Santa Clara University
Professor Allen Hammond IV

LLM dissertation

The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?

Cédric J. Magnin

June 2001

OVERVIEW

TEXT *Pages 1-82*

TABLE OF CONTENTS *Pages I-V*

TABLE OF SOURCES *Pages A-C*

Introduction

During the last twenty years, smart computer users using their machine to commit crimes have fascinated the world and generated a strange feeling composed of admiration and fear.

The entertainment industry understood these emotions quickly and has therefore continuously released new books, movies and shows representing cyber-criminals in action and threatening the world behind their computer.

However, is our society facing a real threat or is it only a myth ?

If it was only a marginal phenomenon, the forty-three Members of the Council of Europe and Observers like the United States, Canada, Israel and Japan would not have drafted the first International Treaty regulating Cyber-crime which entered on June 22nd 2001 the final stage of its adoption's process and which could be opened for signature as early as November 2001.

However, is this new treaty the ultimate tool to fight crime in cyber-space ?

This paper is addressing this issue in three chapters.

The first one depicts the criminological aspects of cyber-crime by defining the phenomenon, identifying the different groups of cyber-criminals and analyzing recent statistics and cases to determin the extent of the threat that our society faces.

A second chapter focuses on the Council of Europe Convention on Cyber-crime. It begins by a presentation of the Institution and of its multilateral treaties adoption's procedure and ends with an analysis of the Convention content and critics.

The third chapter tests the efficiency of the law in general in the international crusade against cyber-crime and proposes alternative methods of combat.

Chapter 1 : What is cyber-crime ?

To understand cyber-crime and to determine how this new form of criminality should be most adequately fought, it is important to understand first its origin and the mind of the cyber-criminals. Moreover, an overview of the most important cases will help to seize the extent and thickness of the threat that cyber-crime poses to society.

A. Origin & definition

Two words are commonly found in literature: “computer crime” and “cyber-crime”.
Are these two words perfect synonyms? Not really. I would say more that they describe the same idea but at different times.
Cyber-crimes are computer crimes committed in a cyber-culture context.

1. Computer crime

Literally, a “computer crime” has two elements: “computer” and “crime”. Therefore, it involves a crime in relationship with a computer.
The relationship could involve the direct usage of a computer by the criminal as one of the first famous computer criminals did, Jerry Schneider[1] when he ripped off Pacific Telephone’s & Telegraph (PT&T) computers in 1971.
But the relationship between the crime and the computer could also be indirect: the criminal will not use a computer to commit his crime but will use someone, often innocent and not knowing at all that he’s being manipulated, to make a change in a computer system. In that

1 Buck Bloombecker, *Spectacular Computer Crimes* [Dow Jones-Irwin, 1990, p.6]

case, the computer criminal will not use his computer himself; he will only manipulate a key computer user.

This is what the same Jerry Schneider did during the Dan Rather TV Show “60 minutes” in 1976 when he robbed a bank live while the audience was watching!

Basically, he used the bank account number of Dan Rather, printed on his bankcard, called the credit department of his bank and asked the clerk to change the credit limit from $500 to $10’000. Since the bank account authorized with a “no question asked” policy the retrieval of the credit limit’s amount only by using the bank card and since the only information necessary to reproduce it was the account number, Jerry could have walked out of Dan Rather’s Show and immediately retrieve the $10’000. --!

During the 1970’s and until the middle of the 1980’s, only a few people owned computers. As a result, only sensitive areas like banks and airports that already required computer services due to their complexity were using computers.

However, this was already enough for potential cyber-criminals to commit a crime. Meanwhile, only a few computer crimes were reported during that period. Even if the big number of unreported computer crimes is taken into account, one key element was not yet present to make computer crimes becoming a more serious issue : the existence of a culture, of an ideology, of a parallel world in which cyber-criminals could be united and grow. This element appeared in the early 1980’s and was called the “cyber-punk” movement, today “cyber-culture”.

2. From Cyberpunk to cyber-culture

Cyberpunk was limited in the early 1980's to a movement in science-fiction literature. However, the context of a world more and more dependent of technology and the success of its literature helped the movement to expand into a vast phenomenon known nowadays as "cyber-culture".

a) Science-fiction literature

The words 'cyber' and 'punk' emphasize the two basic aspects of cyberpunk: technology and individualism. The meaning of the word 'cyberpunk' could be something like 'anarchy via machines' or 'machine/computer rebel movement'.

This word first appeared as the title of a short story "*Cyberpunk*"[2] by Bruce Bethke, published in "AMAZING" science fiction stories magazine volume 57, number 4, in November 1983. The word was coined in the early spring of 1980, and applied to the "bizarre, hard-edged, high-tech" science fiction emerging in the eighties. The story itself is about a bunch of teenage hackers/crackers.

In calling it "cyberpunk", Bethke was actively trying to invent a new term that will express the juxtaposition of punk attitudes and high technology. His reasons for doing so were purely selfish and market-driven: He wanted to give his story a snappy, one-word title that people would remember.

2 Bruce Bethke, *Cyberpunk* [AMAZING Science Fiction Stories, Volume 57, Number 4, November 1983; http://www.cyberpunkproject.org/lib/cyberpunk/]

In the mid-1980s, the cyberpunk science-fiction movement had emerged with Mirrorshades, a collection of short stories edited by Bruce Sterling[3]. The author also edited the movement's magazine, *Shaved TruthSchizmatrix and the artificial kid.*

b) Emergence of the cyber-culture

In the early 1990's, cyberpunk was expanding across the boundaries of science fiction literature and Time magazine[4] described the phenomenon in its March 1st 1993 issue:

"With virtual sex, smart drugs and synthetic rock'n'roll, a new counterculture is surfing the dark edges of the computer age."

"They call it cyberpunk, a late-20th century term derived from CYBERNETICS, the science of communication and control theory, and punk, an antisocial rebel or hoodlum. Within this odd pairing lurks the essence of cyberpunk's international culture - a way of looking at the world that combines infatuation with high-tech tools and disdain for conventional ways of using them. Originally applied to a school of hard-boiled science-fiction writers and then to certain semi-tough computer hackers, the word cyberpunk now covers a broad range of music, art, psychedelics, smart drugs and cutting-edge technology."[5]

Since the mid-1990's, the exponential development of the Internet has helped transforming the dream of a networked humanity into reality. The importance of computers and of the modem that connects its user to the entire world has put more and more spotlight into the

3 Bigthinkerstaff, *Bruce Sterling* : *this week's big thinker*, [TechTv.com, December 6th, 2000 ; http://www.techtv.com/bigthinkers/thisweeksbigthinker/story/0,23008,3015031,00.html]
4 www.time.com
5 "The Cyberpunk Project" editor, *The Coining* [April 3rd 2000 ; http://www.cyberpunkproject.org/idb/cyber_punk.html]

cyberpunk movement. So much light from so many different people has had the effect to transform the movement into a culture called nowadays “cyber-culture”.

Meanwhile, the idea of the movement remains the same.

Recent science-fiction novels show more than before the idea that moves the mind of the “cyber-culture” adepts:

Bruce Sterling, in his 1996 novel “Schizmatrix” describes “an interplanetary civilization divided between cyborg technocrats and bioengineered shapers.”[6] .

Greg Egan, in his 1999 novel “Diaspora “ writes about “posthuman life, nanotech, picotech and femtotech entities. It begins in the year 3000 when most of the human population has either uploaded into the net, become cyborgs or highly modified posthumans, and then gradually expands it scope towards more and more grandiose themes”[7].

B. The cyber-criminals

Motives are good criteria to divide cyber-criminals into different categories.

Two groups oppose themselves: the idealists and the greed-motivated. The first ones are usually eternal teenagers with no criminal history and the second ones are usually older in their mind and often career criminals.

The idealists want to get into the spotlight with the minimum of risks and therefore are cautious not to threaten the existence of their target. Their actions are usually temporary and limited to the hacking of a very secured computer, to the spreading of a computer virus that

6 M Alan Kazlev and Anders Sandberg, *Some Books with similar themes to Orion's Arm* [http://www.kheper.auz.com/orions_arm/books/]

7 All these books and summaries are available at www.amazon.com

is usually harmless for each computer, or to the disruption of a notorious important network.

The Greed-motivated are acting for money and therefore are targeting places where they can steal some: banks and e-commerce websites. They are also unscrupulous and do not hesitate to cash the child pornography machine.

However, a third category has emerged recently and might be the most dangerous and threatening in the future: the cyber-terrorists. These cyber-criminals have usually a lot of power behind them (organized crime Mafia's and foreign hostile governments) to commit great damages and therefore they are usually looking at the economical or physical destruction of their targets.

1. The Idealists (teenagers)

a) Looking for freedom & identity

The idealists, almost all teenagers, are the group of society that adhered the most rapidly to this new "cyber-culture". The explication resides in the fact that the Internet gives them the freedom they are looking for at their age:

Within a few clicks, they can communicate with the world and explore new horizons. They don't have to wait to get a telephone or a car which still does not offer the same level of communication' deepness and intensity that the Internet does.

Moreover, they are the target of the science-fiction literature and of all the entertainment industry that has jumped quickly in the matter to seduce its audience with movies[8] like "the

8 For more information on each movie see www.imdb.com

Net" (1995), "Hackers" (1995), "Enemy of the State" (1998), "the Matrix" (1999), "Hackers 2: takedown" (2000) or "Bait" (2000).

When they decide to commit a "cyber-crime", it is usually only to be in the spotlight of the medias and to show their strength to their friends in order to rise into their local community hierarchy.

b) Their actions are globally very damageable but individually negligible

Still, their action are not damageless: the denial of service attacks that blocked a lot of important e-commerce servers in February 2000 is said to have caused high damages to these companies. More over, the "Melissa" and the "I love you" viruses that spread in the world like wildfires are said to have caused more than $1 billion of damages.

However, these numbers must be taken with caution: first of all, a $1 billion damage that affected $100 million computers worldwide means that the averages damage per computer is marginal ($10). This is usually the case with all teenagers' attacks: they target a lot of victims to be put into the media spotlight but their actual harm to each individual is relatively negligent.

c) Government should fight them through Education not Law:

These cyber-criminals are often helping society: through their highly mediatized and individually harmless actions, they help important organizations to discover their high-tech security holes that other types of Cyber-Criminals could use to commit real harm. Most of

them are never caught and the few ones that are arrested do not stay long in custody and usually end up by becoming computer security consultants!

Recent studies tend to demonstrate that criminalizing their action will not prevent them to act[9]. On the contrary, it might stimulate them: they are looking for danger and if their acts are criminalized the adrenaline will get even higher when they will commit a cyber-crime.

Therefore, before legalizing cyber-crime with mandatory minimum punishments (6 month mandatory minimum in the US[10]) like it is the case with drug crimes in the United States, one should be cautious: these kind of legislation could harm kids that are not a real danger to society.

Moreover, if the goal of cyber-crime legislation is to eradicate cyber-crime, it might well eradicate in stead a whole new culture based on fundamental rights such as freedom of speech and therefore could do more harm than good to the next generation in quest of new dreams and identities.

A much better tool to prevent their action is by investing in education[11]. Schoolteachers, lecturers have an active role to play to make them understand that cyber-crime can harm.

The FBI has already started such a program called “cyber-citizen”[12].

---

[9] Raju Chebium, *Experts say more laws won't stop computer hackers* [CNN Interactive, May 8th 2000 ; http://www.cnn.com/2000/LAW/05/05/love.bug/index.html]

10 Paul Johnson, *Net frauds go unpunished* [DIBS Computer Forensics, November 2000 news ; http://www.computer-forensics.com/news/welcome.html]

11 Michael Vatis, director of the FBI's National Infrastructure Protection Center, said: "One of the most important ways of reducing crime is trying to teach ethics and morality to our kids. That same principle needs to apply to the cyber world."

12 See *The Cybercitizen Partnership* [http://www.cybercitizenpartners.org]

2. The greed-motivated (career criminals)

Criminologists pretend that crime is part of our society. It has always existed and will always exist. Therefore, career criminals are just adapting themselves to a new world full of technology.

Bank robbers used to stop horses, then trains transporting goods full of dollar value. It is therefore a normal evolution that this category of cyber-criminals is now attempting to sneak in the flux of financial information transported electronically and to steal some of it.

a) Unscrupulous

This category of cyber-criminals is dangerous because they are usually unscrupulous and are ready to commit any type of crime, as long as it brings them some cash.

This is why they are at the origin of child pornography often falsely called cyber-porn which englobes legal and illegal pornography on the Internet.

This type of unscrupulous cyber-crime must be prevented. Usually current legislation is enough and just need small adaptation because, as mentioned above, the crime is still the same but it uses a different technology. However, in some areas, new laws need to be adopted otherwise the criminals will escape conviction.

This category is the primary target of each new legislation or international convention.

For example, the United States have already adopted new extensive legislation on the matter of Child Pornography: Federal legislation has been enacted[13] to force any individual or corporation doing online business involving models, actors, actresses and other persons who

13 U.S.C. Title 18, Section 2257

appear in any visual depiction of sexually explicit conduct appearing or otherwise contained in or at a website to keep a record of the proof that they were over the age of eighteen years at the time of the creation of such depictions.

