International Cooperation to Fight Transnational Cybercrime

Ana I. Cerezo[a], Javier Lopez[b], Ahmed Patel[c,1]

[a]Andalusian Institute of Criminology, University of Malaga, Spain
aicerezo@uma.es

[b]Computer Science Department, University of Malaga, Spain
jlm@lcc.uma.es

[c]Centre for Applied Research in Information Systems
School of Computing and Information Systems
Kingston University, Kingston upon Thames, Surrey, UK.
apatelster@gmail.com

ABSTRACT

The ever growing use of computers and information communication technologies in the world of "e-everything" has opened up a range of new activities for crime to take place through electronic means on a global scale, irrespective of national and transnational borders. The effective combating, investigation and prosecution of such crimes require international cooperation between countries, law enforcement agencies and institutions backed by laws, international relations, conventions, directives and recommendations culminating in a set of international guidelines to fight cyber crime. There are many challenges to international cooperation and establishing international guidelines to fight global cyber crime across borders. There is a prerequisite for the harmonization of countries' criminal laws, the sanction of complex jurisdictional issues and the development of new cooperation procedures to challenge cyber crime, its extent and location. It is necessary to identify the perpetrators across borders anywhere in the world, and to investigate and to secure electronic evidence of their crimes so that they may be brought to justice in any compliant jurisdiction with fairness and compliance with human rights standards. This is a daunting task in itself. This paper presents and discusses approaches to overcoming these and other difficulties faced by law enforcement agencies at an international level as well as indicates what possible future work might be required to overcome such difficulties.

Keywords: *Cyber crime, high-tech crime, computer crime, computer forensic, digital investigations, digital evidence, international guidelines, law enforcement, surveillance, privacy, security, encryption, electronic commerce, e-business.*

1. INTRODUCTION

[1] The author carried out the work for this manuscript while visiting the Computer Science Department at University. of Malaga. At present, he is Visiting Professor at Kingston University, UK.

Ana I. Cerezo, Javier Lopez and Ahmed Patel, 2007. *International Cooperation to Fight Transnational Cybercrime. In Proceedings of the International 2nd Annual Workshop on Digital Forensics & Incident Analysis, Samos Greece, August 27, 2007.* ***DOI:*** *10.1109/WDFIA.2007.4299369*

On the positive side, e-business through the Internet has opened a new world of communication for consumers in all facets of life, but on the negative side, it has also created an environment as an open playground for seamless criminal activities on a global scale. The introduction and use of electronic money, virtual banks, exchange marts and shops has become one of the major factors for the development of a new kind of a crime – *transnational cyber crimes*. Crimes can be committed thousands of miles away from the real crime scene. In other words, a cyber criminal does not need to leave his/her own home or cross a national boundary to commit an act in several countries around the globe. The communications may be routed through a variety of ways, ranging from local phone companies, long distance carriers, Internet service providers, wireless and satellite networks, and may go through computers located in several countries before attacking targeted systems around the world. Evidence of the cyber crime may even be stored on a computer in a different country from where the criminal executed the act (Goodman and Brenner, 2002).

Countries need to cooperate because cyber criminals are not confined by national or geographic boundaries, and digital evidence relating to a single crime can be dispersed across multiple regions. While it is important for countries to have cyber crime laws in place, it is equally necessary that these countries have the legal authority to assist foreign countries in an investigation, even if that country has not suffered any damage itself and is merely the location of the intruder or a pass-through site. The idea behind creating international guidelines to fight cyber crime is to facilitate a straightforward process to conduct digital investigations in which computers from more than one country are involved, as well as to eliminate those patches of the world where a cyber criminal is beyond the reach of the national laws (Sieber, 1998).

However, there are many challenges to international cooperation to fight transnational cyber crime. Harmonization of countries' criminal laws, the extent of this kind of crime, locating and identifying perpetrators across borders, securing electronic evidence of their crimes so that they may be brought to justice and other complex jurisdictional issues and procedures, arise at each step. This paper discusses approaches to overcoming these and other difficulties faced by law enforcement on the international front.

