 of the Constitution and Law 5/1992 for the Regulation of the Automated Processing of Personal Data (LORTAD) of 29 October 1992, and Article 197 Criminal Code (Law No. 10/1995 of 23 November 1995); for *Sweden*, chapter 2 Article 3 para. 2 Instrument of Government (i.e., Constitution) as amended 1988; the Data Protection Act of 11 May 1973 (Law No. 289), amended 1979, 1982, 1986, 1990 and 1992); for *Switzerland*, Federal Data Protection Act of 19 June 1992; for the *United Kingdom*, the Data Protection Act of 12 July 1984; for the *United States of America*, the Privacy Act 1974 (5 U.S.C. § 552a) and the Electronic Communications Privacy Act 1986 (codified at 18 U.S.C. §§ 1367, 2232, 2510-2522, 2702-2711, 3117, 3121-3127).

[195] *Id.*

[196] *Id.*

[197] *Id.*

[198] *Id.*

Netherlands, (1993) in Luxembourg, (1994) in Switzerland, (1995) in Spain and again in Finland, and (1997) in Malaysia.[199] In countries such as Denmark, the Federal Republic of Germany or Finland, the respective laws also included new provisions for trade secret protection.[200] While some countries operate under the legal provisions enacted since the early 1980s, other countries are currently amending these provisions again to reflect new challenges to computer-related criminal law posed by the fast developing computer technology.[201]

In 1980s, a third series of additions to nationals law, also took place. This wave was directed toward protecting the intellectual property in the realm of ICTs.[202] The new legislations include copyright protection for computer software, including penal copyright law and legal protection of topographies. [203] Legislations which explicitly provided copyright protection for computer programs were enacted in (1972) in the Philippines, (1980) in the United States of America, (1983) in Hungary, (1984) in Australia, India and Mexico, (1985)

[199] *See* U. SIEBER, *Legal Aspects of Computer Related Crime*, *op. cit* p. 28. Also see for Austria, the Criminal Code Amendment Act of 1987 (Bundesgesetzblatt 1987/605); for Australia, Section 408e of the Queensland Criminal Code as amended in 1979, Sections 222, 276 of the Northern Territory Criminal Code as amended in 1983, Section 115 of the New South Wales Crimes Act 1900 in its application to the Australian Capital Territory, as amended in 1985, the Crimes (Computers) Act No. 36 of 1988 of Victoria, as well as additional legislation passed in the Australian Capital Territory, the Commonwealth, New South Wales, the Northern Territory, South Australia and Victoria; for Canada, The Criminal Law Amendment Act 1985 (S.C. 1985, c. 19); for Denmark, the Penal Code Amendment Act of 6 June 1985 on Data Criminality; for Germany, the Second Law for the Suppression of Economic Crime of 15 May 1986 (Bundesgesetzblatt I, 1986, p. 721); for Finland, the Laws Amending the Criminal Code No. 769/1990 of 24 August 1990 (first phase of the total reform of the Criminal Code), and No. 578/1995 of 28 April 1995 (second phase of the total reform of the Criminal Code); for France, the Law on Infringements in the Field of Informatics of 5 January 1988; for Greece, Law No. 1805/88 of 30 August 1988; for Italy the Amendment of 1978 to Section 420 Penal Code (concerning attacks to public utility plants and research or data processing facilities); for Luxembourg, Law of 15 July 1993 Aiming to Reinforce the Fight Against Economic Crime and Computer Fraud; for Malaysia, Computer Crime Law of 1997; for the Netherlands, Dutch Computer Crime Act of 23 December 1992, as amended in 1994 and 1995; for Japan, the Penal Code Amendment Act of 1987; for Norway, the Criminal Code Amendment Act of 12 June 1987; for Spain, Criminal Code 1995 (Law No. 10/1995 of 23 November 1995), especially Articles 248.2, 256, 264.2, 278 et seq.; for Sweden, Section 21 Data Protection Act of 4 April 1973, and the Criminal Code Amendment Act of July 1986 (Law No. 123); for Switzerland, 1994 Revision of Property Crime Provisions; for the United Kingdom, the Forgery and Counterfeiting Act of 1981, and the Computer Misuse Act 1990 of 29 June 1990, draft for a new Section 15a Theft Act 1968; for the United States of America, the Credit Card Fraud Act of 1984 (Publ. L. 98-473) and the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 and the Computer Fraud and Abuse Act of 1986 (both codified as amended at 18 U.S.C. §§ 1029-1030) as well as State legislation in every state but Vermont. For a comparative analysis of the various laws see *Sieber*, *The International Handbook on Computer Crime*, [1986], pp. 42 and seq.

[200] *Id.*

[201] *Id.*

[202] *See* U. SIEBER, *Legal Aspects of Computer Related Crime*, *op. cit* p. 29.

[203] In Europe, methods for performing mental acts are not regarded as patentable inventions. Due to this principle, Article 52 (2) and (3) of the European Patent Convention (EPC, Munich, 1973) excludes patentability of computer programs as such. In most European countries this limitation of patentability can be found in the national patent legislations. See, for example, for Austria, Section 1 (2) No. 3 Patent Law, amended 8 June 1984 (Bundesgesetzblatt 1984/234); for France, Sections 6 and 11 Patent Law No. 68-1 of 2 January 1968, modified by Law No. 78-742 of 13 July 1978 and Law No. 84-500 of 27 June 1984; for Germany, Section 1 (2) No. 3 and (3) Patent Law of 5 June 1936, amended on 16 December 1980; for Italy, Section 12 Patent Law No. 1127 of 29 January 1939, modified by Law No. 338 of 22 June 1979; for the United Kingdom, Section I (2) (c) of the Patents Act 1977. *See Id.*

in Chile, the Federal Republic of Germany, France, Japan, and the United Kingdom, 1987 in Brazil, Canada and Spain, (1988) in Canada, Denmark and Israel, (1989) in Sweden. [204]

A fourth wave of reform legislation with respect to illegal and harmful contents started in a few countries in the 1980s, but are expanding rapidly since the triumphant rise of the Internet began in the mid-1990s. Legal amendments adapting traditional provisions on the dissemination of pornography, hate speech or defamation to computer-stored data were passed in the United Kingdom in (1994) and in Germany in (1997).[205] Special provisions clarifying the responsibility of service and access providers on the Internet were enacted in the United States of America in (1996) and in Germany in (1997). [206] A last group of issues – discussed in particular in the 1990s – concerns the creation of requirements for and prohibitions of security measures. [207] This field of law includes minimum obligations for security measures in the interest of privacy rights or in the general public interest. It also covers prohibitions of specific security measures in the interest of privacy rights or of effective prosecution of crimes, such as limitations of cryptography. [208]

On such a basis, the adaptation of legislations to new forms of cybercrime resulted in a multitude of different legal questions, which can be traced back to six main series of cybercrime legislation: The Protection of privacy (**2.1.1**), the protection of economic criminal law (**2.1.2**), the protection of intellectual property (**2.1.3**), and finally the protection against illegal contents (**2.1.4**). The following section will differentiate between these main fields of these legislations.