Moreover, the new Council Of Europe Convention on Cyber-crime is addressing the matter at his article 9, the only disposition related to website content[14].

b) Often affiliated with organized crime

They are usually well organized and know how to escape law enforcement agencies. They prefer offshore or low level of enforcement locations to establish their headquarters.

They can act on their own, as mercenaries with organized crime or as "cyber-spy" for foreign governments.

c) Potentially very dangerous and damageable for society

These cyber-criminals are committing important damages and their unscrupulousness, particularly in child pornography and cyber-gambling is a serious threat for society.

Concerning the damages, examples are here to show that the threat is real: the victims of the European bank of Antigua[15] are said to have lost more than $10 million. Moreover, The

14 However, on June 22nd 2001, the European Committee on Crime Problems decided to complement the Convention by an additional protocol making it a crime to spread racist and xenophobic propaganda through computer networks. The United States were strongly opposed to it, arguing that it would violate the first Amendment to the US Constitution addressing Free Speech. See : Dmitri Marchenkov and Sabine Zimmer, *Council of Europe's Committee on Crime Problems approves final draft of Cyber-crime Convention* [Council of Europe Press Service, June 22nd 2001 ; http://press.coe.int/cp/2001/456a(2001).htm]

recent theft of a very valuable trade secret: the source code of the popular Microsoft Windows Exploitation System by a Russian based hacker could be extremely damaging for the company if rumors pretending that the hackers could use the code to break all firewalls and penetrate remotely every computer equipped with Windows were confirmed. Another usage could be the selling of the code to competitors.

The money damages appear to be lower than the ones caused by the teenagers when they send a virus[16] but it is not true: the damage per victim is usually much higher and potentially economically destructive.

d) International cooperation and Law harmonization is the best way to fight them

These cyber-criminals can't be fought by education: they will not behave because most of them are already career criminals.

The only appropriate tool to fight them is by enacting new Laws, harmonize international legislations and encourage coordination and cooperation between national law enforcement agencies[17].

---

15 see below, page 21, under *Electronic offshore-banking, money laundering and fraud: The collapse of the online European bank of Antigua*

16 See below, page 23 under *Personal Files remote destruction and computer freezing: E-mail Virus "I love you"*

17 The 2001 Council of Europe Convention on cyber-crime is trying to achieve these goals

3. The cyber-terrorists

a) The newest and most dangerous category

This category is the newest as well as the potentially most dangerous.

Their primary motive is usually not only money but also a specific cause that they defend.

The common belief that they exist only in the imagination of literature or movie writers needs to be revised.

So far, only the Greed-motivated or the Idealist cyber-criminals have dared to attack National vital infrastructure and have therefore not caused destructive damages.

But the mentality and an ever more powerful, costless and accessible technology as well as our increasing dependency on computers have turned this remote science-fiction threat into close reality.

Very serious cases like the shutdown of an airport tower control during 6 hours, the hacking of California government computers responsible to manage the delivery of electricity or the daily attack and penetration of federal agencies computer servers such as the National Security Agency (N.S.A.) and the Department of Defense (DOD) show the weaknesses and fragility of the National vital infrastructures.

b) The most appropriate way to fight them is by funding national security agencies and reinforcing global networks surveillance

These threats are real and the United States has already cited the billionaire Usama Bin Laden as being one of the potential most dangerous cyber-terrorists.

This person is said to possess its own satellite communication system, has been convicted of several mass murders including the bombing of two U.S. embassies and is the most wanted fugitive listed on the famous FBI list[18] . If he were arrested in the U.S. without committing any form of cyber-crime, he would still face the death penalty for his past actions.

Therefore, it is unlikely that adopting any kind of law will prevent this potential cyber-terrorist to perpetrate his criminal actions.

The only way to prevent the action of potential cyber-terrorists like him is to massively fund global surveillance at a national level and this is what the U.S. Government is doing since 2000[19].

C. The reality of the threat

Different elements are showing the rapid development of this new form of threat.

1. Alarming Cyber-Criminology statistics and prediction studies

Recent surveys[20] suggest that cyber-crimes will continue to increase both in number and severity over the coming years, particularly since cyber-criminals often have access to the newest technology, can reach vast numbers of victims, and can readily avoid detection. A

18 www.fbi.gov
19 see below under “evidence of emerging cyber-terrorism”

20 U.S. Department of Justice : Computer Crime and Intellectual Property Section, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cyber-crime (Draft 24REV2)* [December 1st, 2000 ; http://www.cybercrime.gov/COEFAQs.htm#Q4]

survey conducted by the Computer Emergency Response Team [CERT][21] Coordination Center at Carnegie-Mellon University indicates a 183% increase in the number of computer attack incidents from 1998 to 1999.

In addition, the Spring 2000 Computer Security Institute ("CSI")/FBI Computer Crime and Security Survey projected monetary losses exceeding $265,000,000 in 2000, up from $100,000,000 in 1997 (in all likelihood, these numbers are significantly underestimated because, while 74% of survey respondents acknowledged financial losses due to computer crimes, only 42% could quantify those losses).

A more recent study by Computer Economics[22], an independent research institute, indicates that the dissemination of the "I Love You" virus, and subsequent copycat viruses, already resulted in $6.7 billion in damages to businesses worldwide only in the first semester of the year 2000. According to Computer Economics, virus attacks also resulted in more than $12.1 billion in damages to businesses during 1999.

In addition to the damage resulting from attacks on computer networks, criminals around the globe also are increasingly using computers to reach across borders to commit traditional crimes, including fraud, copyright infringement, distribution of child pornography, and other crimes.

For example, in 1998, Vladimir Levin was convicted of hacking into a major international bank, Citibank, from Russia and transferring $12 million out of accounts located around the

21 http://www.cert.org/
22 www.computereconomics.com

world[23]. More recently, one study estimated that credit card fraud cost merchants $400 million in 1999.

The Business Software Alliance ("BSA") also estimates that software piracy cost the U.S. some 109,000 jobs and $991 million in tax revenue in 1998; moreover, Computer Economics research shows that, by 2005, over $112 billion in software, music, video, and text will be pirated over the Internet.

The Internet also has made it much easier for pedophiles to distribute child pornography and lure children. Prosecutions of child pornography and luring cases in the United States have increased by 10% every year since 1995; in 1999, the U.S. Department of Justice prosecuted over 400 such cases, many of which were international in scope.

2. Rapid growth of Computer Security expenses

Also, statistics show that the amount spent by U.S. companies on computer security is rising rapidly.

According to Forrester Research, companies with top revenue greater than $100 million in the United States were spending at the end of the year 2000 $213 of every $1 million of top-line revenue on security. That's two-hundredths of one percent of top-line revenue[24].

This is another evidence that the society is taking more seriously than before a potential cyber-crime threat.

---

23 See Michelle Delio , *Inside Russia's Hacking Culture* [WiredNews, March 12th 2001 ; http://www.wired.com/news/infostructure/0,1377,42346,00.html]

24 Michael Bertin, *The new security threats* [http://www.zdnet.com/zdhelp/stories/main/0,5594,2669953-1,00.html]

3. Evidence of emerging cyber-terrorism

a) Since 1999, $1.46 billion allocated in the U.S. budget to fight the threat

Recently[25], U.S. President George W. Bush massively pursued the plan set up by his predecessor on January 22nd 1999. That day, U.S. President Bill Clinton allocated $1.46 billion to fight cyber- terrorism. The fund went to implement a plan to protect the nation's computer systems from terrorists[26]. In particular, the money funded the following initiatives:

- Research toward better methods to detect computer hackers.
- The development of detection networks, first for the Department of Defense and later other key agencies, to signal other systems when an intruder is detected in one.
- An information center for the private sector to help it protect against invasion of its computer systems.
- Building up the ranks of government computer experts able to deal with a terrorist crisis.

25 Declan McCullagh, *Cashing in on cyber-crime* [WiredNews, April 14th 2001 ; http://www.wired.com/news/politics/0,1283,43064,00.html]
26 The Associated Press, *Clinton proposes anti-terrorism plan* [CNN Interactive, January 22nd ; http://www.cnn.com/ALLPOLITICS/stories/1999/01/22/clinton.terrorism/]

b) One hundred countries possibly working now on techniques to penetrate the U.S. information infrastructure

According to an interview conducted by CNN Justice correspondent Pierre Thomas[27], every day, the U.S. Pentagon is the target of as many as 100 hacking attempts. This is another evidence that electronic terrorism looms as a new way for criminals to threaten global security.

“According to the National Security Administration, there are over a hundred countries that are working on techniques to penetrate our information infrastructure," said U.S. Senator Jon Kyl, R-Arizona. "Many of them are aimed at the Defense Department and high security areas in both the private sector and the government, so it's a very serious threat."

This is why the U.S. government is working to prepare itself against electronic assaults, much the way it is preparing against other forms of terrorism.

c) All vital infrastructures handled by computers

According to Richard Clark, the coordinator for security, infrastructure, protection and counter-terrorism at the U.S. National Security Council, our dependency on computers will make us increasingly vulnerable in the near future.

"They (computers) run our electric power grid, out telecommunications network, they run our railroads, our banking system, and all of them are vulnerable, at some level, to some degree to information warfare, or cyber-terrorism," Clark said.

---

27 Pierre Thomas, *Governments ready to fight cyber-crime in the new* millennium [CNN interactive, January 2nd 2000; http://www.cnn.com/2000/TECH/computing/01/02/cyberterrorism/#1]

"There really is a broad spectrum of people, groups and countries that engage in cyber-attacks as a general matter for different purposes, " said Michael Vatis, director of the National Infrastructure Protection Center at the FBI.

d) FBI computer crime case load doubling every year

According to CNN Justice correspondent Pierre Thomas, Terrorists, hostile nations, criminals, hackers all present a wide variety of threats and create new pressure for intelligence, defense and law enforcement around the world. The FBI computer crime caseload has doubled each of the last three years. In October 1999, the FBI reported 800 pending cases.

Added Clark, "There are governments that are building units, military units and intelligence units, to engage in information warfare. They are developing capabilities, they are building the units, and in some cases they seem to be doing reconnaissance on our computer networks."[28]

e) A new kind of threat for the United States

Moreover, Terrorism is a new threat in the United States: in Europe, it has existed since a long time and has materialized in airplane hijacking, Officials kidnappings, and public places bombings.

But cyber-terrorism could imply shutting down the electricity in key areas such as hospitals, airports or sensitive governmental agencies, sending computer bombs to key computers that

28 ibidem

could destroy National security information's, sending computer viruses that could activate nuclear missile launch[29] remotely, sending falsified computer orders to remote military ships and therefore starting a war, stealing remotely vital economic trade or military secrets[30] stored on computers, changing remotely information in vital computers such as hospital patients files, etc.

f) A convention to fight cyber-terrorism is being drafted by key Scholars

Scholars are already studying the matter. A recent colloquium organized by the Hoover Institution at Stanford University and a proposed draft of a "Proposal for an International Convention on Cyber Crime and Terrorism"[31] is here to prove that urgent measures need to be taken.

g) An International wealthy potential cybert-terrorist: The Usama Bin Laden cyber-threat is real

Usama Bin Laden is the most wanted fugitive in the world: The FBI offers $5 million for any information leading directly to its capture.

---

29 scenario of the movie "war games"

[30] The October 2000 Microsoft case depicted below and involving the remote theft by a Russia based hacker of Microsoft core software "Windows" source code is a good example.

31 The Hoover Institution,The Consortium for Research on Information Security and Policy (CRISP), The Center for International Security and Cooperation (CISAC), Stanford University, *A Proposal for an International Convention on Cyber Crime and Terrorism* [August 2000 ; http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm]

According to declarations by the U.S. Justice Department and by the President of the United States, this person represents a threat to national Security not only because of his past embassy bombings actions[32] but more because his means are wide enough to organize a potentially devastating cyber-terrorism attack against the USA.

For instance, by using techniques such as "electronic bombings", he could shut down key National infrastructures like airports, electric power, hospital computer networks and the result could be devastating.

4. Cyber-crimes affects all sectors of society, private and public and under various shapes

Recent cases and events have proven that cyber-crime threats are real, diversified, growing, very dangerous and potentially damageable:

a) Electronic offshore-banking, money laundering and fraud: The collapse of the online European bank of Antigua

In 1997, the Bank of England and the State of Idaho requested the authorities of the Caribbean island of Antigua to investigate the headquarters of the European Union Bank ltd., in activity as an offshore bank since 1994. However, it was too late and the two Russian

32 Hans H. Chen and David Eberhart, *Web of Terror : Bin Laden's International Terror Network* [ABPNews, 2000 ; http://www.apbnews.com/newscenter/majorcases/binladen/index.html]

criminals had already left with an illegal benefit estimated to be at least $10 millions when the Antiguan Law Enforcement Officers penetrated the bank office.

Their bank was the first one operating in cyber-space and proposed "exceptional interest rates of 9.91% in a safe and tax exempt environment". The bank was targeting specifically money launderer and tax evaders. Clients could open multiple accounts with their identity known only by the banker and also coded account operated by password rather than by signature. Moreover, customers could also set up a corporation online under Antigua corporate law, which does not require the disclosure of shareholders or beneficial owners[33].

b) Vital Infrastructure disruption: Airport tower control disabled by a teenager computer attack

The March 1997 Airport tower control computer attack[34] case, initiated by a Massachusetts teenager, could have caused terrible death and damage, since the teenager successfully severely disabled telecommunications at a regional airport during 6 hours, in the process cutting off vital services to the airport's control tower and disabling incoming planes from turning on runway lights. He also disrupted telephone service in Rutland, Massachusetts.