2. MAIN CHALLENGES FACED BY LAW ENFORCEMENT

There are many challenges faced by law enforcement agencies. In this section, we analyze the most important ones, such as the lack of harmonization of national criminal laws regarding to cyber crimes and the difficulties to find a clear and comprehensive definition of computer related crime. With the ever-increasing number of cyber crime offences, it is essential to highlight the problems concerning the minimal risk of detection and apprehension. These are lack of training of investigating officials, unknown or anonymous victims, disinclination of victims to report them upon discovering cyber crimes, difficulties of locating and identifying perpetrators across borders and other computer procedural problems of such crimes.

2.1 International harmonization of criminal law and definition of computer related crime

Lack of harmonization of national laws creates too many difficulties. If there is no common understanding of the problem, countries do not know how to respond. For instance, it is difficult to find an agreement on common concepts of cyber crime, computer crime or high-tech crimes.

There has been a great deal of debate among experts regarding what constitutes a computer crime. The intent of different authors to be precise about the scope and use of particular definitions means, however, that the use of these definitions out of their intended context often creates inaccuracies, with a result that a universally agreed definition of *computer crime* has not been achieved to-date.

Computer crime can involve criminal activities that are traditional in nature, all of which are generally subject to criminal sanction. Nevertheless, the computer and the Internet have created a number of potentially new misuses or abuses that may be criminal as well. With respect to traditional forms of crime committed through the use of new technologies, this updating may be done by clarifying or abolishing provisions that are no longer completely adequate, such as statutes unable to create new provisions for new crimes, or as unauthorized access to computers or data networks. Thus, any criminal activity committed exclusively through the Internet should be nominated more specifically a *cyber crime*. The terms *high-tech crime* or *computer-related crime* include both concepts: computer and cyber crime.

2.2 The extent of cyber crime

While it is possible to give an accurate description of the various types of computer offences committed, it has proved difficult to give an accurate overview of the extent of losses and the actual number of cyber criminal acts. Crime statistics do not represent the real number of offences. The amount of these hidden crimes which are unreported or unknown can be attributed to the following reasons:

(1) *High-level information and communications technology*. One of the factors why cyber crime is very difficult to detect is due to the massive compact storage capacity of the computer, manipulation abilities and the speed with which computers and networks operates. In contrast to most conventional types of crimes, victims are informed of the events long after the crime has taken place.

(2) *Lack of training of investigating officials*. Officials often do not have sufficient preparation to deal with problems in the multifaceted environment of data processing.

(3) *Unknown victims*. Most of the time, victims are collective groups. In the case of individual victims, many of them may even fail to realize that a security problem exists and as such they do not have possibilities for responding to incidents of cyber crime.

(4) *Disinclination of victims to report cyber crimes upon discovering.* For companies, mainly in the business area, this reluctance is related to two dilemmas. One, some victims may be unwilling to reveal information about their operations for fear of unfavourable publicity, public embarrassment or loss of

goodwill. Two, other victims may be concerned at the loss of investor or public confidence and the resulting economic effects.

2.3 Difficulties of locating and identifying perpetrators across borders

Cyber crime is infinitely more difficult to prosecute than physical crime. The nature of the Internet, with its far-reaching links and easy anonymity, offers the opportunity for perpetrators to launch attacks and disappear quickly. In addition to requiring cooperation between countries in identifying perpetrators of serious offences of international scope, cooperation is also required for all available resources including law enforcement, military, and intelligence agencies.

2.4 Computer procedural problems

The legal world has been based on paper for so long that adaptation to the digital era has proceeded slowly in relation to the digitalization of the rest of the business world. In the last few years, courts have begun to routinely accept electronic evidence, though always very carefully, knowing that electronic alteration is often simple and that proving it is often hard. Frequently, discussions about electronic evidences become a confrontation among forensic technologists. The replacement of visible and corporeal objects of proof with invisible and intangible evidences in the field of information technology not only creates practical problems but also opens up new legal issues: the coercive powers of prosecuting authorities, specific problems with personal *data* and the admissibility of computer-generated evidence.