2.1.1 The Protection of Privacy

Legislations against infringements of privacy have been adopted in most European countries with data protection laws of more or less general character. An analysis of these acts shows that different international actions have already achieved a considerable uniformity in the general administrative and civil law regulations of the national privacy laws. In spite of this tendency, some differences in these regulations can be remarked. These differences concern the legislative rationale, the scope of application, the procedural requirements for starting the processing of personal data, the substantive requirements for processing personal data, and

[204] *Id.*
[205] M. D. GOODMAN and S. BRENNER, *op. cit.* p. 164.
[206] *Id.*
[207] *See* U. SIEBER, *op. cit* p. 32.
[208] *Id.*

finally the respective control institutions.[209] On such a basis a comparative analysis to the protection privacy will distinguish four main categories of criminal privacy infringements, which can in particular be found in the European privacy laws: infringements of substantive privacy rights (a), infringements against formal legal requirements (b), infringements of access rights (c), and neglect of security measures (d).

The category of "crimes against privacy" is constituted by infringements of substantive privacy rights and includes the following offences: [210]

- The illegal entering, modification, and/or falsification of data with the intent to cause damage.
- The storage of incorrect data. This act in most countries is covered by the general offences of information and in some countries by additional statutes within the privacy laws.
- The illegal disclosure, dissemination, obtainment of and/or access to data, acts which are covered in most laws, however, to different extents.
- The unlawful use of data.

However, as a result of the uncertainties of the substantive provisions, many legal systems rely to a great extent on an additional group of offences against formal legal requirements or orders of supervisory agencies. The formal offences against supervisory agencies and regulations which are, furthermore, included in most privacy laws contain in general more precise descriptions of the prohibited acts than the substantive offences. These formal provisions also vary considerably within the national legislation. The differences among the formal offences are not only based on differences in administrative law concerning the existence, nature, and powers of supervisory agencies, and the respective duties of the data processors. They are mainly evoked by different answers to the fundamental question whether "formal" offences should be regarded as criminal or not.[211] This leads to the fact that some countries, such as France, punish formal offences against supervisory agencies and regulations with severe criminal sanctions, while others, such as Germany, regard such acts as "*Ordnungswidrigkeiten*", or "petty offences", only punishable by fines.

[209] *See* U. SIEBER, *op. cit* p. 64.
[210] *Id.*
[211] *Id.*

In the Italian Data Protection Act,[212] it is a criminal offence not to comply with the decrees of the Supervisory Authority, and it is an administrative offence not to provide the Supervisory Authority with the necessary information or documents.[213] Likewise the formal offences criminalised vary among the various privacy laws: the main type of formal infraction covered in many states by criminal law concerns the infringement of the legal requirements for starting personal data processing (registration, notification, application for registration, declaration, or licensing).[214] Additional – and considerably varying – formal offences which can be found in many European privacy legislations are: the infringement of some regulations, prohibitions, or decisions of the surveillance authorities; the refusal to give information or the release of false information to the surveillance authorities; the hindering of the surveillance authorities; the refusal to grant access to property and the refusal to permit inspections by surveillance authorities; the obstruction of the execution of a warrant; the failure to appoint a controller of data protection in the company, as well as neglecting to record the grounds or means for the dissemination of personal data.[215]

The third category of criminal privacy infringement is the individual's rights of information or freedom of information. With regard to a party's right of access, in many countries such as in Luxembourg and Sweden – it is an offence to give false information, not to inform the registered party or not to reply to a request. According to German law, this act is considered to be an "*Ordnungswidrigkeit*" which is punishable by a fine.[216] A non-criminal comprehensive system providing access to government information can be found especially in the United States of America.[217]

Finally, some legislators punish the neglect of security measures with an administrative fine or with a penal sanction.[218]

---

[212] Law no. 675 of 31 December 1996, on the protection of individuals and other subjects with regard to processing of personal data "Italian Data Protection Act", governs the processing of personal data, when the processing takes place Italy. The Italian Data Protection Act ensures the respect of the rights, fundamental freedoms and dignity of natural persons, particularly with regard to privacy and personal identity.

[213] *See* U. SIEBER, *op. cit* p. 68.

[214] *Id.*

[215] Most of the respective provisions are contained in the general data protection acts cited by U. SIEBER in chapter I, fn. *Id*. For more information see, for Austria, Section 50 (1) of the Data Protection Act; for Denmark, Section 27 (1) No. 1 and 2, Section 27 (2) No. 4 Private Register Act; for Germany, Section 44 of the Federal Data Protection Act of 1990; for France, Sections 41 and 42 of the Act on Data Processing, Data Files, and Individual Liberties; for Italy, Sections 34-39 of the Data Protection Act; for Luxembourg, Sections 32, 37 of the Act Regulating the Use of Nominal Data; for Sweden, Section 20 (1), (2), (6) Data Act; for the UK, Sections 5 (5); 6 (6); 10 (9); 12 (10) of the Data Protection Act; for the USA, Section 522a para. i (2) of the Privacy Act 1984.

[216] *See* Luxembourg section 34 of the Act Regulating the Use of Nominal Data. For Sweden, see section (20) 5 Data Act.

[217] *See*, for the USA, the Freedom of Information Act 5 U.S.C. § 552.

[218] *See* Denmark, section 27(1) no. 2 Private Registers Act. Luxembourg, section 36 of the Act Regulating the

2.1.2 Computer Related Economic Crimes

This reform of computer-related economic crimes was developed at the beginning of the 1980s, as a reaction to computer-related economic crimes.[219] These amendments were necessary, because new forms of ICTs crimes posed a threat, not only to the traditional objects of criminal law protection, but also to intangible goods.[220] To avoid such evil acts, many countries passed new legislations and provided new offences for the prevention of illegal access to computer systems.

(A)Hacking

In those jurisdictions where there has been the greatest development of the criminal law in response to computer misuse, particularly the United States, the most important approach has been to criminalize the initial unauthorized access of the computer (Hacking). Some computer crime statues penalize 'computer trespass, whatever the motivation or reason for the intrusion.[221] Thus, according to Scott, [222] regardless of what a defendant does after gaining unauthorized access, the access itself may well constitute a criminal offence. In response to the new cases of "hacking", many countries developed new statutes protecting a "formal sphere of secrecy" for computer data by criminalising the illegal access to or use of a third person's computer or computer data. Legislation covering wiretapping and unauthorised access to data processing and communication systems [223] have therefore, been enacted in Canada, Denmark, Germany, Finland, France, the Netherlands, Norway, Spain, Sweden, Switzerland, the United Kingdom [224] and the United States. [225] Moreover, some of the new

---

Use of Normal Data. Also see for Italy, article 36 of Data Protection Act, article 36(2) of the new Italian Data Protection Act.

[219] *See* U. SIEBER, *op. cit* p. 69.

[220] Such as computer softwares.

[221] M. WASIK, *Crime and the Computer* (Oxford, Rendon Press Oxford), [1998] p. 70.

[222] *Id.*

[223] In fact, the definition of the term computer in most countries often suffers from overbreadth. It includes for example handheld calculators, new kitchen stoves and electronic typewriters. These problems are avoided in a 1983 Tennessee statue which defines "computer" in terms of function as "a device that can perform substantional computation, including numerous arithmetic or logic operations, without intervention by a human operator during the processing of a job. *See* Tennessee Code An. Section 39-3-1403(2).