---

33 Pr. Ernesto Savona, "*Offshore and Internet: a risky pair* [Transcrime:Research Center on Transnational Crime, University of Trento, Italy, April 26th 2000; www.jus.unitn.it/transcrime and http://www.gamblingmagazine.com/articles/21/21-144.htm]

34Paul Festa, *Airport hack raises flags* [CNETNEWS, March 19th 1998 ; http://news.cnet.com/news/0,10000,0-1005-200-327600,00.html]

c) Denial of Service attack: E-Commerce websites

The February 2000 denial of service attacks[35] was initiated by a single man (teenager!) in Canada, who slowed down dramatically the most famous e-commerce servers like amazon.com, ebay, yahoo! or CNN. These servers could almost not sell their products any more during a few days. They claimed to have globally endured more than $1 billion in damages.

d) Personal Files remote destruction and computer freezing: E-mail Virus "I love you"

The I love you Virus sent in May 2000 by one person in the Philippines who was finishing his P.H.D. in computer science spread out like a wildfire worldwide through popular e-mail softwares like Microsoft Outlook Express and destroyed low important computer files in millions of hard-drives in a matter of days. It is said to have caused more than $6 billion of damages worldwide, most of it in the USA[36],

e) Stock crash due to false Information broadcasted on key sensitive financial news agency: Emulex

In August 2000, a man based in New York managed to have a false information broadcasted on key financial news networks. The information pretended that Emulex, a company listed

---

35 For a technical description, see CNET News.com Staff, *How a denial of service attacks works*, [CNETNEWS, February 9th 2000 ; http://news.cnet.com/news/0-1007-200-1546362.html]

36 Raju Chebium, *Experts say more laws won't stop computer hackers* [CNN Interactive, May 8th 2000 ; http://www.cnn.com/2000/LAW/05/05/love.bug/index.html]

on the NASDAQ Stock market, was experiencing huge losses and that forecast for the next quarter were so bad that the CEO was resigning. Traders, who follow very closely all information published on the financial networks, immediately sold massively the stock, which dropped more than $2.5 billion in market value. Very quickly, Emulex made a statement denying the information and 30 minutes after the dropping, the stock had recovered all its loss.

Still, the cyber-criminal had enough time to make a benefit of $250'000[37] and was arrested a few days later.

f) Hacking of Vital corporation software source code: Microsoft Windows source code theft by a Russia based hacker

The October 2000 Microsoft Windows source code theft and hacking attack, potentially dangerous for the 95% computer users in the world relying on the MS operating system and potentially extremely damageable for the Company was operated by "an unknown hackers with a St. Petersburg (Russia) e-mail address who has accomplished what a U.S. Justice Department antitrust lawsuit failed to do: extract the secret blueprints for Microsoft's Windows operating system."[38] .

The Hacker penetrated key Microsoft servers, downloaded the source code and e-mailed it to a St. Petersburg IP address.

---

37 Bill Mann, *Arrest Made on Emulex Case* [The Motley Fool, August 31st 2000 ; http://www.fool.com/news/2000/emlx000831.htm]

38 Melissa Akin, *Microsoft Hacked Via St. Petersburg* [The Moscow Times, October 28th 2000 ; http://dev.themoscowtimes.com/stories/2000/10/28/001.html]

Microsoft thinks that this is an industrial espionage case and that one of its competitor has bought the code.

Its chief executive, Steve Ballmer has commented that: "They did in fact access the source codes. You bet this is an issue of great importance.

"I can also assure you that we know that there has been no compromise of the integrity of the source codes, that it has not been tampered with in any way." Microsoft spokesman Rick Miller added: "We're still looking into it. We're still trying to figure out how it happened. This is a deplorable act of industrial espionage, and we will work to protect our intellectual property." [39]

g) Intellectual property fraud using new circumventing technologies: the DVD case

The DVD case[40] "will have wide-ranging ramifications for the future of publishing on the Internet and for copyright law"[41].

On May 2nd 2001, the case was still pending in the Federal Appeal court and experts say it is likely the case will go to the Supreme Court.[42]

---

39 www.microsoft.com
40 Lynn Burke , *DVD Case: It's a Linux Thing* [WIREDNews, January 28th 2000 ; http://www.wired.com/news/politics/0,1283,33925-2,00.html]
41 David M. Ewalt, *Federal Court Hears DVD Case Appeal* [InformationWeek, May 2nd 2001 ; http://content.techweb.com/wire/story/TWB20010502S0002]
42 ibidem

This is the first case that analyzes deeply the October 28th 1998 U.S. Digital Millennium Act[43] [DMCA] prohibiting the usage of circumventing technologies that in reality perpetrate a copyright infringement.

The clash began in January 2000, when the Motion Picture Association of America[44] sued a famous online magazine called "2600" and known as "the Hacker Quarterly"[45], whose operator, Eric Corley, also known as Emmanuel Goldstein, the leader on the underground in George Orwell's 1984 famous novel, is viewed as the leader in the Hacker Community.

He was sued for publishing and linking to the DeCSS code, a program that strips encryption from DVD movies. (DVDs are encrypted using Content Scrambling System, and the program that decrypts CSS is called DeCSS.) 2600 argued that the program is a legitimate tool, created to allow Linux users to watch legally purchased movies on their computers. But the MPAA asserted that DeCSS is a pirating tool that facilitated the illegal copying of movies.

On August 17th 2000[46], New York Federal District Judge Lewis Kaplan sided with the movie industry in that case, forbidding 2600 from publishing or linking to the DeCSS code.

In turn, lawyers for the movie industry argued that DeCSS is primarily a tool for pirating movies, and that 2600 should be forbidden from helping to distribute it. "DeCSS is a digital crowbar created for the sole purpose of ripping open DVDs ... for fair use perhaps, but

---

43 U.S. Copyright Office, *The Digital Millennium Copyright Act* [www.loc.gov/copyright/legislation/dmca.pdf]
44 www.mpaa.org
45 www.2600.com
46 http://www.2600.com/dvd/docs/2000/0817-decision.pdf

more likely for creating copies," said assistant U.S. attorney Daniel Alter, representing the U.S. Justice Department, which has intervened in the case on the side of the MPAA.

Following the hearing, civil-liberties groups expressed their disagreement on the case with Hollywood's Entertainment giant Corporations. "The fundamental issue here is who is responsible for a criminal act," said John Gilmore, co-founder of the Electronic Frontier Foundation, a non-profit public-interest group representing 2600. "Is it the person who committed the act or the person who provided the tool?"[47]

h) Online fraud: The Experian report and the FBI Operation “Cyber loss”

An interesting report published by a credit agency called Experian[48] has shown that Nine out of 10 Internet frauds in the UK go unpunished.

According to the report, Net shops are encouraging thieves by not reporting crime and failing to cross-check credit card addresses with delivery addresses, the report said.

Just six out of 10 businesses said they bothered to report fraud, and more than half of those that did said the police failed to follow up complaints.

Experian said that consumers were protected from risk because their credit card companies were liable for losses, but added that the damage to Internet shops was significant, amounting to 10 per cent of total sales at some sites.

---

47 David M. Ewalt, *Federal Court Hears DVD Case Appeal* [InformationWeek, May2nd 2001, http://content.techweb.com/wire/story/TWB20010502S0002]
48 http://www.experian.com/

On the other hand, the May 23rd 2001 "Operation Cyber Loss"[49] organized by the FBI and the U.S. department has the goal of arresting the criminals who harmed 56'000 victims suffering cumulative losses of $117 million in cases involving on-line auction fraud, systemic non-delivery of merchandise purchased over the Internet, credit/debit card fraud, identity theft, various investment and securities frauds, multi-level marketing and Ponzi/Pyramid schemes. Approximately 90 subjects have been charged as a result of Operation Cyber Loss for wire fraud, mail fraud, conspiracy to commit fraud, money laundering, bank fraud, and intellectual property rights (software piracy).

Combining the "cyber-loss" FBI operation and the report published by Experian helps to evaluate the real annual amount of online fraud, probably much higher than the declared $117 million.

i) Vital infrastructure hacking: Electricity's flow handling computers hacked in California

Between April 25th and May 11th 2001, Hackers have penetrated key Californian computers handling the flow of electricity across the state. They finally did not disrupt the service[50].

The hackers' success, though apparently limited, brought to light lapses in computer security. At the target of the cyber-attack was the California Independent System Operator [Cal-ISO], which oversees most of the state's massive electricity transmission grid. Officials at Cal-ISO say that the lapses have been corrected and that there was no threat to the grid. But others

---

49 Thomas T. Kubic, FBI Deputy Assistant Director, *US Congressional statement on the Internet Fraud Crime Problems* [FBI publications, May 23rd 2001; http://www.fbi.gov/congress/congress01/kubic052301.htm]

50 Dan Morain, *Hackers Victimize Cal-ISO* [LA Times, June 9th 2001 ; http://www.latimes.com/news/state/20010609/t000047994.html]

familiar with the attack reported to the L.A. times[51] that hackers came close to gaining access to key parts of the system, and could have seriously disrupted the movement of electricity across the state.

51 www.latimes.com

Chapter 2 : The 2001 Council of Europe Convention on Cyber-crime

This Convention is entering the final phase of its adoption. It was approved by the European Committee on Crime Problems on June 22nd 2001 and is now being submitted to the Committee of Ministers which will meet in September and who will most likely approve the final draft and open the signature process as early as November 2001.

However, until this time, it can still be amended.

Moreover, the Council of Europe represents a lot of interests from many countries and non Governmental organizations.

Therefore, in a first section, the Institution of the Council of Europe and its treaty's adoption procedure will be analyzed. In a second section, focus will be made on the Convention content and critics.

A. The Institution of the Council Of Europe [COE]

1. Generalities

The Council of Europe (hereafter [COE]) consists of 41 member States, including all of the members of the European Union. It was established in 1949 primarily as a forum to uphold and strengthen human rights, and to promote democracy and the rule of law in Europe.

Its headquarters are located at the "Palais de l'Europe" in Strasbourg (France).

Any state localized within the geographical boundaries of Europe can become a member of the Council of Europe provided that it accepts the principle of the rule of law and guarantees human rights and fundamental freedoms to everyone under its jurisdiction.

The Council of Europe's official languages are English and French, but the Parliamentary Assembly also uses German, Italian and Russian as working languages. Other languages may be interpreted during debates, under certain conditions.

Over the years, the CoE has been the negotiating forum for a number of conventions, some of them on criminal matters, in which the United States has participated.

However, the most important Convention of the Council of Europe is the *CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS*[52], opened for signature in 1950 and entered into force in 1953.

2. Origin

The origin of the COE can be retraced in a famous speech given at Zurich, Switzerland[53] by former United Kingdom Prime Minister Winston Churchill on September 19th 1946, calling for the definitive ending of the feud between France and Germany and for these two States, in friendly alliance, to constitute the nucleus of "a kind of United States of Europe". Later he was to write: "My counsel to Europe can be given in a single word: Unite!".

Following these words, a large number of private movements and organizations concerned to sponsor and foster the idea of a United Europe sprang up, arousing great interest among wide sections of the population. In 1947 these various groups decided to coordinate their activities and increase their effectiveness by jointly creating one central movement, to be known as the "European Movement".

---

[52] Council of Europe Treaties, *Convention for the Protection of Human Rights and Fundamental Freedoms* [November 4th 1950-November 1st 1998; http://conventions.coe.int/treaty/EN/Treaties/Html/005.htm]

53 Sir Winston Churchill, *September 19th 1946 Speech given at the University of Zurich, Switzerland* [http://stars.coe.fr/a_propos/Histoire/zurich_e.htm]

Finally, on the 5th of May 1949 the five Governments Members of the Brussels Treaty (1948: Belgium, France, Luxembourg, the Netherlands and the United Kingdom) and the Governments of Denmark, Norway and Sweden, Ireland and Italy signed in London the Statute of a new body, the Council of Europe.

3. Purposes

Originally an instrument of unity for the western part of Europe, the COE has today bypassed this goal and reaches a broader audience (it is formed by 43 Members State) and a global approach to specific issues affecting countries worldwide.

Specifically, the Council of Europe is an intergovernmental organization that aims:

- to protect human rights, pluralist democracy and the rule of law;
- to promote awareness and encourage the development of Europe's cultural identity and diversity;
- to seek solutions to problems facing European society (discrimination against minorities, xenophobia, intolerance, environmental protection, human cloning, Aids, drugs, organized crime, etc.);
- to help consolidate democratic stability in Europe by backing political, legislative and constitutional reform.

4. Organs

a) The Committee of Ministers

(1) Composition & voting rights

It is formed by the Minister of Foreign Affairs of each member State (or their Permanent Representatives).

Each Member has one vote.

(2) Semestrial meetings

The Committee meets at ministerial level twice a year, once in May and again in November. The meetings, known as "sessions", are normally held in Strasbourg and usually last one full day or two half days.