2.5 Conflicts of jurisdiction

There are also a number of complex jurisdictional issues to confront, given the multiplicity of countries potentially involved in a cyber crime. How can it be determined in which country the crime was actually committed? Or who should have jurisdiction to prescribe rules of conduct or of adjudication?

2.6 Summing up

Law enforcement typically stops at the borders of nation states and must go through proper legal channels and procedures to receive assistance in pursuing cyber crime investigations and prosecutions. It also becomes necessary to seek the assistance and support of agencies such as Interpol, Europol, etc. to not only help in the investigations and prosecution processes but also in extradition of criminals from one jurisdiction to another. These processes require a complex set of different skill levels for cyber crime investigations, forensic analysis, custody of the evidence, prosecution and extradition within a country, between countries and agencies to be efficient and effective.

Support assistance is also required to accommodate different jurisdictions legal system and procedures. Foreign or external assistance may be needed even if the act is local within a country because the criminal activity transcends the *e-world* of signals, codes, wires and machines across one or more transnational borders. Thus, more often than not, data communications may pass through several countries, requiring law enforcement to seek international assistance and cooperation to ascertain whether the

perpetrator or criminal is a local person or not. This in effect requires international cooperation and harmonisation of procedures and guidelines to combat and prosecute cyber crime (Computer Law Division of the Science and Technology Law Section, 2002).

In subsequent sections of this paper, we describe how some international institutions are creating a system of cooperation trying to solve all these problems.

3. INTERNATIONAL LEGAL INSTRUMENTS

At first glance, the worldwide legislation regarding cyber crime seems to be somewhat of a mess. There are numerous international approaches and coalitions around the world all attempting to create a stable online environment both domestically and internationally.

The lead international bodies are the United Nations, the G-8 Subgroup on High-Tech Crime, the Organisation for Economic Cooperation and Development and the Council of Europe.

3.1 The Organization for Economic Cooperation and Development (OECD)

The first comprehensive international effort was initiated in 1983 by the OECD. It dealt with the criminal law problems of computer related crimes. This organization began the initiative to achieve the harmonization of European computer crime legislation. Between 1983 and 1985, the OECD carried out a study of the possibility of an international harmonization of criminal laws to address computer related crimes. In September 1985, the committees recommended that member countries consider the extent to which knowingly committed acts in the field of computer-related abuse should be criminalized and covered by national penal legislation.

In 1986, the study resulted in a report which surveyed existing laws and proposals to be reformed, and recommended a minimum list of abuses that countries should consider penalizing by criminal law (OECD-ICCP, 1986).

In 1992, the Council of the OECD and two dozen of its member countries approved a *Recommendation of the Council Concerning Guidelines for the Security of Information Systems* intended to make available a foundational information security structure for the public and private areas. The *Guidelines for the Security of Information Systems* were joined to the Recommendation (OECD, 1992).

This framework includes codes of conduct, laws and technical measures. It focuses on the implementation of minimum standards for the security of information systems. However, these *Guidelines* request that Member States establish adequate penal, administrative or other sanctions for misuse and abuse of information systems. The OECD announced on August 2002 the completion of *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (OECD, 2002). These guidelines provide a set of principles that help to ensure the security of today's interconnected communications systems and networks.

3.2 The United Nations

In 1990, the eight *United Nations Congress on the Prevention of Crime and the Treatment of Offenders* approved a resolution in which it requested to Member States to increase their efforts to fight computer related crimes by considering, if necessary, the following measures: modernization of national criminal laws and procedures; improvement of computer security and prevention measures; adoption of adequate training measures; and elaboration of rules of ethics in the use of computers.

The eighth UN Congress also recommended in this resolution that the *United Nations Committee on Crime Prevention and Control* "should promote international efforts in the development and dissemination of a comprehensive framework of guidelines and standards that would assist Member states in dealing with computer-related crime and that it should initiate and develop further research and analysis in order to find new ways in which member states may deal with this problem in the future" (Piragoff, 1998). It also recommended that these issues should be considered by and ad hoc meeting of experts and requested the Secretary-General to consider the possibility of the publication of a technical publication on the prevention and prosecution of computer-related crime.