[224] It became quite clear after the decision of the House of Lords in *Gold and Schifreen* that there was no specific criminal offence en England which could be used to deal with the unauthorized use of a legitimate user's password or the use of a false password to gain access to information stored in a computer. There is no general offence of impersonation in English law and none of the traditional property offences in the Theft Act 1986 and 1978 can be made out on these facts. It had been through by some (R.A.BROWN) that an offence under the Forgery and Counterfeiting Act 1981 might be utilize in such a case, but a prosecution under this statue, while proving successful at trial, ultimately resulted in the convictions being overturned on appeal. This meant a substantial limitation on the prospects for successful prosecution of the hacker or other computer misuser, where no dishonest or malicious intent at the time of access could be proved, and where no offence consequent upon

laws which have been proposed demonstrate various approaches, which range from provisions criminalising "mere" access to DP-systems,[226] to those punishing access only in cases where the accessed data are protected by security measures,[227] where the perpetrator has harmful intentions,[228] where information is obtained, modified or damaged,[229] or where a minimum damage is caused. [230] Some countries [231] combine several of these approaches in one or more provisions with a "basic" hacking offence and the creation of qualified forms of access (in a more serious "ulterior" offence) carrying more severe sanctions. A wide range of criminal law protection exists, e.g., in the new English law which enacted three new "hacking offences" covering in a "basic" offence, a person "if he causes a computer to perform any function with the intent to secure access to any program or data held in any computer".

(B) Computer Espionage

Computer espionage is about the purposeful discovery of "information" [232] or "evidence".[233] An industrial spy may be looking for secret information on a Microsoft project manager's laptop that specifically relates to the company's future and hush-hush longhorn operating system. [234] Depending on what the information is, it could evolve into evidence. For example, a phone number stored in a PDA address book could belong to a known drug dealer and become supporting evidence for a criminal case. [235] In addition to information and evidence, there are two other important concepts in computer espionage: The activity is typically unauthorized and unknown. In most cases, the victim is not going to give explicit or implicit

access had been committed. On this point see M. WASIK, *op. cit.* p. 71.

[225] *See* for Canada, Article 342.1 Criminal Code ; for Denmark, Section 263 (2) and (3) Penal Code, for Germany Section 202a Penal Code; for Finland, chapter 38 Section 8 of the Penal Code (as amended 1990); for France, Article 462-2 Criminal Code, amended in 1988; for Greece, Article 370 C (2) Criminal Code, as amended in 1988; for the Netherlands, Article 138a (1), (2) Criminal Code, amended 1992; for Norway, Section 145 Penal Code, amended 1987; for Spain, Article 256 Criminal Code 1995; for Sweden, Section 21 Data Protection Act; for the UK, Sections 1, 2 Computer Misuse Act 1990; for Switzerland, Article 143bis Criminal Code; for the USA, the Electronic Communications Privacy Act of 1986 (18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126), the Computer Fraud and Abuse Act of 1984 and 1986 (codified at 18 U.S.C. §§ 1029, 1030) as well as different state laws.

[226] Australia, Denmark, England, Greece and the majority of states of the United States of America.

[227] Germany, the Netherlands, Norway.

[228] Canada, France, Israel, New Zealand, Scotland.

[229] Some states of the USA.

[230] Spain.

[231] Finland, the Netherlands, the United Kingdom.

[232] The American Heritage Dictionary of the English Language defines information as "knowledge of specific events or situations that has been gathered or received by communication, intelligence, or news".

[233] Evidence is "a thing or things helpful in forming a conclusion or judgement".

[234] *See* J. McNAMARA, *Secrets of Computer Espionage* (USA, Wiley), [2003], p. 2.

[235] *Id.*

permission to have someone snoop through his computer.[236] Exceptions might be in the workplace in which employee monitoring takes place. In general, spies can be lumped into seven different categories: (1) Business spies;[237] (2) Bosses;[238] (3) Cops; (4) Private eyes and consultants; (5) Spooks; (6) Criminals; (7) Whistleblowers; (8) Friends and Family.[239]

On such a basis the question arises as to what extent pure acquisition of incorporeal information can or should be covered national legislations. Many European countries, such as Belgium, Italy, are reluctant to apply the traditional provisions on theft and embezzlement to the unauthorised "appropriation" of secret information, because these legislations generally require that corporeal property is taken away with the intention of permanently depriving the victim of it. [240] In Japan, according to articles 235, 252 and 253 of the penal Code, the definition of the intention of unlawful appropriation has been widened, and now includes the intent to use property only temporarily; nevertheless. Japanese law still requires the taking of tangible property and cannot be applied if data are accessed via telecommunication facilities.

In the United States, some courts regarded computer data as property in the sense of traditional larceny provisions and in many states the legislatures have defined computer data or trade secrets as "property" or a "thing of value", to enable the application of the larceny

[236] In August of 2002, several dozen FBI agents raided the offices of Business Engine, a Silicon Valley software company specializing in Web-based collaboration tools. The raid was prompted when computer Niku Corporation discovered in its server logs that someone with an IP address that mapped back to business Engine had used Niku passwords to access the company's network more than 6,000 times. More than 1,000 documents had been downloaded during the intrusions, including information about upcoming features, lists of potential customers, pricing and sales call schedules. Subsequent investigations revealed that since October 2001, outsiders had logged onto the internal Niku network, using up to 15 different accounts and passwords to access proprietary documents. As of late September 2002, the once-thriving Niku was on the brink of being delisted by NASDAQ because of its low stock value. It does not take a Harvard MBA to speculate that an extensive economic espionage campaign could have contributed to Niku's ill fortunes. Niku has filled suit against Business Engine, and it will be interesting to watch the details of this case emerge.

[237] Consider a study released in 2002 by the American Society for Industrial Security, U.S Chamber of Commerce, and PricewaterhouseCoopers, a survey of Fortune 1000 corporations and 600 small to mid-sized U.S companies: (a) Forty percent of the companies that reported to the survey reported having episodes of known or suspected loss of proprietary data; (b) Proprietary information and IP losses accounted for between $53 billion and $ 59 billion; (c) Economic spies are looking for information; they most commonly target research and development, customer lists and related and financial data; (d) Despite the potential impact of possibly successful attacks, only 55 percent of the responding companies aid their management was concerned about information loss and were taking precautions to prevent it. The implication of this is a significant number of managers underestimate or don't understand the risks and costs of data theft. *See Id,* and for more information on the differences between legitimate competitive intelligence and illegal espionage, visit the Society of Competitive Professionals Web Site at <http://www.scip.org>.