(3) Main Functions

It is the decision-making body of the Council of Europe.

Its main functions are Monitoring respect of commitments by member States, Admitting new member States, Interacting with the Parliamentary Assembly, establishing Political dialogue, Adopting recommendations to member States, Supervising the execution of judgments of the European Court of Human Rights and concluding conventions and agreements.

(4) The function of concluding conventions and agreements

(a) General Scope

The legal basis of the competence enabling the Committee of Ministers to conclude conventions and agreements can be found in the article 15a of the Statute creating the Council of Europe[54] : “the Committee of Ministers shall consider the action required to further the aim of the Council of Europe, including the conclusion of conventions and agreements and the adoption by governments of a common policy with regard to particular matters."[55]

This competence has resulted in the adoption of 170 treaties that have been opened for signature. The best known is the European Convention of Human Rights[56].

(b) Adoption of the final text and the explanatory report

According to the article 15a of the Statute, the text of any treaty is finalized when the Committee of Ministers adopts it.

More precisely, under Article 20, the adoption of a treaty requires cumulatively:

a two-thirds majority of the representatives casting a vote;

a majority of those entitled to vote.

---

[54] *Statute of the Council of Europe* [Council of Europe Legislative texts, May 5th 1949; http://conventions.coe.int/treaty/EN/Treaties/Html/001.htm]

55 Chapter IV of the Statute forming the COE (Articles 14 - 21), notably Article 15.

[56] See note # 52 for an online version

The same majorities are required to authorize the publication of any explanatory report.

(c) Signature and Ratification

The Committee also fixes the date that the treaty will be opened for signature.

Conventions are only binding on those States that ratify them.

b) The Parliamentary Assembly

(1) Historical importance

The Parliamentary Assembly of the Council of Europe, which held its first session on August 10th 1949, can be considered "the oldest international parliamentary Assembly with a pluralistic composition of democratically elected members of parliament established on the basis of an intergovernmental treaty"[57].

(2) Composition & voting rights

(a) Deputies, Observers and Special Guests

It is composed of 582 Deputies, 15 Observers and 15 Special Guests.

All Deputies, bearing the equally attributed title of "Representatives" or "Substitutes" of The Parliamentary Assembly are appointed by the respective national parliaments of the 43 Member States.

[57] *Council of Europe Parliamentary Assembly historical survey* [Council of Europe Official publications, June 22nd 2001; http://stars.coe.fr/index_e.htm]

Whilst in the Committee of Ministers each member state has one vote, in the Parliamentary Assembly the number of representatives and consequently of votes is determined by the size of the country. The biggest number by country is eighteen, the smallest two.

(b) Special groups of Deputies

(i) The Bureau

The President, eighteen Vice-Presidents and the Chairpersons of the political groups or their representatives make up the Bureau of the Assembly. The big countries have a permanent seat in the Bureau; the smaller countries take turns. The duties of the Bureau are manifold: preparation of the Assembly's agenda, reference of documents to committees, arrangement of day-to-day business, relations with other international bodies, authorizations for meetings by Assembly committees, etc.

(ii) The Standing Committee

The Standing Committee consists of the Bureau, the Chairpersons of national delegations and the Chairpersons of the general committees. It is generally convened at least twice a year and its major task is to act on behalf of the Assembly when the latter is not in session. Each year one of the Standing Committee meetings, together with a number of other committees, takes place normally in one of the member states.

(iii) The Joint Committee

The Joint Committee is the forum set up to coordinate the activities of, and maintain good relations between, the Committee of Ministers and the Assembly.

It is composed of a representative of each member Government and a corresponding number of representatives of the Assembly (the members of the Bureau and one representative of each parliamentary delegation of member States not represented on the Bureau).

(iv) The Secretariat of the Assembly

The secretariat of the Assembly is headed by the Secretary General of the Assembly who is elected by it for a period of five years.

Its staff is divided into the Private Office of the President, the Secretariat of the Bureau and the Joint Committee, the Table Office and Inter-parliamentary Relations, the Administration and Finance Department and the Political and Legal Affairs Department including a number of operational Divisions to cover the work of the committees.

(v) The Assembly Committees

According to its Rules of Procedure, the Assembly has ten committees with either 79 or 48 seats[58].

At times there are also ad hoc committees directly responsible to the Bureau.

In the interest of its work, a committee may also appoint one or more standing or ad hoc sub-committees, of which it shall determine the exact composition and competence at the time of their appointment. Membership must not be more than one third of the total

---

58 The ten committees and their respective amount of seats : political affairs: 79; economic affairs and development: 79; social, health and family affairs: 79; legal affairs and human rights: 79; culture science and education: 79; environment and agriculture: 79 ; immigration, refugees and demography: 79 ; rules of procedure and immunities: 48 ;equal opportunities for women and men: 48 ;monitoring: 76 . The *Bureau* and the *Standing Committee* do not count in this list.

number of members of the parent committee. Sub-committees do not adopt reports. Their decisions are submitted to the plenary committee, which appointed it.

(3) Meetings frequency

(a) The Parliamentary Assembly

The sessions of the Parliamentary Assembly are divided into four part-sessions, each lasting for about a week and held in January / February, April / May, June / July and September / October.

(b) The Committees

Committees meet either in Strasbourg or Paris, possibly in Brussels when a joint meeting with a body of the European Parliament is envisaged or in Budapest at the European Youth Center. The meetings generally last one day.

(4) Main Functions

It is the deliberative body of the Council of Europe.

It has a legislative and political role.

The legislative role is achieved by the debates over the drafting of the four possible categories of texts and the preparation of the reports submitted to the Committee of Ministers.

The Political role comes from the fact that all Deputies are also Deputies in their National Parliament, thus representing the political forces in the Member States. The Assembly is therefore often also another forum for voicing National issues.

(5) The legislative role

(a) Adoption of 4 categories of Texts

The Assembly can adopt four different types of texts: recommendations, resolutions, opinions, and orders.

- Recommendations contain proposals addressed to the Committee of Ministers, the implementation of which is within the competence of governments.
- Resolutions embody decisions by the Assembly on questions which it is empowered to put into effect or expressions of view for which it is responsible alone.
- Opinions are mostly expressed by the Assembly on questions put to it by the Committee of Ministers, such as the admission of new member states to the Council of Europe, but also on draft conventions, the budget and the implementation of the Social Charter.
- Orders are generally instructions from the Assembly to one or more of its committees.

(b) Drafting of reports

In general, reports are generated by a motion for a recommendation or resolution. This motion has to be tabled by ten or more members of the Assembly belonging to at least five national delegations. It is then referred to a committee for report and possibly to other committees for opinion. The main committee then appoints a Rapporteur who drafts, with the help of the Council of Europe secretariat, his national delegation, his own expertise or

some specially recruited expert, a report which is divided into two parts: the operational draft resolution, recommendation, opinion or order and the explanatory memorandum.

5. Members, Observers, Special Guests & Consultants

a) Members of the Council of Europe

The Council of Europe[59] should not be confused with the European Union. The two organizations are quite distinct. While the 15 European Union states, however, are all members of the Council of Europe, the latter comprises 43 Members[60].

b) Special Guests to the Parliamentary Assembly

Introduced in 1989, this status is provided in order to facilitate the process of accession of the countries from Central and Eastern Europe.

The “Special Guests” status is available to all national legislative assemblies of European non-member states which have signed the Helsinki Final Act and the Charter of Paris for a New Europe. These delegations have the same number of seats as for the Members States but they do not have the right to vote or to stand for election.

---

59 www.coe.int

60 The 43 Members and their date of admission to the Council of Europe [day/month/year] : Albania (13.07.1995), Andorra (10.10.1994), Armenia (25.1.2001), Austria (16.04.1956), Azerbaijan (25.1.2001), Belgium (5.5.1949), Bulgaria (7.5.1992), Croatia (6.11.1996), Cyprus (24.5.1961), Czech Republic (30.6.1993), Denmark (5.5.1949), Estonia (14.5.1993), Finland (5.5.1989), France (5.5.1949), Georgia (27.4.1999), Germany (13.7.1950), Greece (9.8.1949), Hungary (6.11.1990), Iceland (9.3.1950), Ireland (5.5.1949), Italy (5.5.1949), Latvia (10.2.1995), Liechtenstein (23.11.1978), Lithuania (14.5.1993), Luxembourg (5.5.1949), Malta (29.4.1965), Moldova (13.7.1995), Netherlands (5.5.1949), Norway (5.5.1949), Poland (29.11.1991) ,Portugal (22.9.1976), Romania (7.10.1993), Russian Federation (28.2.1996), San Marino (16.11.1988), Slovakia (30.6.1993), Slovenia (14.5.1993), Spain (24.11.1977), Sweden (5.5.1949), Switzerland (6.5.1963), the "former Yugoslav Republic of Macedonia" (9.11.1995), Turkey (13.4.1950), Ukraine (9.11.1995), United Kingdom (5.5.1949)
Ukraine is about to be expu

Currently there are a two Special Guests: Bosnia- Herzegovina (since January 28th 1994) and the Federal Republic of Yugoslavia (since January 22nd 2001)

c) Observers to the Committee of Ministers

The Observers States to the Committee of Ministers can participate but not vote or stand for election in all decisions made by the executive body of the Council of Europe.

The United States have widely provided their expertise and given their opinion during the deliberations related to the COE Convention on Cyber-crime. This participation has enabled the United States to prevent the adoption of important amendments like the criminalization of "racists" websites that, in the US point of view, is contrary to the U.S. Constitutional Protection of Free Speech.

Currently 5 countries have this status: Canada (since May 29th 1996), Holy See (since March 7th 1970), Japan (since November 20th 1996), Mexico (since December 1st 1999) and the United States of America (since January 10th 1996).

d) The Observers to the Parliamentary Assembly

The Observers States to the Parliamentary Assembly can participate but not vote or stand for election in all decisions made by the legislative body of the Council of Europe.

Their voice can be heard during key deliberations, for instance when the Members are discussing the adoption of a convention draft: Observers can give their opinion and provide their expertise article by article and amendment by amendment even if they can't vote at the end. Thus, they have the Power to greatly influence the final decision.

Therefore, this status is more important than it looks like.

Currently, 3 States have this status: Canada (since May 28th 1997), Israel (since December 2nd 1957) and Mexico (since November 4th 1999).

e) Consultative Role of the Non Governmental Organizations (NGOs)

By granting consultative status to over 350 non-governmental organizations (NGOs), the Council of Europe is building a real partnership with those who represent ordinary people. Through various consultation arrangements (including discussions and colloquies) it brings NGOs into intergovernmental activities and encourages dialogue between members of parliament and associations on major social issues.

B. The Convention's history

1. The legislative process

The Council of Europe Convention on Cyber-crime is the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks.

The legislative process started in the last quarter of 1997. The Committee of Experts on Crime in Cyber-Space[61] (PC-CY) started the elaboration of the text.

On April 27th, 2000, this Committee released its first draft of the Convention.

Since then, the drafting group continually released new drafts. The latest version, number 27, was released on May 25th 2001, debated and approved during the 50th plenary session of the

61 The Committee can be contacted at daj@coe.int

European Committee on Crime Problems [CDPC], held between June 18th-22nd 2001 and is now available online[62].

During the session, a protocol was added to complement the Convention. It will make a crime the spreading of racist and xenophobic propaganda through computer networks[63].

The last version will be released on June 29th. The CDPC will then submit the final draft to the Committee of Ministers who will debate its adoption at its next meeting, scheduled for September 2001.

Once adopted, it will be open for signature to the 43 members of the Council of Europe[64] and observer Nations, including the United States.[65] This process could start as early as November 2001.

Finally, the Convention will enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe will have expressed their consent to be bound by the Convention[66].

2. Acts at the origin of the Convention

In the late 90's, Cyber-crime became an issue of growing concern in the International Community.

---

62 Council of Europe, *Draft Convention on cyber-crime (Version No 27 revised)* [http://conventions.coe.int/treaty/EN/cadreprojets.htm]

63 a move vehemently opposed by the United States who argued that such provision would violate the First Amendment to the US Constitution protecting Free Speech.

64 www.coe.int

65 In previous drafts and until the release of art. 36 § 1in draft #24, the convention was open for signature only to member States of the Council of Europe.