In 1994, the U.N published the *United Nations Manual on the Prevention and Control of Computer Related Crime* (United Nations, 1994). This Manual studied the phenomenon of computer-related crimes, substantive criminal law protecting privacy, procedural law, and the needs and avenues for international cooperation.

Finally, a Resolution on combating the criminal misuse of information technologies was adopted by the General Assembly on December 4, 2000 (A/res/55/63), that included:

"(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies.

(d) Legal systems should protect the confidentiality, integrity, and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized."

3.3 The G-8 Subgroup on High-Tech Crime

The G-8 has been meeting annually since 1975 to discuss issues of importance, including the information highway, crime and terrorism. In January 1997, under the sponsorship of the US Government, a *Subcommittee on High-tech Crime* was created. The working group meets regularly to discuss related issues. It has focused its efforts on:

a) Establishing an international network of 24-hour high-tech points of contact to facilitate law enforcement communications for investigations. Experts can contact directly with other experts in different countries in order to start all arrangements. In this way, the ball remains in motion. Within 24 to 48 hours, a country receives the data requested.

b) Developing computer forensic principles for circumstances where digital evidence retrieved in one country requires authentication in the courts of another country. The working group experts at present are charting the need and content of a training program[2] for the gathering and preservation of evidence. Thus, all police officers) practice searches and seizing using the same procedure. The evidences also become mutually recognizable by each participating jurisdiction.

c) Making recommendations for tracing terrorist and criminal communications across borders.

In December 1997, they adopted ten *Principles to Combat High-Tech Crime* and ten point *Action Plan to Combat High-Tech Crime*. The first principle was the development of comprehensive substantive and procedural computer crime laws at international level. The goal was to ensure that no criminal receives *safe havens* anywhere in the world. Other principales included are:

- Review legal systems to ensure they appropriately criminalise abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.
- Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.
- Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance, transborder searches and computer searches of data where the location of that data is unknown.
- Develop expedited procedures for obtaining traffic data from all communications carriers in the communication channel and study ways to expedite data internationally.
- Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidences.

In 1999, they established in Moscow principles of transborder access to stored computer data. In July 2000, the G8 issued in Mont Tremblant (Canada) a communiqué which declared, in pertinent part, that it “would take a concerted approach to high-tech crime, such as cybercrime, which could seriously threaten security in the global information society”. The communiqué noted that the G8 approach to these matters was set out in an accompanying document, the *Okinawa Charter on Global Information Society*.

3.4 The Council of Europe (CoE): The Cybercrime Convention

The *Council of Europe* 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. Based in Strasbourg, its work programme includes legal co-operation, social and economic questions, health, education and culture. It provides a forum for both EU and non-EU nations to agree on harmonizing conventions. Some nations from outside Europe have been admitted as observers to the Council, including Canada, Japan and U.S.

[2] See http://jya.com/g8-edicks.htm

Since the late 1980s, the CoE has been working to address the growing international concern over the threats posed by hacking and other computer-related crimes. In 1989, the Council published a study and recommendations addressing the need for new substantive laws criminalizing certain conduct committed through computer networks (Recommendation No. R. (89) 9, which was adopted by the Council on 13 September 1989) (Council of Europe, 1990). This document "recommends the Governments of member states to take into account, when reviewing their legislation or initiating new legislation, the report on computer-related crime (…) and in particular the guidelines for the national legislatures".

The guidelines for national legislatures include a "minimum list", which reflects the general consensus of the *Select Committee of Experts on Computer-Related Crime of the Committee on Crime Problems*, regarding certain computer-related abuses that should be dealt with by criminal law, as well as an "optional list", which describes acts that have already been penalized in some states but on which an international consensus for criminalisation could not be reached.

In 1994, the *Association Internationale de Droit Pènal* adopted a resolution on computer-related crime that elaborated some of the points of the Recommendation and suggested that the list required further refinement and the addition of other types of abuses as candidates for criminalization in light of advances in Information Technology.