[238] In 1995, a subsidiary of Chevron was sued for sexual harassment over an e-mail that circulated through the company entitled ' 25 Reasons Why Beer is Better Than Women'. The case was settled out of court for $2.2 million, and Chevron now monitors employee e-mail. In July 2000, Dow Chemical fired 50 employees and disciplined 200 others for accessing online pornography. In October 1999, 40 employees at Xerox were fired fir surfing forbidden Web sites. Whether employees like it or not, employee monitoring has become a commonly used management tool. *See Id.*

[239] *Id.*

[240] *See* for Belgium section 461 Penal Code; for Italy sections 624, 646 Penal Code.

provisions or new general provisions on computer crime.[241] As a result of the differences in the nature of corporeal property and intellectual values, the difference between traditional property rights and intellectual property rights, as well as the difference between traditional theft of tangible things and the theft of information, M. SIEBER declares that a theory of property should be denied for the general protection of intellectual values.[242] He also argue that:

> "One has to keep in mind that civil law does not regard information per se as protectable and that even with the statutory monopolies of copyrights, patents, trademarks and industrial designs, the creator, inventor or designer of the work is only given exclusive ownership rights within certain limits (especially with respect to time and geographic areas)".[243]

Reform laws strengthening penal trade secret protection have been enacted recently in Canada, Denmark, Germany, the Netherlands, Sweden, the United Kingdom and the United States.[244] This meaning of trade secret protection and fair competition is in harmony with the modern American information theory which rejects the static "property-theory" and turns to procedural "relationship-theories" and "entitlement-theories" by looking at the relationship between discloser and disclose.[245] However, M. SIEBER argues: "it can be said that criminal trade secret law and civil unfair competition law are less developed in Anglo-American countries (especially in Canada) as well as in Asian countries (especially in Japan), than in continental Europe". "In Japan, e.g., the amendments to the Unfair Competition Act enacted in 1990 did not include any penal sanctions". [246]

In order to achieve an international consensus M. SIEBER recommends that legal systems in their penal codes establish penal trade secret protection backed up by adequate civil provisions concerning unfair competition.[247] These penal and civil provisions should generally apply to all trade secrets and not be limited to the computer and data processing area.[248]

---

[241] *See* SIEBER, *Legal Protection of Computer Data, Programs and Semiconductor Products – A Comparative Analysis with Suggestions for Legal Policy*, in *International Chamber of Commerce* [1988], pp. 7 et seq.
[242] *Id.*
[243] *Id.*
[244] On this point this e.g., for Denmark, the qualifications in Section 263 and 264 Penal Code, amended in 1985; for Germany, Section 17 of the Act Against Unfair Competition, amended in 1986; for Sweden, Section 21 Data Protection Act, chapter 10 Section 5 Criminal Code, Protection of Trade Secrets Act 1990; for Switzerland, Article 143 Criminal Code; for the USA, The Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1839). *Id.*
[245] *See* U. SIEBER, *op. cit* p. 85.
[246] *Id.*
[247] *Id.*
[248] *Id.*

(C) Computer Fraud

Considerations of the topic of computer fraud raises three major questions: What is it? How extensive is it? Is it illegal? In common with most aspects of the topic, definitional problems abound. [249] In the United Kingdom, the Audit Commission has conducted four triennial surveys of computer-related fraud based on a definition referring to: 'any fraudulent behaviour connected with computerisation by which someone intends to gain financial advantage'.[250] Such a definition is capable of encompassing a vast range of activities some of which may have only the most tenuous connection with a computer. The Council of Europe, in its report on computer-related crime[251] advocates the establishment of an offence consisting of: [252]

" *The input, alteration, erasure or suppression of computer data or computer programmes [sic], or other interference with the course of data processing, that influences the result of data processing thereby causing economic loss or possessor loss of property of another person, or with the intent of procuring an unlawful economic gain for himself or for another person*".

However this definition is broad in scope. It would appear for example that the proposed offence would be committed by a person who wrongfully uses another party's cash dispensing card to withdraw funds from a bank account. Although there can be little doubt about the criminality of such conduct, the involvement of the computer is purely incidental.[253] In most areas of traditional legal interests, the involvement of computer data does not cause specific legal problems. The respective legal provisions are formulated in terms of results and it is completely irrelevant if this result is achieved with the involvement of a computer or not.[254] However, even in this area computer-specific qualifications are proposed in some countries.[255] When examining the field of financial manipulations, the situation will be different: Many countries [256] require that the offender take an "item of another person's property". The statutory provisions are not applicable if the perpetrator appropriates deposit money. In many legal systems, these traditional provisions also cause difficulties, as far as manipulations of cash dispensers are concerned.

---

[249] C. REEDS, *op. cit.* p. 246.
[250] *Id.*
[251] *See* Recommendation No. R (89) 9 adopted by the Council of Ministers on 13 September 1989.
[252] *Id* p. 28.
[253] C. REEDS, *op. cit.* p. 246.
[254] *See* U. SIEBER, *op. cit* p. 81.
[255] For example the USA.
[256] For example Greece, Luxembourg and Germany.

The statutory provisions of fraud in most legal systems demand a deception of a person. They cannot be used when a computer is "cheated". The statutory definitions of breach of trust or "*abus de confiance*" which exist in several countries – such as in Belgium, Germany, Japan, France, or Switzerland – only apply to offenders in high positions and not to punchers, operators or programmers; some provisions also have restrictions concerning the protected objects. On such a basis, many European countries looked for solutions *de lege lata* which did avoid stretching the wording of already existing provisions too much.[257] Laws on ICTs fraud have been enacted in Australia, Austria, Denmark, Greece, Germany, Finland, Japan, the Netherlands, Sweden, Norway, Spain, and the USA. Similar reform proposals are being discussed in the United Kingdom while others are already discussing amending and tightening the existing rules. Moreover, the Swedish legislature expanded the provisions on breach of trust to technicians in qualified positions of trust. In general, such legal amendments are necessary since computer-based attacks to traditional legally protected interests should not be privileged. In terms of the time at which an offence is committed, the case of *R* v *Thompson* [1984] I WLR 962 furnishes a helpful illustration.[258] Thompson, a computer programmer, was employed by a bank in Kuwait. Whilst so employed, he devised a plan to defraud the bank. Details of customer's accounts were maintained on computer. A number of these accounts were dormant, i.e, no transactions had taken place over a significant period of time. Thompson devised a program which instructed the computer to transfer sums from these accounts to accounts which he had opened with bank. In an effort to minimise the risks of detection, the transfers were not to be made until Thompson had left the bank's employ and was on a plane returning to England. On his return, Thompson opened a number of accounts with English banks and wrote to the manager of the Kuwaiti bank instructing him to arrange for the transfer of the balances from his Kuwaiti accounts. This was done but subsequently his conduct was discovered and Thompson was detained by the police. Charges of obtaining property by deception were brought against him and a conviction secured. An appeal was lodged on the question of jurisdiction. Whilst not denying any of the facts received above, Thompson argued that any offence had been committed in Kuwait and, therefore, that the English courts had no jurisdiction in the matter.

This plea did not commend itself to the Court of Appeal which held that the offence was committed at the moment when the Kuwaiti manager read and acted upon Thompson's letter. At this stage, Thompson was subject to the jurisdiction of the English courts.

[257] For example Germany and the United States of America.
[258] *See* [1984] 1 WLR 962 at pp. 967-8, *in* C. REEDS, *op. cit.* p. 248.