66 Draft #27 of the Convention, Art 36 § 3 [http://conventions.coe.int/treaty/EN/cadreprojets.htm]

Recent developments which further advance international understanding and cooperation in combating cyber-crimes, include actions of the United Nations[67], the OECD[68], the European Union[69] and the G8[70]. However, the Council of Europe Convention on Cyber-crime legislative process was initiated by the following three groups of texts:

a) The European Recommendations

In particular, the following European Recommendations have influenced widely the Council of Europe Convention on Cyber-crime:

- Recommendation N° R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications,
- Recommendation N° R (88) 2 on piracy in the field of copyright and neighboring rights, the Recommendation N° R (87) 15 regulating the use of personal data in the police sector
- The Recommendation N° R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services]
- Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and

67 www.un.org
68 Described at www.oecd.org , OECD is the abreviation for the Organisation for Economic Cooperation and Development
69 europa.eu.int
70 Described at http://www.g7.utoronto.ca/g7/what_is_g7.html as being, since the first reunion in 1975, the annual meeting of the heads of state or government of the major industrial democracies in order to deal with the major economic and political issues facing their domestic societies and the international community as a whole. It is composed of France, the United States, Britain, Germany, Japan, Italy, Canada, The European Community and Russia

- Recommendation N° R (95) 13 concerning problems of criminal procedural law connected with Information Technology;

b) The European Resolutions

Moreover, the two following European Resolutions had a great impact on the drafting as well:

- Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the work carried out by the European Committee on Crime Problems (CDPC) on cyber-crime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offenses;
- Resolution N° 3 adopted at the 23rd Conference of the European Ministers of Justice (London, June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions so as to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international cooperation, which duly takes into account the specific requirements of the fight against cyber-crime.

c) The October 1997 Action plan of the Council of Europe

Finally, The last important text in the inception process of the Convention is the Action plan adopted by the Heads of State and Government of the Council of Europe, on the occasion

of their Second Summit held in Strasbourg, the 10th and 11th of October 1997, to seek common responses to the development of the new information technologies, based on the standards and values of the Council of Europe.

3. Role of the United States

a) The most vulnerable country in the world

The United States is not a Member of the Council of Europe and can't be one because it does not belong to the geographic boundaries of Europe.

However, this country has an Observer status in the COE.

Since the biggest amount of computers in the world and consequently the biggest amount of individuals and companies connected to the Internet are located in the United States, it is not by accident that the highest amount of computer related crimes are located in this country according to the statistics published by the Computer Crime and Intellectual Property Section of the U.S. Department of Justice [CCIPS][71].

Most of the vital infrastructures of the U.S. government but also of most U.S. companies are handled by a computer and most of these computers are now networked.

Therefore, the United States is more threatened than any other country in the world by cyber-crime.

---

71 U.S. Department of Justice, *Intellectual Property Crime Statistics from the Attorney General's Annual Report* [January 23rd 2001 **;** http://www.usdoj.gov/criminal/cybercrime/ipstats.htm]

b) Strong knowledge and expertise to offer

The United States have had a very active role in the drafting of the Council of Europe Convention on Cyber-crime even if they had only an "Observer" status.

The U.S. law enforcement agencies experience[72], the government researches, the existing statutes and cases represent a tremendous amount of expertise that the Council of Europe has used extensively when drafting the text.

The United States was invited to participate as an "observer" in both the 1989 and 1995 Recommendations, as well as in the development of the Convention on cyber-crime. Because of the vulnerability of the United States to cyber-crime, the benefits to be gained from a well-crafted instrument focused on increasing international cooperation in this area, its desire to help shape such an important instrument, and the importance of the information technology sector, the United States accepted the CoE's invitation to participate in the Convention negotiations. The other non-CoE States participating in the negotiations are: Canada, Japan, and South Africa. By virtue of their having participated in the Convention's elaboration, the United States and these other non-CoE States will have the right to become parties to the Convention if they choose to do so.

The United States, represented by the Department of Justice and the Department of State, in close consultation with other U.S. government agencies, has actively participated in the negotiations in both the drafting and plenary sessions, working closely with both CoE and non-CoE member States. Because the provisions in the draft Convention are generally

72 James K. Robinson, Assistant Attorney General for the Criminal Division of the U.S.Department of Justice, *Internet as the Scene of Crime* [International Computer Crime Conference, Oslo, Norway, May 29th –31st, 2000 ; http://www.cybercrime.gov/intl.html#Vb]

adopted by consensus both in the drafting and plenary groups, rather than by member state vote, the United States has had a real voice in the drafting process[73].

c) Potential benefit of the Convention for the United States

As stated above, the United States is heavily dependent on computers that are networked, and it offers many targets across every sector of society. Left unchallenged, computer crime poses a serious threat to the health and safety of our citizens, and may stifle the Internet's power as a tool to communicate, engage in commerce, and expand people's educational opportunities around the globe.

Thus, as the Computer Hacking and Intellectual Property section of the U.S. Department of Justice has said[74], the United States has much to gain from the Convention that is a strong, well-crafted multilateral instrument that removes or minimizes the many procedural and jurisdictional obstacles that can delay or endanger international investigations and prosecutions of computer-related crimes.

Moreover, the U.S government federal agency has affirmed that the "Convention breaks new ground by being the first multilateral agreement drafted specifically to address the problems posed by the international nature of computer crime. Although

---

73 U.S. Department of Justice : Computer Crime and Intellectual Property Section, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cyber-crime (Draft 24RE V2)* [December 1st, 2000 ; http://www.cybercrime.gov/COEFAQs.htm#Q3]

74 U.S. Department of Justice : Computer Crime and Intellectual Property Section, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cyber-crime (Draft 24RE V2)* [December 1st, 2000 ; http://www.cybercrime.gov/COEFAQs.htm#Q4]

we believe the vast bulk of the obligations and powers contemplated by the draft Convention are already provided for under United States law, the Convention makes progress in this area by:

- requiring signatory countries to establish certain substantive offenses in the area of computer crime,
- requiring parties to adopt domestic procedural laws to investigate computer crimes and
- providing a solid basis for international law enforcement cooperation in combating crime committed through computer systems.

If the United States were to become a party to this Convention, it would directly benefit by having better methods of obtaining international assistance from other parties in computer-related crime cases, particularly because the other parties to the Convention would have similar minimum definitions of computer crimes and the domestic procedural tools

needed to investigate those crimes.

C. Structure

The Convention consist of forty-eight articles regrouped in four chapters. The first one gives general definitions. The second one harmonizes substantive and procedural National Laws related to cyber-crime. The third one details the treaty's new International cooperation system and the fourth one addresses Treaty validity, enforcement, signature, ratification and reservation issues.

1. Chapter one - Use of terms (art. 1)

2. Chapter two - Measures to be taken at the national level (art. 2-22)

a) Section 1 -- Substantive criminal law –

(1) Title 1 - Offenses against the confidentiality, integrity and availability of computer data and systems (art. 2-6)

(2) Title 2 - Computer-related offenses - (art 7-8)

(3) Title 3 - Content-related offenses - (art. 9)

(4) Title 4 - Offenses related to infringements of copyright and related rights - (art. 10)

(5) Title 5 – Ancillary liability and sanctions, comprises 3 articles - (art. 11-13)

b) Section2 – Procedural law –

(1) Title 1 - Common provisions -(art. 14-15)

(2) Title 2 - Expedited preservation of stored computer data- (art. 16-17)

(3) Title 3 - Production order - (art. 18)

(4) Title 4 – Search and seizure of stored computer data - (art 19)

(5) Title 5 – Real-time collection of computer data (art 20-21)

c) Section 3 – Jurisdiction – (Art. 22)

3. Chapter III – International cooperation

a) Section 1 – General principles

(1) Title 1 – General principles relating to international cooperation (art. 23)

(2) Title 2 – Principles relating to extradition (art. 24)

(3) Title 3 – General principles relating to mutual assistance (art. 25-26)

(4) Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements (art. 27-28)

b) Section 2 – Specific provisions

(1) Title 1 – Mutual assistance regarding provisional measures (art. 29-30)

(2) Title 2 – Mutual assistance regarding investigative powers (art. 31-34)

(3) Title 3 – 24/7 Network (art. 35)

4. Chapter IV – Final provisions (art 36-48)

D. Purpose

The Purpose of the Council of Europe Convention on Cyber-crime is described in the 9th paragraph of its preamble:

"the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offenses, by facilitating the detection, investigation and prosecution of such criminal offenses at both the domestic and international level, and by providing arrangements for fast and reliable international cooperation"

Precisely, the official Explanatory memorandum of the Convention asserts[75], at his point # 16 that the Convention aims principally at:

(1) harmonizing the domestic criminal substantive law elements of offenses and connected provisions in the area of cyber-crime

(2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offenses as well as other offenses committed by means of a computer system or evidence in relation to which is in electronic form

(3) setting up a fast and effective regime of international cooperation.

E. General scope

The Council of Europe Convention on Cyber-crime is the first ever international treaty to address criminal law and procedural aspects of various types of criminal behavior directed against computer systems, networks or data and other types of similar misuse.

The draft provides, among others, for the coordinated criminalization of computer hacking and hacking devices, illegal interception of data and interference with computer systems, computer-related fraud and forgery. It also prohibits on-line child pornography, including the possession of such material after downloading, as well the reproduction and distribution of copyright protected material. A protocol was added on June 22nd 2001 to complement the Convention and make a crime of xenophobic and racism propaganda. The draft Convention

75 Council of Europe, *Draft Convention on cyber-crime* [http://conventions.coe.int/treaty/EN/cadreprojets.htm]

will not only define offenses but will also address questions related to the liability of concerns individuals and corporate offenders and determine minimum standards for the applicable penalties.

The draft text also deals with law enforcement issues: future Parties will be obliged to empower their national authorities to carry out computer searches and seize computer data, require data-subjects to produce data under their control, preserve or obtain the expeditious preservation of vulnerable data by data-subjects. The interception of data transmitted through networks, including telecommunication networks, is also under discussion. These computer-specific investigative measures will also imply cooperation by telecom operators and Internet Service Providers, whose assistance is vital to identify computer criminals and secure evidence of their misdeeds.

As computer crimes are often international in their nature, national measures need to be supplemented by international cooperation. The draft treaty therefore requires future Parties to provide each other various forms of assistance, for example by preserving evidence and locating on-line suspects. The text also deals with certain aspects of trans-border computer searches. Traditional forms of mutual assistance and extradition would also be available under the draft Convention and a network of 24 hours/ day, 7 days/week available national contact points would be set up to speed up international investigations.

F. Important general concepts or terms left to national interpretation

a) Definition of "computer system", "computer data", "service provider" and "traffic data".

It was understood by the drafters that under this Convention Parties would not be obliged to copy verbatim into their domestic laws the four concepts defined in Article 1, provided that these laws cover such concepts in a manner consistent with the principles of the Convention and offer an equivalent framework for its implementation[76].

b) Technology-neutral language opened to future technologies

Although the substantive law provisions relate to offenses using information technology, the Convention uses technology-neutral language so that the substantive criminal law offenses may be applied to both current and future technologies involved[77]

c) All offenses must be “intentional”

All the offenses contained in the Convention must be committed "intentionally" for criminal liability to apply. In certain cases, an additional specific intentional element forms part of the offense. For instance, in Article 8 on computer-related fraud, the intent to procure an

76 Explanatory memorandum, point # 22
77 Explanatory memorandum, point # 31

economic benefit is a constituent element of the offense. The drafters of the Convention agreed that the exact meaning of 'intentionally' should be left to national interpretation[78].

d) The addition of "qualifying circumstances" in the offense definition

Moreover, some articles in section 1 allow the addition of qualifying circumstances when implementing the Convention in domestic law. In other instances even the possibility of a reservation is granted (cf. Articles 40 and 42). These different ways of a more restrictive approach in criminalization reflect different assessments of the dangerousness of the behavior involved or of the need to use criminal law as a countermeasure. This approach provides flexibility to governments and parliaments in determining their criminal policy in this area[79].

e) The term "without right," which appears in all the substantive offense provisions (Articles 2-12)

The term "without right" has a broad meaning and is intended to take into account well-established principles regarding criminal culpability, including application of legal defenses and justifications, contract law, and traditional legislative exemptions.

The specific demarcation between a conduct that is "with right" and one that is "without right" is left by the convention to national law interpretation. Thus, if a conduct is

78 Explanatory Memorandum, poin # 39
79 Explanatory Memorandum, poin # 40

"legitimate" under a particular signatory's national law, then it will not be "without right" under the same law.

This freedom could lead to substantial differences among national laws.

For example, the Convention does not purport to exhaustively define the line between what sorts of "interception" are lawful and which are not under Article 3 ("Illegal Interception"). Therefore, nothing in this Convention would change the U.S. wiretap statute (18 U.S.C. 2511(2)(a)(I)), which specifically allows monitoring by a service provider of traffic on its own network undertaken to protect its rights and property. Exactly what sorts of interception are "with right" and which "without right" in a particular signatory country would continue to be determined under national law[80].

G. Critics

1. Main concerns

Global Internet Liberty Campaign[81], a non-profit independent organization, has highly criticized the treaty.

---

[80] U.S. Department of Justice : Computer Crime and Intellectual Property Section, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cyber-crime* (Draft 24REV2) [December 1st, 2000 ; http://www.cybercrime.gov/COEFAQs.htm#Q9]

[81] it was formed at the annual meeting of the Internet Society in Montreal. Members of the coalition include the American Civil Liberties Union, the Electronic Privacy Information Center, Human Rights Watch, the Internet Society, Privacy International, the Association des Utilisateurs d'Internet, and other civil liberties and human rights organizations, see http://www.gilc.org/about/principles.html for further details.

Global Internet Liberty Campaign said it believes that "the draft treaty is contrary to well-established norms for the protection of the individual, that it improperly extends the police authority of national governments, that it will undermine the development of network security techniques, and that it will reduce government accountability in future law enforcement conduct."[82]

a) ISP mandatory requirement to retain records of their customers' activity

One the most controversial issues in the Convention are the provisions that will require Internet Service Providers to retain records regarding the activities of their customers. (Articles 17, 18, 24, 25).