This was followed by a Council of Europe second study concerning *Problems of Criminal Procedural Law Connected with Information Technology*, published in 1995, which contained principles concerning the adequacy of criminal procedural laws in this area (Recommendation No. R. (95) 13) (Council of Europe, 1996). Some of these principles covered search and seizure, obligation to cooperate with investigating authorities, the use of encryption and international cooperation. With respect to the latter issue, the report specifically recommended that seizure of data should be negotiated as to how, when and to what extent transborder search and seizure of data should be permitted. It also recommended improved liaison between investigating authorities. Mutual assistance instruments and relations should be used in order to collect computerized evidence, search and seize, provide traffic data related to the source or destination of a telecommunication and intercept a telecommunication. The report examines the problems from the perspective of the investigation of both computer-related crimes and traditional crimes, where evidence may be found or transmitted in an electronic form.

Building on the principles developed in the 1989 and 1995 reports, on April 24, 1997, the CoE established a *Committee of Experts on Crime in Cyberspace (PC-CY)* to begin drafting a binding convention to facilitate international cooperation in the investigation and prosecution of cyber crimes.

Some years later, the *Council of Europe's Committee of Experts on Crime in Cyber-Space* took their assignment seriously to heart by preparing a Draft Convention on Cybercrime. The preparation of this Convention was a long process. It took four years and twenty-seven drafts before the final version, dated, May 25, 2001 was submitted to the *European Committee on Crime Problems* at its 50th Plenary Session, held on June 18-22, 2001.

This is the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks. For that reason, the international discussion about computer crime has covered the CoE efforts with much more detail than other international efforts, mainly because the others have been practically subsumed by CoE work.

The Convention was approved in November 2001 in Budapest. It required parties to establish laws against cyber crime, to ensure that their law enforcement officials have the necessary procedural authorities to investigate and prosecute cyber crime offences effectively, and to provide international cooperation to other parties in the fight against computer-related crime. Moreover, it can be considered as the first international treaty dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. Additionally, it contains a series of powers and procedures such as the search of computer networks and interception.

Regarding the content of the Convention, this encloses four chapters: (I) Use of terms; (II) Measures to be taken at domestic level – substantive law and procedural law; (III) International co-operation and (IV) Final clauses[3].

Chapter I is begins with a description of *data* and its character, demonstrating that the difficulty in understanding the Information Technology-related legal issues is partly due to the fact that we are moving in the borderland between specific and abstract objects.

Chapter II is divided into two sections: Section 1 deals with 'substantive criminal law' and Section 2 deals with 'procedural law'. According to the *Explanatory Memorandum* accompanying the Draft Convention, Section 1 seeks "to improve the means to prevent and suppress computer and cyber crime by establishing a common minimum standard of relevant offences". Parties to the Convention would agree to adopt such legislative and other measures as may be necessary to establish certain activities of computer related crimes under their 'domestic law'. This section covers both criminalisation provisions and other connected provisions in the area of computer and cyber crime. It first defines 9 offences grouped in 4 different categories: (1) *Offences against the confidentiality, integrity and availability of computer data and systems*; (2) *Computer-related forgery and fraud*; (3) *Child pornography*; (4) *Offences related to infringements of copyright and related rights*. The following nine offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights.

The Convention does not itself create substantive criminal law offences or detailed legal procedures. Parties agree to ensure that their domestic laws criminalize several categories of conduct and establish the procedural tools necessary to investigate such crimes under their own national laws.

The scope of Section 2 of Chapter II (procedural law issues) goes beyond the offences defined in Section 1 in that it applies to any offence committed by means of a computer system or the evidence of which is in electronic form. This Section determines the common conditions and safeguards, applicable to all procedural powers in this Chapter.

[3] See the Convention at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

It then sets out the following procedural powers: expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data and interception of content data. Chapter II ends with the jurisdiction provisions.

Chapter III contains the provisions concerning traditional and computer crime-related mutual assistance as well as extradition rules. It covers traditional mutual assistance in two situations: where no legal basis (treaty, reciprocal legislation, etc.) exists between parties – in which case its provisions apply – and where such a basis exists – in which case the existing arrangements also apply to assistance under this Convention. Computer or computer-related crime specific assistance applies to situations, and covers, subject to extra-conditions, the same range of procedural powers as defined in Chapter II. In addition, Chapter III contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Parties.