2.1.3 Offences Against Intellectual Property

Intellectual property is, in essence, a right given to authors or creators of 'works', such as books, films or computer programs, to control the copying or other exploitation of such works. [259] In marked contrast to patent rights, copyright begins automatically on the creation of a 'work' without the need for compliance with any formalities.[260] In the field of information and telecommuincation technologies, the concept of Intellectual Property is especially important for the protection of semiconductor topographies, computer programs and databases. After computer software had been excluded from patent protection throughout the world in the 1970s, various countries at first passed new laws which assured a civil law copyright protection for these programs. [261] Since 1984 additional legislations and laws for the protection of topographies of semiconductor chips were adopted. Special legal protection on databases was first enacted in 1997. More severe provisions of criminal copyright law entered into force in numerous legal systems since the mid 1980s. [262]

(i) *Protection of Computer Programs*

Most countries have explicitly provided copyright protection for computer programs by legislative amendments since the 1980s. This has been the case for example in Canada, Denmark, Germany, Finland, France, Hungary, Japan, Luxembourg, Malaysia, Mexico, the Republic of China, Singapore, Spain, Sweden, the United Kingdom and the USA.[263] As a consequence, in all countries, the courts recognise copyright protection of computer programs today.[264] This fundamental recognition of the inclusion of computer programs in copyright protection was strongly promoted by the EC Directive on the protection of computer programs and by other international proposals in this field.[265] Moreover differences in the nature and scope of the IP rights available in the EU States have frequently given rise to trade barriers. In seeking to limit the effects of such restrictions, the European Commission and the European Court have drawn distinctions between the existence and the exercise of IP rights. Ownership of an IP right is not inherently anti-competitive; indeed the Treaty of Rome

[259] C. REED, *op. cit.* p. 104.
[260] *Id.*
[261] *See* U. SIEBER, *op. cit* p. 84.
[262] *Id.*
[263] *See* Council Directive of 14 May 1991 on the legal protection of computer programs
[264] *See* U. SIEBER, *op. cit* p. 85.
[265] C. REED, *op. cit.* p. 104.

sanctions import and export restrictions which can be justified as being 'for the protection of industrial or commercial property'. [266]

In June 1988 the English Commission published a Green Paper entitled *Copyright and the Challenge of Technology*. [267] In that discussion document the Commission inclined towards the view that copyright is the most appropriate from the protection for computer programs and should provide the foundation for a Directive on software protection. [268] Following a period of consultation which ended in December 1988, a Directive on the Legal Protection of Computer Programs (The Software Directive) was adopted by the Council of Ministers on 14 May 1991. [269] Several principals and rules were laid down in the Directives currently in force in this area, in particular 92/100/EEC, [270] 93/83/EEC, [271] 93/98/EEC, [272] 96/9/EC, [273] and 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. [274]

(ii) *Protection of Semiconductor Products*

With regard to the miniaturisation of computers and the development of "fifth generation", [275] computers, the technique of integrated circuits has become more and more sophisticated.[276] Due to the possibilities of copying the topography of semiconductor products, there is a demand for an effective protection of these products in order to stop unauthorised reproduction. [277]

---

[266] *Id.*
[267] *Id.*
[268] *Id.*
[269] 91/250/EEC, OJ L122, 17 May 1991, p. 42.
[270] Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property (OJ L 346, 27.11.1992, p. 61). Directive as amended by Directive 93/98/EEC.
[271] Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission (OJ L 248, 6.10.1993, p. 15).
[272] Council Directive 93/98/EEC of 29 October 1993 harmonising the term of protection of copyright and certain related rights (OJ L 290, 24.11.1993, p. 9).
[273] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases (OJ L 77, 27.3.1996, p. 20).
[274] Available at <http://www.fipr.org/copyright/eucd.html#note7> (visited at 01/04/2005).
[275] Fifth generation computing devices, based on artificial intelligence, are still in development, though there are some applications, such as voice recognition, that are being used today. The use of parallel processing and superconductors is helping to make artificial intelligence a reality. Quantum computation and molecular and nanotechnology will radically change the face of computers in years to come. The goal of fifth-generation computing is to develop devices that respond to natural language input and are capable of learning and self-organization.
[276] *See* U. SIEBER, *op. cit* p. 85.
[277] *Id.*

In many countries, the determination of laws required to protect semiconductor products was difficult. In the United States a special protection for computer chips was provided by the Semiconductor Chip Protection Act of 1984.[278] Special laws protecting the topographies of semiconductor products were also adopted in Europe. For example in Denmark, Germany, France, Italy, the Netherlands, Spain, Sweden and the United Kingdom.[279] Some these countries [280] include criminal sanctions which, among other things, punish the infringement of a circuit layout right. Such penal sanctions for clear cases of infringements of circuit layout rights seem to be appropriate.

In the United States, if the work is original (i.e, not staple, commonplace or familiar in the industry: s. 902(b)) and first exploited in the US or exploited elsewhere by a US national or domiciliary the designer of the mask work receives the exclusive right to reproduce or to import or distribute the work or products containing the work (s. 905). [281] In *Brooktree Corporation* v *Advanced Micro Devices Inc.* (1988) No. 88-1750-E (cm) (SD Cal 13 December 1988), the court noted that both parties agreed that if the defendant could produce an adequate paper trial establishing reverse engineering the appropriate standard for infringement would be that the two masks were 'substantially similar'. [282] However, the US Court of Appeals for the Federal Circuit in this case held that a 'paper trail' does not conclusively prove a reverse engineering defence under the US Act. The Court explained that the statue does not excuse copying where the alleged infringer first tried and failed to reserve engineer a chip without copying. [283] The court rejected the claim that the reverse engineering defence can be established by the sheer volume of paper, pointing out that the paper trail is evidence of independent effort but not incontrovertible proof of either the originality of the end product or the absence of copying.[284]

[278] *See* D. LADD and *al. Protection for semiconductor chip masks in the United States : analysis of the Semiconductor Chip Protection Act of 1984* (USA, Munich : Deerfield Beach), [2004].
[279] For a comparative overview see Sieber, *Legal Protection of Computer Data, Programs and Semiconductor Products – A Comparative Analysis with Suggestions for Legal Policy, in: International Chamber of Commerce (ed.), International Contracts for Sale of Information Services* [1989] , pp. 7 et seq.
[280] *See* the Austrian, Dutch, Finnish, German, Japanese and Swedish laws.
[281] C. REEDS, *op. cit.* p. 200.
[282] *Id.*
[283] *Id.*
[284] *Id.*

2.1.4 Offences of Dissemination of Pornography and Harmful Contents

"A century that began with children having virtually no rights is ending with children having the most powerful legal instrument that not only recognizes but protects their human rights." – Carol Bellamy, UNICEF Executive Director

Over recent years, offences related to the production, possession and the distribution of "child pornography" have assumed great prominence. As soon as we examine what we mean by child pornography, we begin to encounter uncertainties and confusions. The term "child" and "pornography" on their own are themselves contentious, with complex and sometimes contradictory meanings. [285] The ways that we define what it is to be a child are socially and temporally situated, as are views about the appropriateness of adult sexual interest and children constitutes pornography. Given this, definitions of child pornography can therefore be quite complex. [286] Consistent with the UN Convention on the Rights of the Child, in the West we tend towards an all embracing view that childhood ends at 18, and seek to extend legal protection from sexual and labour exploitation to all below that age. [287] In contrast, social and physiological insights into what constitutes a "child" emphasise that it is not simply a chronological judgement, but it is also a social and cultural statement.