According to Global Internet Liberty Campaign[83], these provisions pose a significant risk to the privacy and human rights of Internet users and are at odds with well-established principles of data protection such as the Data Protection Directive of the European Union. Similar communications transaction information has been used in the past to identify dissidents and to persecute minorities.

The whole of Article 18 could be incompatible with Article 8 of the European Convention on Human Rights [ECHR] and with the jurisprudence of the European Court of Human Rights.

---

82 Global Internet Liberty Campaign, *Member Letter on Council of Europe Convention on Cyber-crime,* [October 18th 2000; http://www.gilc.org/privacy/coe-letter-1000.html]
83 www.gilc.org

However, the Computer Hacking and Intellectual Property section of the FBI has strongly rejected the critics.

They have said that[84] "the News reports that have stated that the Council of Europe Convention will require Internet service providers to collect and retain data, adopt mandatory business practices, and build certain technical capabilities into their infrastructures are falsely based".

The section further affirms that[85] "the Convention does not contain any mandatory retention provisions or requirements that service providers collect or maintain categories of data generally; nor does it require certain technical capabilities.

The governmental organization said that first, it is important to distinguish between data retention requirements, which would require providers to collect and keep all or a large portion of a provider's traffic as a routine matter, and preservation requirements, which enable law enforcement authorities, during the course of a criminal investigation, to instruct a service provider to set aside specified data that is already in the service provider's possession".

Therefore, the U.S. Government agency asserts that there is no data retention in the Convention; there is, however, data preservation provision.

---

84 U.S. Department of Justice : Computer Crime and Intellectual Property Section, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cyber-crime (Draft 24RE V2)* [December 1st, 2000 ; http://www.cybercrime.gov/COEFAQs.htm#Q13]

85 ibidem

Moreover, they said that preservation is not a new idea; it has been the law in the United States for nearly five years: 18 U.S.C. 2703(f) requires an electronic communications service provider to "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process" upon "the request of a governmental entity." This applies in practice only to reasonably small amounts of specified data identified as relevant to a particular case where the service provider already has control over that data. Similarly, as with traditional subpoena powers, issuance of an order to an individual or corporation to produce specified data during the course of an investigation carries with it an obligation not to delete or destroy information falling within the scope of that order when that information is in the person's possession or control.

They end their argumentation by adding that the Convention does not require any particular architecture or capability; nothing in the Convention states that a service provider must be able to obtain evidence that it is not technically capable of collecting. However, while there are no mandatory technical requirements placed upon service providers, there is no prohibition on States imposing such requirements if necessary under their legal systems.

Still, ISPs have strongly opposed the mandatory requirements and their voice has been largely broadcasted. This is the most controversial part of the Convention. In fact, this concern itself could prevent some countries who will vote on the matter, to ultimately ratify the Convention.

b) Absence of a data protection clause

Some Countries have adopted a legislation preventing public and private entities to keep personal profile sensitive datas on individuals after a legally binding period of time, provided that their necessity is not proven anymore. Therefore, these entities are forced to erase the informations after a short period of time that the law determines.

Still, a lot of important countries including those with the biggest personal profile databases like the United States have not passed such a law. This issue is not addressed by the Convention.

Consequently, critics assert that the increase of the powers of law enforcement will water down the protection of human rights.

"The council thought of putting in a data protection clause, which we would have liked, but it was shot down. Now the police can decide to hold on to data gathered on somebody if it is not needed anymore," said Gus Hosein, a senior fellow at civil liberty campaign group Privacy International and a lecturer at the London School of Economics[86].

c) Lack of dual criminality provision

The lack of a dual criminality provision, where extradition or international cooperation is concerned, can put a burden on U.S. Internet Service Providers [ISPs].

---

86 Joris Evers, *Council of Europe wraps up cybercrime treaty*, [CNN Interactive, May 29th 2001; http://www.cnn.com/2001/TECH/internet/05/29/cybercrime.treaty.idg/index.html]

Under the Convention, U.S. ISPs could be forced to respond to requests on matters that are not illegal in the U.S., but are elsewhere. Hate speech[87], for example. An ISP could be forced to hand over information about a customer to German authorities, while in the U.S. the customer is protected by the First Amendment to the U.S. constitution.

d) Too large definition of "Illegal devices" in Article 6

The Conception of "Illegal Devices" set out in Article 6 lacks sufficient specificity to ensure that it will not become an all-purpose basis to investigate individuals engaged in computer-related activity that is completely lawful.

Technical experts have made clear that this provision will also discourage the development of new security tools and give government an improper role in policing scientific innovation.

This critic has been severely contested by the Computer Hacking and Intellectual Property section of the U.S. Department of Justice[88].

The section has said[89] that nothing in the draft Convention suggests that states should criminalize the legitimate use of network security and diagnostic tools.

---

[87] On June 22nd 2001, an additional protocol was added to the Convention making it a crime to spread racist and xenophobic propaganda through computer networks.

88 www.cybercrime.gov

89 U.S. Department of Justice : Computer Crime and Intellectual Property Section, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cyber-crime (Draft 24REV2)* [December 1st, 2000 ; http://www.cybercrime.gov/COEFAQs.htm#Q11]

On the contrary, Article 6 obligates parties to criminalize the trafficking and possession of "hacker" tools only where such conduct is (i) intentional, (ii) "without right", and (iii) done with the intent to commit an offense of the type described in Articles 2-5 of the Convention. Because of the criminal intent element, fears that such laws would criminalize legitimate computer security, research, or education practices are unfounded.

Moreover, paragraph 2 of the Article 6 makes clear that legitimate scientific research and system security practices, for example, are not criminal under the Article.

Finally, in practice, the existing U.S. laws that already criminalize possession and trafficking in "access" or "interception" tools (as opposed to "damage" tools) with similar criminal intent have not led to investigations of network security personnel.

However, the section did not convince private technical experts who are still very united in their opposition to this article of the Convention.

e) No provision exempting Service Providers for potential criminal liability

Critics asserts that the criminal provisions of Articles 9 and 11 could lead to a chilling effect on the free flow of information and ideas. Imposing liability on Internet Service Providers for third party content places an unreasonable burden on providers of new network services and will encourage inappropriate monitoring of private communications.

Furthermore, Service Providers have expressed high concern that they might be held criminally liable for failing to monitor customer or user content, or for the criminal actions of their employees.

The Computer Hacking and Intellectual Property section of the U.S. Department of Justice rejected[90] this remark.

It said that nothing in the Convention requires service providers to monitor content.

Their position is that under the Convention, service providers do not face criminal liability if they have only an "intent to transmit data" without knowledge of what the data contains. Once a provider becomes specifically aware that its system is being used to transmit or store criminal content, instructions, etc., questions of liability may arise.

For example, Article 11 on aiding and abetting contemplates liability where the person who commits one of the substantive offenses in the Convention is aided by another person who shares the mental state required for the commission of the crime. However, individuals or legal persons (including service providers) that do not share the objective of committing the crime cannot incur liability through unknowing incidental assistance provided to a criminal actor. Indeed, the Convention explicitly requires that the actor intentionally aid or abet a crime under the convention.

---

90 U.S. Department of Justice : Computer Crime and Intellectual Property Section, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cyber-crime (Draft 24REV2)* [December 1st, 2000 ; http://www.cybercrime.gov/COEFAQs.htm#Q14]

In addition, Article 12, governing corporate liability, restates the traditional corporate liability principle that if a person with significant authority within a corporation intentionally undertakes or, through a lack of supervision, permits the undertaking of criminal activity for the corporation's benefit, the corporation may face criminal, civil or administrative liability. This Article is based upon similar provisions in other multilateral law enforcement treaties and does not go beyond current U.S. law governing the vicarious liability of corporations. In fact, the Convention's liability requirements would apply to a more limited group of persons than under U.S. federal law.

f) Definition of Child Pornography in art. 9 violates Freedom of Speech rights

In article 9, related to Child Pornography, the Convention criminalizes images that "appear" to represent children engaged in sexual conduct.

Critics have said that the word "appear" violates the U.S. constitution and that it would in fact prohibit certain adult pornography protected by Freedom of Speech constitutional rights.

The computer hacking and intellectual property section of the Department of Justice has rejected[91] the critics.

The section argument is that Child pornography on the Internet is an extremely serious problem, and one on which all the negotiating States have agreed to adopt a strong position.

---

91 U.S. Department of Justice : Computer Crime and Intellectual Property Section, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cyber-crime (Draft 24RE V2)* [December 1st, 2000 ; http://www.cybercrime.gov/COEFAQs.htm#Q12]

Furthermore, it asserts that the Convention is intended to cover virtual child pornography because it is nearly impossible to distinguish it from real child pornography, though in fact few instances of virtual child pornography have been found. Virtual child pornography, like real child pornography, can be and has been used to entice minors into sexual relationships and is often traded for real child pornography.

Therefore, the section believes that the provision of the Convention is consistent with United States law in this area.

However, adult pornography usually does not use the service of old models and it is true that the difference between an adult and a child is difficult to make if the criteria is based on the "appearance". This is why Pornography providers have highly opposed the provision. If the Convention is adopted, the U.S. Supreme Court might finally decide if this provision is constitutional because the U.S. Government has already claimed that the adoption of the Convention will not require any statutory change in United States Law[92].

g) Dramatic extension of copyright crimes in an area where National law is very unsettled

Critics also object to the dramatic extension of copyright crimes in the proposed Article 10.

92 U.S. Department of Justice : Computer Crime and Intellectual Property Section, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cyber-crime (Draft 24RE V2)* [December 1st, 2000 ; http://www.cybercrime.gov/COEFAQs.htm#Q7]

They claim[93] that it is hardly a settled matter that criminal penalties are the appropriate remedy for copyright infringement, nor do the underlying treaties referenced impose such requirements. New criminal penalties should not be established by international convention in an area where national law is so unsettled. More generally, they disagree with initiatives that allow for mutual assistance without dual-criminality. They think that this requirement is central to preserving the sovereign authority of nations.

h) International Cooperation and Investigative Procedures defined too vaguely

Critics believe that clear procedures must be agreed upon in international investigations, and that no law enforcement agency within a different jurisdiction should act on behalf of another nation without clear investigative procedures within its own jurisdiction. They are concerned for the consistency of individual rights protections.

I think personally that they are right. International investigations can't work in practice if the investigative procedures are not clearly defined and the Convention is not going far enough in this matter.

93 Global Internet Liberty Campaign, *Member Letter on Council of Europe Convention on Cyber-crime,* [October 18th 2000; http://www.gilc.org/privacy/coe-letter-1000.html]

j) The Convention was kept secret until the release of the 19th draft

The drafting process was secret until draft 19 was publicly released in April 2000. Even now, Justice officials won't comment publicly on their role in drafting the terms of the treaty. The department does defend the treaty on an FAQ on its Web site: "The United States has much to gain from a strong, well-crafted multi-lateral instrument that removes or minimizes the many procedural and jurisdictional obstacles" that endanger investigations.

Still, critics don't like that the treaty was kept under wraps until it was well along the way to final form. "A lot of the provisions were largely locked in" by the time the treaty was publicly released, Baker says.

The Justice Department responds by noting that, since last April, it has made numerous presentations and met repeatedly with business and other private-sector interests. It is "about as open a process as I can think of," says Betty Shave of Justice's computer crime and intellectual property section, who has represented the department in negotiations.

k) It is unsure if the US will finally ratify it

Short of an international backlash, treaty watchers are uncertain how the U.S. Congress will respond to the treaty if the United States signs it. Whether senators decide that the need to combat cyber-crime trumps concerns about submitting U.S. citizens and companies to foreign criminal process remains an open question. Moreover, the recent introduction of the prohibition of xenophobic and racism propaganda on June 22nd 2001 which has been said to

be contrary to the First Amendment to the US Constitution could also prevent the adoption of the Convention by the US Congress.

However, at this time there are no indications that the Bush administration will stop this initiative begun during the Clinton presidency. But even if the United States doesn't sign the treaty, it will likely affect U.S. companies doing business internationally, their business partners, and their clients.

i) Search and seizure of stored computer data lacks necessary procedural safeguards

Concerns has been expressed regarding Article 14 setting out the requirements for search and seizure of stored computer data. This provision lacks necessary procedural safeguards to safeguard the rights of the individual and to ensure due process of law. In particular, there is no effort to ensure that an independent judicial review, ensuring the respect of basic freedoms and liberties, occurs before a search by the state is undertaken. Such searches would constitute an "arbitrary interference" under international legal norms.

Even if a lot of countries have sufficient procedural law to protect their individuals, some don’t. However, almost all countries parties to the convention are also part to the Council of Europe Convention of Human Rights and this Treaty could be the basis for such protection in the Country that still lack procedural safeguards law.

Articles 14 and 15 could establish a requirement for government access to encryption keys that would compel individuals to incriminate themselves, which may well be incompatible with Article 6 of the European Convention on Human Rights and with the jurisprudence of the European Court of Human Rights. Another issue is the ambiguity that arises within this same article on government access to decryption keys. The Council of Europe should clarify this provision so that member countries do not take the convention to be a mandate for passing legislation allowing for self-incrimination.