In the case of extradition, it specifies that the obligation to extradite applies only to offences established in the Convention that are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year or by a more severe penalty. Any country may refuse to extradite an individual if it is not satisfied that all of the terms and conditions of the extradition are adequate.

Finally, Chapter IV contains the final clauses, which – with certain exceptions – repeat the standard provisions in the Council of Europe treaties. The Convention was opened for signature at a signing ceremony in Budapest on November 2001. During the ceremony, thirty countries signed the Convention, including twenty six member States of the Council of Europe, and the four observer States that participated in the negotiations. Since then, additional States have signed. The terms of the Convention require that it will enter into force only once it has been ratified by five countries, at least three of which are member States of the Council of Europe. As of May 2005, the Convention has been ratified by ten countries (Albania, Croatia, Bulgaria, Hungary, Lithuania, the Former Yugoslav Republic of Macedonia, Romania, Slovenia, Cyprus and Estonia) all of which are members of the Council of Europe. Thus, it has entered into force in July 2004.

This Convention will be supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence. This protocol was proposed by some member States. It was the subject of negotiations in late 2001 and early 2002. The Committee of Ministers adopted final text of this protocol on November 7, 2002. The protocol was opened for signature in late January 2003. It is important to note that the protocol is separate from the main Convention. That is, a country that signed and ratified the main Convention, but not the protocol, would not be bound by the terms of the protocol. Thus, its authorities would not be required to assist other countries in investigating activity prohibited by the protocol.

Next, we show a comparative table covering the topics dealt with by main international groups:

	OECD	UN	G8	CoE
Harmonization of European computer crime legislation	X	X	X	X
Elaboration of rules of ethics in the computer using	X	X		
Implementation of standards for the security of information systems (technical measures)	X	X	X	X
Developing computer forensic principles			X	X
Establishing law enforcement communications for investigators			X	X
Seizure of data banks				X
Adoption of training measures	X	X	X	X
Prevention computer crime strategies		X	X	X
Victims				X

4. SOME CONVENTION CONCERNS

From civil liberties and computer industry organisations, the CoE convention is considered fundamentally distorted. It fails to address privacy rights and focuses almost completely on law enforcement demands. As Greg Taylor indicates in his article the convention "includes very detailed and sweeping powers of computer search and seizure and government surveillance of voice, email and data communications, but no correspondingly detailed standards to protect privacy and limit government use of such powers" (Taylor, 2002). This is despite the fact that the major trouble of Internet users worldwide is concerned with privacy of the individual as a fundamental human right (Council of Europe, 2002)

4.1 Access to Encryption Keys

In the last few years, after substantial international discussion over surveillance, privacy and electronic commerce, the use of encryption has been accepted by many countries, except for some traditional dictatorial countries. Clause 4 of Article 19 (Search and Seizure of Stored Computer Data) is a measure requiring that countries approve laws that can compel users to supply their encryption keys and the plaintext of the encrypted files. So far, only a few countries, such as Singapore, Malaysia, India and the UK, have implemented such provisions in their laws. In those countries, police have the power to fine and imprison users who do not provide the keys or the plaintext of files or communications to police. It should be noted that the UK Government faced considerable opposition over its initiative. Such approaches raise issues involving the right against self-incrimination, which is respected in many countries worldwide.

4.2 Mutual Assistance and Dual-Criminality

The CoE convention is unsuccessful on constantly insisting on dual criminality as a prerequisite for mutual assistance between countries. No nation should ask another to interfere with the privacy of its people or to inflict arduous requirements on its service providers to examine acts which are not a crime in the requested nation. Governments

should not investigate a citizen who is acting legitimately, regardless of whatever mutual assistance conventions are in place.