However, assuming a child is involved, what then constitutes pornography? In some jurisdictions pornography is linked to sexualised behaviour. This can make a critical difference as to how any given putative example of child pornography is regarded. [288] Thus, it is quite possible for a picture to be regarded under laws that emphasise sexual qualities as child pornography, but to fail to jurisdictions where obscenity or public morality definitions prevail. Another major difficulty relates to what, in the context of adult images, might be regarded as erotica. Pictures of this kind would generally be regarded as child pornography where reference is made to sexual qualities, but might not if obscenity or indecency criteria are used. [289] At its worst, child pornography is a picture of a child being in some sense sexually abused. Goldstein (1999) differentiated between pornography and erotica in that the

[285] M. TAYLOR, *ChildPornography: An Internet Crime* (NY, Maw Taylor), [2003]
[286] *Id.*
[287] The Convention on the Rights of the Child is the first legally binding international instrument to incorporate the full range of human rights – civil and political rights as well as economic, social and cultural rights. Two Optional Protocols, on the involvement of children in armed conflict and on the sale of children, child prostitution and child pornography, were adopted to strengthen the provisions of the Convention in these areas. They entered into force, respectively on 12 February and 18 January 2002.
[288] M. TAYLOR, *op. cit.* p. 3.
[289] For example 'erotica' can be described sexually explicit material that depicts adult men and women consensually involved in pleasurable, non-violent, non-degrading, sexual interactions. Whereas pornography might be thought to be depict activity that is non-consenting.

objects that form erotica may, or may not be, sexually oriented or related to a given child or children involved in a sexual offence, but the pictures in themselves may be legal. [290] The functions of such pictures may be as an aid to fantasy, but in the context of a particular child, they may also serve to: [291]

- Symbolically keep the child close;
- Remind the offender of what the child looked like at a particular age;
- Make the child feel important or special;
- Lower the child's inhibitions about being photographed;
- Act as memento that might give the offender status with other people whom he associates with;
- Demonstrate propriety by convincing children that what the offender wants them to do is acceptable because he had engaged in a similar way with other children;
- Provide a vehicle for blackmail;
- Act as an aid to seduce children, by misrepresenting moral standards and by depicting activities that the offender wishes to engage the child in.

In cyberspace preferential sex offenders study the targets of teenagers; they know where children of preferred age group will be and what sorts of things interest them.[292] Before the Internet, preferential sex offenders haunted the citizens band and ham radio. The technology lent itself to use by children. It enabled telecommuincation with many people at the same time, and did not require a minimum age to use it. Sitting in his or her room, a child could with other people.[293] Depending on whether citizens band or ham radio frequencies were employed, a child could reach people over considerable distances. On such a basis, preferential sex offenders often use the latest technology to attract victims. [294] For instance, an offender might coax a child his home with an offer to allow the child to play the latest video game.

[290] M. TAYLOR, *op. cit.* p. 75.
[291] *See Id.*
[292] *See* M. FREEARO, *Investigating Child Exploitation and Pornography: The Internet, Law and Forensic Science* (Elsevier Academic Press, London), [2005] p. 15.
[293] *Id.*
[294] *Id.*

Initially, child pornographers were subject to laws in many countries (epically in continental Europe). Some of them regulated this offence in the national penal codes. [295] Others treated it with special laws on pornography.[296] Finally, some countries faced it by laws for protection of minors or laws on telecommuincation.[297]

During the 1970s and 1980s the United States Supreme Court made a number of landmark decisions governing obscenity and child pornography. In 1973 the court decided *Miller v. California* (1972)[298] the case that set the standard for determining obscenity. [299] The test set fourth in *Miller* dictates that for a work to be condemned as "absence" , one must determine that, taken as whole, it appeals to the prurient interest, portrays sexual conduct in an patently offensive way measured by community standards; and lacks serious social value, whether literary, artistic, political or scientific. [300]

Shortly thereafter, the court decided *NewYork v. Ferber* (1984). [301] *Feber* held the states have a compelling interest in protecting children; that child pornography is inextricably intertwined with child exploitation and abuse because it is both a record of the abuse and it encourages production of similar materials; and that child pornography has very little social, scientific, political, literary or artistic value. [302] In this affair, the court distinguished "child pornography" from "obscenity" and material need to be obscene for it to be illegal child pornography. The court further distinguished child pornography from obscenity in *Osborne v. Ohio* (1990); [303] holding that in contrast to obscenity, states could regulate the "mere" possession of child pornography.

Actually, the dissemination of publications containing child pornography is punishable under all of the above mentioned concepts and in all examined legal systems.[304] Especially the last few years have produced a trend towards extending the penal protection against child pornography by special provisions. As a consequence in most countries nowadays exist special penal provisions against child pornography. Only in a few countries, the dissemination

[295] For example Germany, Spain, Italy and Belgium.
[296] For example the UK and the Republic of Ireland.
[297] For example the USA.
[298] Miller *v*. California. 314 US. 15 [1972].
[299] "Obscenity" is a legal determination. For material to be absence, it must appeal to prurient interest: portray sexual conduct in a patently offensive manner as measured by community standards; and lack serious literary, artistic, political, scientific or other social value.
[300] *See* M. FREEARO, *op. cit.* p. 16.
[301] *NewYork v. Ferber* 458 US. 747.
[302] *See* M. FREEARO, *op. cit.* p. 16.
[303] *Osborne v. Ohio* 458 US. 103
[304] *See* M. FREEARO, *op. cit.* p. 16.

of child pornography is still covered by general provisions against pornography.[305] The age of the children protected by the laws against child pornography differs considerably: When it comes to protecting minors from being exploited as actors, the age limit is 14 years in (Germany and Austria), 15 years in (France and Poland), 16 years in (Switzerland and the United Kingdom) and finally 18 years in (Sweden, and the US). [306] Sometimes other persons requiring protection similar to the one given to minors are also included. In many countries the liability for "hard-core" pornography is not limited to child pornography, but also covers pornography combined with excessive use of violence, sodomy, negrophilia or sexual presentations involving human secretions. Sometimes depictions not portraying an actual case of sexual child abuse (e.g. simulated computers animation, so-called "morphing") are also penalised.[307]

Some legal systems cover visual depictions of pornography. Other countries include sound recordings as well. In several legal systems it has been discussed to what extent depictions on computer networks may be treated the same as depictions on paper.[308] Some countries have amended their respective laws to include pornographic material on computer storage devices.[309] Therefore, most countries currently penalise storing pornographic material in computer systems on discs and tapes.[310] Thus, there is consensus that depictions which are illegal on paper should also be illegal if stored and used on computers. But it is not yet possible to comment how far the penal provisions can be extended to cover mere depictions on computer screens as well as video sequences.

The punishable acts of child pornography include the dissemination, the providing with and the publishing of child pornography. Moreover, in recent years there is a trend to extend the penal provisions also to the possession of child pornography. At the moment, some countries are discussing draft bills incorporating the possession of child pornography in new penal provisions.[311] Thus, the number of countries without any provisions against the possession of child pornography is decreasing. If the difficulties in prosecuting the authors of illegal contents in international computer networks continue, the trend to extend criminal liability to the "consumers" of child pornography may become even stronger.[312]

[305] E.g. Italy, Finland, and Luxembourg.
[306] *See* U. SIEBER, *op. cit* p. 93.
[307] E.g. Canada and Germany.
[308] U. SIEBER, *op. cit* p. 93.
[309] E.g. Germany, UK and Ireland.
[310] E.g. Germany, Denmark and Norway.
[311] E.g. Belgium, Austria and USA.
[312] *See* U. SIEBER, *op. cit* p. 93.