2. High-Tech US corporations vehemently oppose the treaty[94]

High-Tech U.S. Corporations represented mainly by AT&T and AOL Time Warner think that the Department of Justice and the Federal Bureau of Investigation are using a foreign forum to create an international law-enforcement regime that favors the interests of the "feds" over those of ordinary citizens and businesses. In particular, they claim that the real goal of the Convention is to make it easier for the Law Enforcement agencies to get evidence from abroad and to extradite and prosecute foreign nationals for certain kinds of crimes.

Maybe the ordinary US citizen trusts the law-enforcement chiefs in Washington D.C. to do the right thing, but here's the catch. The same new powers given to the United States will also be handed over to Bulgaria, Romania, Azerbaijan, and other Council of Europe nations

[94] Mike Godwin, *International Treaty on Cybercrime Poses Burden on High-Tech Companies* [IP Worldwide, Yahoo! Publications, April 5th 2001 ; http://biz.yahoo.com/law/010405/81513-1.html]

that -- although officially democratic now -- don't have a strong tradition of checks and balances on police power.

This is why US High-Tech Corporations are asking the following question : “Do we want investigators rummaging around your clients' computer systems on warrants issued by former Soviet-bloc nations?”

That's the prospect that has pushed AT&T Corporation and other high-technology companies into feverishly trying to stop, or at least soften, the treaty. The U.S. Chamber of Commerce and the Information Technology Association of America also oppose it.

Stewart Baker, a partner at Washington, D.C.'s Steptoe & Johnson, is one of the chief lobbyists for the treaty's opponents. As a former general counsel of the National Security Agency and recipient of the U.S. Department of Defense Medal for Meritorious Civilian Service, he's got street credentials on these issues in corporate America.

What worries Mr. Baker and his colleagues? Let’s consider the following hypothetical: A Los Angeles screenwriter corresponds by e-mail with a neo-Nazi in Germany while researching a script. Shortly after, the screenwriter finds federal agents examining the files on his home computer. The agents also visit AOL Time Warner to retrieve records of the screenwriter's AOL usage.

The agents are fulfilling a warrant issued by German authorities allowing them to search for Nazi propaganda. Such material is unlawful in Germany but not in the United States. They framed their warrant in terms of "suspected terrorist activity."

Maybe the screenwriter should have anticipated this scenario, given the vigor with which

German and other European authorities pursue hate crime on the Internet. Maybe he's willing to run that risk and bear the burden of this kind of search. But what about AOL?

AOL already gets dozens of search warrants and subpoenas every month. What would change under this treaty is that, in addition to getting those submitted by U.S. law-enforcement officials, they'd also have to respond to warrants and court orders from dozens of nations. All Internet service providers and phone companies -- and perhaps other businesses -- would have to cooperate with these investigations. They worry that they would also have to foot the bill for compliance.

Maybe AOL and AT&T should expect this sort of intrusion as a cost of doing business in the Internet era. But what about all other high-tech corporations? What about all individuals? The treaty would likely apply to any business or individual operating a computer connected to a network, according to Marilyn Cade, AT&T's director of Internet and e-commerce policy. If you cable together two computers, you could be forced to comply with investigations that originated in Sofia or Riga.

Foes acknowledge that there might be a need for a limited treaty harmonizing laws globally. Last year, for example, the Philippines was unable to prosecute the creator of the "love bug" virus. Its laws did not fit his deeds. But this proposal, they say, goes too far.

3. Motion Picture Majors & Computer-crime comparative law experts highly support the Convention

On the other hand, the Motion Picture Association of America, the Recording Industry of America Association and the Business Software Alliance all favor the treaty[95] in particular because of its requirement that certain large scale Copyright infringements be handled under criminal law. In general, such "attacks" are now handled under civil law in most countries. This companies and their members of course constantly face problems connected to the unauthorized transmission of their copyrighted materials. Thus, they believe that ensuring a greater number of countries make such attacks illegal and actionable under national law will help greatly their crusade against international copyright infringements.

Moreover, a report reviewing the state of computer crime laws in 52 nations, released on December 2000 by McConnell International[96] and named the "Cyber Crime and Punishment report »[97] strongly supports the Council of Europe's approach, and says the group has been "realistic, practical, efficient, balanced, and respectful of due process that protects individual rights."

This company is a Washington policy consultant founded by Bruce McConnell, a White House aide under U.S. Presidents George Bush and Bill Clinton.

Among the 52 nations computer crime laws reviewed, ten different offenses were sorted into four general areas: data crimes, network crimes, access crimes and related misdeeds, such as

---

[95] see Mike Godwin, *International Treaty on Cybercrime Poses Burden on High-Tech Companies* [IP Worldwide, Yahoo! Publications, April 5th 20001 ; http://biz.yahoo.com/law/010405/81513-1.html]

96 http://www.mcconnellinternational.com/

97 McConnell International, *cyber crime . . . and punishment? archaic laws threaten global information* [December 2000, http://www.mcconnellinternational.com/services/securitylawproject.cfm]

computer forgery and computer-related fraud. Of the countries analyzed, the report found that nine had extended their criminal laws online to prosecute a majority of the offenses on the list.

"The long arm of the law does not yet reach across the global Internet," McConnell said. "Organizations must rely on their own defenses for now. Governments, industry and civil society must all work together to develop consistent and enforceable national laws to deter future crimes in cyber-space."[98]

98 Joris Evers, *Council of Europe wraps up cybercrime treaty*, [CNN Interactive, May 29th , 2001 ; http://www.cnn.com/2001/TECH/internet/05/29/cybercrime.treaty.idg/index.html]

Chapter 3 : Which approach to fight cyber-crime efficiently?

A. Efficiency of international regulation in the crusade against cyber-crime

Law enforcement agencies are complaining that it is much more difficult to apprehend and convict a cyber-criminal than a normal criminal.

Their main argument is that the international nature of the Internet helps cyber-criminals to hide behind foreign unregulated sovereign jurisdiction.

Their argumentation can be summarized in the following sentence:

"the rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily by any current territoriality based sovereign."[99]

Therefore, using the tool of signature-pending Council of Europe Convention on Cyber-crime, International Governments are trying to harmonize their cyber-crime laws and develop cooperation and coordination between national Law enforcement agencies[100].

However, will these international regulating efforts be sufficient to prevent or at least slow the rapid proliferation of cyber-crime worldwide?

The doctrine is divided on the matter.

Some do not think so:

---

99 David Johnson and David Post, *Law and Borders – The Rise of Law in Cyberspace* [Stanford Law review 48 (1996) : 1367, 1375 ; http://www.cli.org/X0025_LBFIN.html]

100 see Chapter 2 : the Council of Europe Convention on Cyber-crime

"Some things never change about governing the Web. Most prominent is its innate ability to resist governance in almost any form[101]".

Some asserts that it depend on its architecture:

"Whether the Net is unregulable depends, and it depends on its architecture. With some architecture, behavior on the Net cannot easily be controlled; with others it can. With some it cannot be controlled through top-down regulation; with others it can. Among the many possible architecture that the Net might have, the aim of this part is to argue that it is evolving in a very particular direction: from an unregulable space to one that is highly regulable. The "nature" of the Net might once have been its unregulability; that "nature" is about to flip."[102]

The best approach of Governments to apprehend cyber-crime might be by using a multidisciplinary approach: fighting cyber-crime only by regulating cyber-space, even through international Conventions appear not to be sufficient. Especially, cyber-law experts have continuously said that "more litigation will not deter hackers from trying to infect the world's computer systems with viruses" [103]. Moreover, they added that : "Better security technology, diligent enforcement of existing laws, better-trained law enforcement officers and enhanced cooperation between the authorities and the computer industries are some of the measures the experts recommend."

---

101 Tom Steinert-Threlkeld, *Of Governance and Technology* [Inter@ctive WeekOnline, October 2nd 1998 ; http://www.zdnet.com/intweek/filters/tthrelkl.html]

102 Lawrence Lessig, *Codes and other laws of Cyberspace*, [Basic Books, 1999, p.25 ; www.lessig.org]

[103] Raju Chebium, *Experts say more laws won't stop computer hackers* [CNN Interactive, May 8th 2000 ; http://www.cnn.com/2000/LAW/05/05/love.bug/index.html]

Industry leaders, like Jeff Richards, executive director of the Internet Alliance, an industry group based in Washington further added[104] : "CEOs must personally involve themselves in security and privacy; I think legislation in this case should be generally a last resort." He said he feared that more legislation could restrict open access to the Internet. Also, it claimed that the industry-wide commitment to boosting cyber-security would also enhance consumer confidence.

The cyber-citizen project that aims at educating young people and teach them that committing cybercrimes is "bad' is a good example. Another approach, threatening for the privacy rights of the individuals, is the constant government surveillance of all communications networks, whether national or international.

However, the success of all these methods in fighting adequately Cyber-crime remains to be seen.

B. Multidisciplinary approach to fight cyber-crime

1. Implementing "future Technology" provisions in actual legislation

To keep the actual law always up-to-date and regulate now the future technological developments of tomorrow, Congressmen have started a practice of implementing in new high-tech legislation special provisions related to "future technologies".

That way, the Law can make criminal a conduct that do not exist at the time of its adoption but that might eventually exist in the future.

[104] ibidem

The United States legislation possesses numerous legislations with this kind of provision and not only in criminal matters. A good example is the recent adoption of the Digital Millennium Copyright Act [DMCA] and its concept of "circumventing technologies".

However, in a lot of international criminal law systems, no conduct should be made criminal without a strict legal basis. This is the old Latin principle of "nullum crimen, nulla poena sine lege "[105].

Therefore, such provisions might not stand all National Supreme Court tests.

Moreover, you can't predict the future and there will always be new conducts that will not fit even a broad "future technology" provision.

2. International harmonization of national legislation?

In a networked world, it has become increasingly easy for criminals to escape conviction by acting from another country where a conduct is either not criminalized or not prosecuted. They can also give the illusion to law enforcement agencies that they are in foreign country. The example given to the European Parliament on September 19th 2000 by Mr. Kevin DiGregory, Deputy Assistant General in the Criminal Division of the U.S. Department of Justice speaks for itself[106]:

---

105 for an application of this principle in Colombian law, see : http://www.juridicacolombiana.com/pagina/jurisprudencia/j_c_suprema/Penal/providencias/1997%20pp/11706%20(31-07-97).htm

106 Kevin DiGregory, *Fighting Cybercrime – What are the Challenges facing Europe ? The Transatlantic perspective*, [U.S. department of Justice, September 19th 2000, http://www.cybercrime.gov/EUremarks.htm]

“Consider a computer hacker in Paris on the Left Bank of the Seine who disrupts a corporation's communications network on the Right Bank. Before accessing his victim's computer, he routes his communication through providers in Romania, Australia, and Argentina. In this case, French police will need assistance from law enforcement authorities in Bucharest, Canberra, and Buenos Aires, before discovering that the criminal is right in their midst.

In these cases law enforcement is impeded by national borders in ways that criminals simply are not. While the Internet may be borderless for criminals, law enforcement agencies must respect the sovereignty of other nations. As a result, we are increasingly dependent on cooperation with foreign law enforcement agencies in fighting computer crime. Unfortunately, differing legal systems and disparities in the law often present major obstacles in our efforts.

The failure of a country to criminalize computer-related offenses is one such obstacle. When one country's laws criminalize certain activities on computers and another country's laws do not, cooperation in solving a crime and prosecuting the perpetrator may not be possible. That is, when a criminal weaves his communications through three, four, or five countries before reaching his intended victims, inadequate laws in just one of those countries can, in effect, shield that criminal from law enforcement around the world. “

Therefore, International Cooperation and Law Harmonization are important and essential to fight cyber-crime.

However, with the number of sovereign jurisdiction existing in the world, there is still a very long way until the world legislation will be harmonized. Most probably, it will never happen even in a remote future: the area of the Law that requires the strongest protection: Human rights, have been harmonized in less than 50 countries in the world and this process started in the 1950's. Therefore, an area of the Law that requires less attention like cyber-crime might never be harmonized in the entire world.

Consequently, cyber-criminals will always be able to act or appear to be acting from sovereign countries that lack cyber-crime legislation or where criminal prosecution is insufficient.

Therefore, to fight adequately cyber-crime, regulation is not the ultimate goal. It is only part of a multidisciplinary approach that needs to be taken.

3. Educating the "cyber-citizens" ?

Since smart, adaptive cyber-criminals will always be able to escape prosecution if they act or appear to be acting from the right complaisant country, Governments should use other tools to fight them than national or international regulation.

A good start would be education: the United States already has started the "cyber-citizen"[107] project. Its goal is to convince young citizens that they should "behave" on the Internet and that committing cyber-crime is a serious issue and not a game.

This approach might help reducing cyber-crime among teenagers that are acting for pride in their community.

---

107 http://www.cybercitizenship.org/

This parallel way of combating cyber-crime should be explored more deeply : dialogue can prevent the usage of repression.

Moreover, this parallel tool is at least perfectly legal and not contested by foreign countries.

4. Surveillance of International communication networks ?

"Big Brother is watching you!" This famous phrase from the George Orwells' novel "1984" is on the lips of a growing amount of world citizens.

The recent debate over the International Echelon surveillance system that allows participating National spy agencies to monitor most of the world's telephone, e-mail and telex communications[108] is here to prove that Governments are not waiting for legislation to be adopted to pursue crime in general and cyber-crime in particular.