2.2 The International Dimension

Several international and supranational organizations have recognized the inherently transborder nature of cybercrime, the ensuing limitations of unilateral approaches and the need for international harmonization of technical, legal and other solutions. [313] The main actors in this field are the Organization for Economic Cooperation and Development (OECD), the Council of Europe, the European Union and – recently – the P8 and the Interpol. In addition, the UN, WIPO and GATS have also played an important role. These international and supranational organisations have significantly contributed to the harmonisation of criminal law as well as of underlying civil and administrative law in all of the above-mentioned areas of computer-related criminal law reform.[314]

The first comprehensive inquiry into the penal law problems of computer related crimes on international level was initiated by the OECD.[315] In 1983, a group of experts recommended that the OECD take the invitation in trying to achieve the harmonization of European computer crime legislation.[316] Thus, the OECD carried out from 1983 to 1985, a study of the possibility of an international harmonization of criminal laws to address computer related crimes. [317] The study resulted in a 1986 report, Computer Related Crime: Analysis of Legal Policy which surveyed existing laws and proposals for reform and recommended a minimum list of abuses that countries should consider penalizing by criminal law. [318]

From 1985 until 1989, the select Committee of Experts on Computer Related Crime of the Council of Europe discussed the issues raised by cybercrime and drafted recommendation 89(9) , which was adopted on September 13, 1989. This recommendation emphasized the importance of an adequate and quick response to the newly challenge of cybercrime. [319] In the guidelines of for national legislatures to review enhance their laws, the Recommendation featured a 'minimum list' of necessary candidates of such crimes to be prohibited and prosecuted by international consensus, as well as an 'optional list' that describes prominent offences on which international consensus would be difficult to reach. [320]

---

[313] M. D. GOODMAN and S. BRENNER, *op. cit.* p. 165.
[314] *See* U. SIEBER, *op. cit* p. 33.
[315] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 165.
[316] *See* U. SIEBER, *op. cit* p. 33.
[317] *See* United Nations Manuel on the Prevention and Control of Computer Related Crime, § II (c) (2) – 117 (1995).
[318] *Id.*
[319] *See* Council of Europe, Recommendation no. 4(89) 9 of the Committee of Ministers to Member States on Computer-Related Crime.
[320] *Id.*

In 1990, the English United Nations Congress on the Prevention of Crime and Treatment of Offenders addressed the legal problems posed by cybercrime. [321] It produced a resolution which called for Member States to intensify their efforts to combat computer-related crimes by modernizing their national legislations, improving security measures and promoting the development of comprehensive international framework of guidelines and standards for prosecuting these crimes in the future.[322] Two years later, the Council of the OECD and 24 of its Member countries adopted a Recommendation of the Council Concerning Guidelines for the Security of Information Systems intended to provide a foundational information security framework for the public and private sectors. [323] The *Guidelines for the Security of Information Systems* were annexed to the Recommendation.[324] This framework includes codes of conduct, laws and technical measures. They focus on the implementation of minimum standards for the security of information systems.[325] However, these *Guidelines* request that Member States establish adequate penal, administrative of other sanctions for misuse and abuse of information systems.

In 1995, the U.N published the *United Nations Manuel on the Prevention and Control of Computer Related Crime*. [326] This Manuel studied the phenomenon of computer-related crimes, substantive criminal law protecting privacy, procedural law, and the needs and avenues for international cooperation. [327] In the same year, the Interpol organised its first Conference on Computer Crime. [328] This conference confirmed that a high level of concern existed in the law enforcement community over the propagation of computer crime. Later on, Interpol held several conferences on the same theme. In the same year also, the Council of Europe adopted Recommendation No. R (95)13 of the Committee of Ministers to Member states, spelling out the principles that should guide states and their investigating authorities in the domain of IT. [329] Some of these principles cover search and seizure, obligation to co-operate with investigating authorities, the use of encryption and international co-operation. [330]

---

[321] *See* U. SIEBER, *op. cit.*
[322] *See* Eighth U.N Congress on the Prevention of Crime and the Treatment of Offenders. Doc. A/CONF.144/L.11 of 4 September 1990 section 2.
[323] On this point see OECD Recommendation on the Council concerning Guidelines for the Security of Information Systems [1992].
[324] *See* OECD, *Recommendation of the Council Concerning Guidelines for the Security of Information Systems* [1992].
[325] *Id.*
[326] *See* United Nations Manuel on the Prevention and Control of Computer Related Crime.
[327] *Id.*
[328] *See* U. SIEBER, *op. cit.*
[329] On this point see, *Council of Europe adopted Recommendation No. R (95)13 of the Committee of Ministers to Member states*, [1995].
[330] *Id.*

On April 24, 1997, the European Commission adopted a resolution on the European Commission's 'communication on illegal and harmful content on the Internet, supporting the initiatives undertaken by the Commission and stressing the need for international co-operation in various areas, to be initiated by the Commission.' [331] One year later, the European Commission presented the European Council with a report on computer-related crime it had contracted for.[332]

Some years later, the Council of Europe's Committee of Experts on Crime in Cyber-Space took his assignment to heart, preparing a Draft Convention on Cybercrime. [333] The preparation of this Convention was a long process; it took four years and twenty-seven drafts before the final version, dated, May 25, 2001 was submitted to the European Committee on Crime Problems at its 50th Plenary Session, held June 18-22, 2001.[334] Chapter II of this Convention contains the provisions that are relevant to the issues under consideration in this article. This Chapter is divided into two sections: Section 1 deals with 'substantive criminal law'; Section 2 deals with 'procedural law'. According to the Explanatory Memorandum accompanying the Draft Convention, Section 1 seeks 'to improve the means to prevent and suppress computer-or computer related crime by establishing a common minimum standard of relevant offences'. [335]

Parties to the Convention would agree to adopt such legislative and other measures as may be necessary to establish' certain activities of cybercrimes under their 'domestic law'.[336] According to Section 1 of Chapter II of the Convention, these activities are: (1) *Offences against the confidentiality, integrity and availability of computer data and systems*; (2) *Computer-related offences*; (3) *Child pornography*; (4) *Offences related to infringements of copyright and related rights*; (5) *provisions governing the imposition of aiding and abetting and corporate liability.*

From their part, the G8, held in May of 2000 a cybercrime conference to discuss 'how to jointly crack down on cybercrime'. [337] This conference brought together about 300 judges, police, diplomats and business leaders from the G8 states. It drafted an agenda for a follow-up

[331] *See* U. SIEBER, *op. cit.*
[332] *See* Communication From the European Commission of the Council and the European Parliament Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer Related Crime, [2000].
[333] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 171.
[334] *Id.*
[335] *See* the Convention at : <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.
[336] *Id.*
[337] *See Group of Eight Meets to Discuss International Cooperation on Cybercrime*, at: <http://www.computing.co.uk/news/1101275> (visited 06/04/2005).