This might be the ultimate and only efficient tool to prevent and fighting cyber-crime.

However, it is not tomorrow that communications on any networks of the world will be efficiently intercepted and analyzed in order to successfully prevent cyber-criminals from committing their crimes.

The only fact that the U.S. government is using currently $1.41 billion of his annual budget to finance studies and to develop new ways of protecting itself against cyber-crime is sufficient to prove that even this surveillance system is not totally efficient.

108 Nicky Hager, *Exposing the global surveillance system* [http://www.dis.org/erehwon/echelon.html]

Conclusion

Criminologists, law enforcement agencies, national security advisors, military officials, high-tech corporations and research institutes all agree that cyber-crime poses today a real threat to society. Previously only a marginal issue among cyber-punk teenagers, the phenomenon has now taken a new shape. These crimes are now orchestrated by greedy-motivated groups of individuals with substantial resources who are often linked to organized crime, international terrorist groups or foreign enemies. Recent cases have shown their goals involving the destruction of sensitive computer systems handling vital tasks such as State's electricity flow, airplane landing and take-off management and also the theft of major corporation's vital trade-secrets. The US administration has even stated recently that cyber-attacks are the major threat that the country faces and allocated $1.8 billion of the 2001 federal budget to fight it. However, a recent study has shown that out of the 52 countries analyzed, only 9 have a cyber-crime legislation, allowing cyber-criminals like the Philippine scientist who spread worldwide the 2000 "I love you" virus to escape conviction.

This is why the 2001 Council of Europe Convention on Cyber-crime is a treaty of great importance who could be opened for signatures as early as November 2001. It harmonizes substantive criminal laws and procedures related to cyber-crime and sets up an international cooperation system among national law enforcement agencies to fight the cyber-criminals more efficiently and in real time. However, only a multidisciplinary approach also involving the education of the cyber-citizens and the high-tech CEOs, a higher standard of protection of the national infrastructures and a bigger investment in computer and network security and in research and development can successfully reduce the threat.

TABLE OF CONTENTS

Introduction _____ *1*

Chapter 1 : What is cyber-crime ? _____ *2*

A. Origin & definition _____ **2**

1. Computer crime _____ 2
2. From Cyberpunk to cyber-culture _____ 4
   a) Science-fiction literature _____ 4
   b) Emergence of the cyber-culture _____ 5

B. The cyber-criminals _____ **6**

1. The Idealists (teenagers) _____ 7
   a) Looking for freedom & identity _____ 7
   b) Their actions are globally very damageable but individually negligible ____ 8
   c) Government should fight them through Education not Law: _____ 8
2. The greed-motivated (career criminals) _____ 10
   a) Unscrupulous _____ 10
   b) Often affiliated with organized crime _____ 11
   c) Potentially very dangerous and damageable for society _____ 11
   d) International cooperation and Law harmonization is the best way to fight them _____ 12
3. The cyber-terrorists _____ 13
   a) The newest and most dangerous category _____ 13
   b) The most appropriate way to fight them is by funding national security agencies and reinforcing global networks surveillance _____ 13

C. The reality of the threat _____ **14**

1. Alarming Cyber-Criminology statistics and prediction studies _____ 14
2. Rapid growth of Computer Security expenses _____ 16
3. Evidence of emerging cyber-terrorism _____ 17
   a) Since 1999, $1.46 billion allocated in the U.S. budget to fight the threat___ 17
   b) One hundred countries possibly working now on techniques to penetrate the U.S. information infrastructure _____ 18
   c) All vital infrastructures handled by computers _____ 18
   d) FBI computer crime case load doubling every year _____ 19
   e) A new kind of threat for the United States _____ 19
   f) A convention to fight cyber-terrorism is being drafted by key Scholars ___ 20
   g) An International wealthy potential cybert-terrorist: The Usama Bin Laden cyber-threat is real _____ 20
4. Cyber-crimes affects all sectors of society, private and public and under various shapes _____ 21

a) Electronic offshore-banking, money laundering and fraud: The collapse of the online European bank of Antigua _____ 21
b) Vital Infrastructure disruption: Airport tower control disabled by a teenager computer attack _____ 22
c) Denial of Service attack: E-Commerce websites _____ 23
d) Personal Files remote destruction and computer freezing: E-mail Virus "I love you" _____ 23
e) Stock crash due to false Information broadcasted on key sensitive financial news agency: Emulex _____ 23
f) Hacking of Vital corporation software source code: Microsoft Windows source code theft by a Russia based hacker _____ 24
g) Intellectual property fraud using new circumventing technologies: the DVD case _____ 25
h) Online fraud: The Experian report and the FBI Operation "Cyber loss" ___ 27
i) Vital infrastructure hacking: Electricity's flow handling computers hacked in California _____ 28

Chapter 2 : The 2001 Council of Europe Convention on Cyber-crime _____ 30

A. The Institution of the Council Of Europe [COE] _____ 30
1. Generalities _____ 30
2. Origin _____ 31
3. Purposes _____ 32
4. Organs _____ 33
a) The Committee of Ministers _____ 33
(1) Composition & voting rights _____ 33
(2) Semestrial meetings _____ 33
(3) Main Functions _____ 33
(4) The function of concluding conventions and agreements _____ 34
(a) General Scope _____ 34
(b) Adoption of the final text and the explanatory report _____ 34
(c) Signature and Ratification _____ 35
b) The Parliamentary Assembly _____ 35
(1) Historical importance _____ 35
(2) Composition & voting rights _____ 35
(a) Deputies, Observers and Special Guests _____ 35
(b) Special groups of Deputies _____ 36
(i) The Bureau _____ 36
(ii) The Standing Committee _____ 36
(iii) The Joint Committee _____ 36
(iv) The Secretariat of the Assembly _____ 37
(v) The Assembly Committees _____ 37

(3) Meetings frequency _____ 38
(a) The Parliamentary Assembly _____ 38
(b) The Committees _____ 38
(4) Main Functions _____ 38
(5) The legislative role _____ 39
(a) Adoption of 4 categories of Texts _____ 39
(b) Drafting of reports _____ 39
5. Members, Observers, Special Guests & Consultants _____ 40
a) Members of the Council of Europe _____ 40
b) Special Guests to the Parliamentary Assembly _____ 40
c) Observers to the Committee of Ministers _____ 41
d) The Observers to the Parliamentary Assembly _____ 41
e) Consultative Role of the Non Governmental Organizations (NGOs) _____ 42

B. The Convention's history _____ 42
1. The legislative process _____ 42
2. Acts at the origin of the Convention _____ 43
a) The European Recommendations _____ 44
b) The European Resolutions _____ 45
c) The October 1997 Action plan of the Council of Europe _____ 45
3. Role of the United States _____ 46
a) The most vulnerable country in the world _____ 46
b) Strong knowledge and expertise to offer _____ 47
c) Potential benefit of the Convention for the United States _____ 48

C. Structure _____ 49
1. Chapter one - Use of terms (art. 1) _____ 50
2. Chapter two - Measures to be taken at the national level (art. 2-22) _____ 50
a) Section 1 -- Substantive criminal law – _____ 50
(1) Title 1 - Offenses against the confidentiality, integrity and availability of computer data and systems (art. 2-6) _____ 50
(2) Title 2 - Computer-related offenses - (art 7-8) _____ 50
(3) Title 3 - Content-related offenses - (art. 9) _____ 50
(4) Title 4 - Offenses related to infringements of copyright and related rights - (art. 10) _____ 50
(5) Title 5 – Ancillary liability and sanctions, comprises 3 articles - (art. 11-13) _____ 50
b) Section2 – Procedural law – _____ 50
(1) Title 1 - Common provisions -(art. 14-15) _____ 50
(2) Title 2 - Expedited preservation of stored computer data- (art. 16-17) _ 50
(3) Title 3 - Production order - (art. 18) _____ 51
(4) Title 4 – Search and seizure of stored computer data - (art 19) _____ 51
(5) Title 5 – Real-time collection of computer data (art 20-21) _____ 51
c) Section 3 – Jurisdiction – (Art. 22) _____ 51

3. Chapter III – International cooperation _____ 51
a) Section 1 – General principles _____ 51
(1) Title 1 – General principles relating to international cooperation (art. 23) _____ 51
(2) Title 2 – Principles relating to extradition (art. 24) _____ 51
(3) Title 3 – General principles relating to mutual assistance (art. 25-26) _ 51
(4) Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements (art. 27-28) _____ 51
b) Section 2 – Specific provisions _____ 52
(1) Title 1 – Mutual assistance regarding provisional measures (art. 29-30) 52
(2) Title 2 – Mutual assistance regarding investigative powers (art. 31-34) 52
(3) Title 3 – 24/7 Network (art. 35) _____ 52
4. Chapter IV – Final provisions (art 36-48) _____ 52

D. Purpose _____ 52

E. General scope _____ 53

F. Important general concepts or terms left to national interpretation _____ 55
a) Definition of "computer system", "computer data", "service provider" and "traffic data". _____ 55
b) Technology-neutral language opened to future technologies _____ 55
c) All offenses must be “intentional” _____ 55
d) The addition of “qualifying circumstances” in the offense definition _____ 56
e) The term "without right," which appears in all the substantive offense provisions (Articles 2-12) _____ 56

G. Critics _____ 57
1. Main concerns _____ 57
a) ISP mandatory requirement to retain records of their customers’ activity __ 58
b) Absence of a data protection clause _____ 61
c) Lack of dual criminality provision _____ 61
d) Too large definition of “Illegal devices” in Article 6 _____ 62
e) No provision exempting Service Providers for potential criminal liability _ 63
f) Definition of Child Pornography in art. 9 violates Freedom of Speech rights 65
g) Dramatic extension of copyright crimes in an area where National law is very unsettled _____ 66
h) International Cooperation and Investigative Procedures defined too vaguely 67
j) The Convention was kept secret until the release of the 19th draft _____ 68
k) It is unsure if the US will finally ratify it _____ 68
i) Search and seizure of stored computer data lacks necessary procedural safeguards _____ 69
2. High-Tech US corporations vehemently oppose the treaty _____ 70
3. Motion Picture Majors & Computer-crime comparative law experts highly support the Convention _____ 73

Chapter 3 : Which approach to fight cyber-crime efficiently? 75

A. Efficiency of international regulation in the crusade against cyber-crime 75

B. Multidisciplinary approach to fight cyber-crime 77

1. Implementing "future Technology" provisions in actual legislation 77
2. International harmonization of national legislation? 78
3. Educating the "cyber-citizens" ? 80
4. Surveillance of International communication networks ? 81

Conclusion 82

TABLE OF SOURCES

1. Laws

- *The United States Code, Title 18, section 2257*
  [http://www4.law.cornell.edu/uscode/18/2257.html]
- *The November 4th 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms of November*
  [http://conventions.coe.int/treaty/EN/Treaties/Html/005.htm]
- *The 2001 Council of Europe Convention on Cyber-crime (Version No 27 revised)*
  [http://conventions.coe.int/treaty/EN/cadreprojets.htm]
- *The November 20th 1998 Digital Millennium Copyright Act*
  [www.loc.gov/copyright/legislation/dmca.pdf]
- *The May 5th 1949 Statute of the Council of Europe*
  [http://conventions.coe.int/treaty/EN/Treaties/Html/001.htm]

2. Law review articles

- David Johnson and David Post, *Law and Borders – The Rise of Law in Cyberspace*
  [Stanford Law review 48 (1996) : 1367, 1375 ;
  http://www.cli.org/X0025_LBFIN.html]

3. Books

- Bruce Bethke, *Cyberpunk*
  [AMAZING Science Fiction Stories, Volume 57, Number 4, November 1983 ;
  http://www.cyberpunkproject.org/lib/cyberpunk/]
- Buck Bloombecker, *Spectacular Computer Crimes*
  [Dow Jones-Irwin, 1990, p.6]
- Lawrence Lessig, *Codes and other laws of Cyberspace*
  [Basic Books, 1999, p.25 ; www.lessig.org]

4. Newspapers & magazines

- biz.yahoo.com/law
- content.techweb.com
- dev.themoscowtimes.com
- news.cnet.com

- www.apbnews.com
- www.cnn.com
- www.computereconomics.com
- www.computer-forensics.com
- www.fool.com
- www.gamblingmagazine.com
- www.iwar.org.uk
- www.latimes.com
- www.techtv.com
- www.wired.com
- www.zdnet.com

5. Research Institutes

- www.cert.org
- www.experian.com
- www.g7.utoronto.ca
- www.juridicacolombiana.com
- www.jus.unitn.it/transcrime
- www.law.cornell.edu
- www.mcconnellinternational.com

6. Government agencies

- press.coe.int
- stars.coe.fr
- www.coe.int
- www.cybercitizenpartners.org
- www.cybercrime.gov
- www.fbi.gov
- www.usdoj.gov

7. International Organizations

- europa.eu.int
- www.oecd.org
- www.un.org

8. Associations

- www.2600.com
- www.cyberpunkproject.org
- www.dis.org
- www.gilc.org
- www.mpaa.org

9. Databases

- www.imdb.com

10. Corporations

- www.amazon.com
- www.microsoft.com