summit to be held in July. [338] At the July, 2000 summit, the G8 issued a communiqué which declared, in pertinent part, that it 'would take a concerted approach to high-tech crime, such as cybercrime, which could seriously threaten security in the global information society'. [339] The communiqué noted that the G8 approach to these matters was set out in an accompanying document, the OKINAWA Charter on Global Information Society. [340]

2.3 Additional Strategies to Fight Cybercrime: Suggestions for Legal Policy

Cumulatively, the national efforts and those of the international organizations have reinforced each other, achieving a nearly global attention to the problem of cybercrime and terrorism and promoting international harmonization of legal approaches.[341] National efforts to fight cybercrime tend to be a different levels sophistication and priority, but such efforts are present in at least 40 major countries. Many of them are developing specialized police capabilities thought equipment training and laws. International and supranational organizations have significantly contributed to the harmonization of criminal laws as well as of underlying civil law in all of the areas of computer related criminal law reform. The European Community's power to adopt binding directives opened a new age of legal harmonization in Europe. [342] However, a major problem in writing, enforcing, prosecuting, and interpreting cybercrime laws, is the lack of technical knowledge on the part of legislators and experts charged with these duties. Legislators, in most cases, don't have a real understanding of the technical issues and what is or not desirable- or even possible- to legislate. Police investigators are becoming more technically savvy, but in many small jurisdictions, no one in the department knows how to recover critical digital evidence. [343]

Judges, too, often have a lack of technical expertise that makes it difficult for them to do what courts do: interpret the laws. The fact that many computer crime laws use vague language exacerbates the problem. The answer to all these dilemmas is the same: education and awareness programs. These programs must be aimed at everyone involved in the fight against cybercrime, including:[344]

- Legislators and other politicians.
- Criminal Justice professionals.

[338] *See* M. D. GOODMAN and S. BRENNER, *op. cit.* p. 173.
[339] *Id.*
[340] *Id.*
[341] *Id.*
[342] *Id.*
[343] *See* D. SHINDER, *op. cit.* p. 35.
[344] On the following points see *Id.* pp. 35 and s.

- IT professionals.
- The community at large and the cyberspace community in particular.

2.3.1 Educating Cybercrime Fighters

This strategy requires that we educate and train everyone who will be involved in preventing, detecting, reporting, or prosecuting cybercrime. Even potential cybercriminals, with the right kind of education, could be diverted from criminal behaviour. The training necessary for legislators to understand the laws they propose and vote on is different from training needed for detectives to ferret out digital evidence. The latter should receive not only theoretical but hands-on training in working with data discovery and recovery, encryption and decryption, and reading and interpreting audit files and event logs. Prosecuting attorneys need training to understand the meanings of various types of digital evidence and how to best present them at trial.

The next best solution is to establish and train units or teams that specialize in computer-related crime. If every legislative body had a committee of members who are trained in and focus on technology issues; if every police department had a computer crime investigation unit with special training and expertise; and if every district attorney's office had one or more prosecutors who are computer crimes specialists we would be a long way toward building an effective and coordinated cybercrime-fighting mechanism.

Those agencies that are still lacking in such expertise can benefit greatly by working together with other more technically sophisticated agencies and partnering with carefully selected members of the IT community to get the training they need and develop a cyber-crime-fighting plan for their jurisdictions. The Internet reaches into the most remote areas of the country and the world. Cybercrime cannot remain only the province of law enforcement in big cities; cybercriminals and their victims can be found in any jurisdiction.

2.3.2 Educating Information Technology Professionals

IT professionals already understand computer security and how it can be breached. The IT community needs to be educated in many other areas:

- How laws are made. This area includes how IT professionals can get involved at the legislative level by testifying before committees, sharing their expertise, and making opinions known to members of their governing bodies.

- How crimes are prosecutes. This area includes how IT professionals can get involved at the prosecution level as expert witness.
- Computer crime awareness. An understanding of what is and isn't against the law, the difference between criminal and civil law, penalty and enforcement issues.

Thus, in order to actively engage the IT world in the fight against cyber-crime, we face the challenge of educating IT personnel in how cybercrime laws actually work to their benefit. We won't be able to do this unless, we can show IT professionals that the laws themselves are fair, that they are fairly enforced, and that they can be effectively enforced. One way IT personnel can become more familiar with and more comfortable with the legal process is though more exposure to it. Law enforcement personnel should actively solicit their help and involve them as much as possible in the fight against cybercrime, giving IT professionals a personal stake in the outcome.

2.3.3 Using Technology to Fight Cybercrime

One of the best weapons against technology crimes is technology. The IT industry is hard at work, developing hardware and software to aid in preventing and detecting network intrusions. Third-party security products, from biometric authentication devices to firewall software, are available in abundance to prevent cybercriminals from invading our system or network. Monitoring and auditing packages allow IT professionals to collect detailed information to assist in detecting suspicious activities. Many of these packages include notification features that can alert network administrators immediately when a breach occurs. Many security technologies are based o or use cryptographic techniques. An investigator might encounter encrypted data or even suspect that the existence of additional data is being concealed using steganography. An understating of how cryptography developed and how it works in the computerized environment can be invaluable in investigating many types of cybercrime.

2.3.4 Using Peer Pressure to Fight Cybercrime

One way to reduce the incidence of Internet crime is to encourage groups to apply peer pressure to their members. If cybercriminals are shamed rather than admired, some well be less likely to engage in the criminal conduct. Many teenage hackers commit network break-ins in order to impress their friends. If more technology-sizing that respect for other's property and territory in the virtual world is just as important as it is in the physical world-

hackers might be no more behind by the majority of upstanding students that are the 'bad kids' who steal cars or break into houses.

There is no doubt that some people will commit crimes regardless of peer pressure. However, this pressure is a valuable tool against many of those cybercriminals who otherwise upstanding members of the community and whose criminal behaviour online erroneously reflects the belief that "everyone does it".

2.3.5 Educating and Engaging the Community

We must educate the community at large, especially the subset that consists of the end user of computer and network systems. There are the people who are frequently direct victims of cybercrime and who all are ultimately indirect victims in terms of the extra costs they pay when companies they patronize are viticimized and the extra taxpayer dollars they spend every year in response to computer-related crimes. Law enforcement and IT professionals need to work more closely with the community to build a cyber-fighting team that has the skills, the means and the authority necessary to greatly reduce the instances of crime on the Internet.

Conclusion

Cybercrime is a persisting international evil that transcends national boundaries in a manner that renders this form of organized crime a global concern. Cybercrime may take several forms including online fraud, theft and cyberterrorism. It has been seen that amongst the major reasons that facilitate the perpetration of this crime is the globalisation of technology and the revolutionary advancement of ICTs that have impacted on criminal activity. Broadband, wireless technologies, mobile computing and remote access, Internet applications and services, software and file transfer protocols are amongst the tools utilized by cybercriminals to commit their crime. The increasing proliferation in usage of technology assisted criminal activity and cybercrime merits further attention from the global community by enacting the necessary legislative provisions and implementing effective technological and enforcement tools that reduce ICT-facilitated criminal activities. By and large, it is submitted that cybercrime should be subject to a global principle of public policy that aims at combating and preventing this form of organized crime through raising global awareness and increasing literacy rates, coordinating legislative efforts on national, regional and global levels, and

establishing a high level global network of cooperation between national, regional, and international enforcement agencies and police forces.