5. INITIAL STRATEGIES TO FIGHT TRANSNATIONAL CYBERCRIME

International organizations efforts have achieved worldwide attention to the problem of transnational cyber crime and promoted international harmonization of legal approaches. Nevertheless, national efforts to combat cyber crime, present in at least forty countries, tend to be at different levels of sophistication and priority. Many of these countries are developing specialized police competences, training and laws. International organizations have considerably contributed to the harmonization of criminal laws as well as of underlying civil law in all of the areas of computer related criminal law reform. The European Community's power to adopt binding directives opened a new age of legal harmonization in Europe. However, the main problem in writing, enforcing, prosecuting, and interpreting cyber crime laws, is the lack of technical knowledge on the part of legislators and experts charged with these duties. Legislators, in most cases, do not have a real understanding of the technical issues and what is or not desirable- or even possible- to legislate. Police investigators are becoming more technically confidence, but in many small jurisdictions, no one in the department knows how to recover critical digital evidence (Chawki, 2005).

Additionally, judges often have a lack of technical expertise that makes it difficult for them to do what courts do: interpret the laws. The fact that many computer related crime laws use unclear language intensifies the problem. The solution to these problems is the same: education and awareness programs. These programs must be aimed at everyone involved in the fight against cyber crime, including legislators and other politicians, criminal justice professionals, IT professionals and the community.

5.1 Technology

Technology is the best way to fight against cyber crimes. The IT industry is hard at work, developing hardware and software to aid in preventing and detecting cyber criminals. Many security technology systems use cryptographic techniques for achieving this (Mao, 2003) (Oppliger, 2005). An investigator might encounter encrypted data or even suspect that the existence of additional data is being concealed using steganography methods (Wainer, 2002). An understating of how cryptography developed and how it works in the computerized environment can be invaluable in investigating and uncovering many types of cyber crime. The technology also needs very skilled personnel to use it accurately and present it in layman terminology in courts of law.

5.2 Cybercrime fighters

It is necessary to educate and train everyone who is involved in preventing, detecting, reporting, or prosecuting cyber crime. A coordinated and concentrated effort must be made to provide investigators, prosecution authorities and the courts with the necessary technical means and expertise to properly research cyber crime. To adopt this strategy will require a dedication to efficient training.

The training necessary for legislators to understand the laws they propose is different from training needed for investigators to find out digital evidence. The latter should receive not only theoretical but also hands-on training in working with data discovery and recovery, encryption and decryption, and reading and interpreting audit files and event logs. Prosecuting attorneys need training to understand the meanings of various types of digital evidence and how to best present it in a court of law during a trial. Teaching computer techniques to individuals in all sectors of the justice system will promote an appreciation of the complexities that have arisen in this new area of enforcement and will foster consistency in the application of criminal sanctions and procedures.

Some EU funded programmes show that training in cybercrime detection, gathering and presentation is taking place in Europe:

a) AGIS[4] programme is one example. It is a framework programme for police and judicial co-operation in criminal matters. The main activities of these transnational projects involve training, studies and research, dissemination of results obtained, establishment of networks, conferences and seminars.

b) CEPOL5 has been set up as a network for improved co-operation of the training institutions for senior police officers in the field of research and science in the EU countries. One of the aims of CEPOL is to establish new form of communications to foster teamwork on police science through a European Police Journal, a weekly newsletter, high-level seminars, a research advisory committee, etc.

c) The Institute of Computer Forensic Professionals (ICFP)[6] mission is the education of the principles and practices in digital forensic. To deal with this objective, the ICFP has designed baseline standardization programs in the several disciplines of computer forensics that can be put into practice trough a variety of different sources.

d) The European Judicial Network (EJN)[7] in criminal matter has been created to improve, helping national judges and prosecutors, judicial cooperation to combat transnational criminality (carrying out cross-border investigation and prosecution). One of the tasks of EJN is to provide a certain amount of up-to-date background information, notably by means of an appropriate telecommunications network.

5.3 Information Technology Professionals

The IT community needs to be educated in many other issues like how laws are made, how crimes are prosecuted and how computer related crime understanding is approached. The first issue includes how IT professionals can get involved at the legislative level by testifying before committees, sharing their expertise, and making

[4] See website: http://europa.eu.int/comm/justice_home/funding/agis/funding_agis_en.htm
[5] See website http://www.cepol.net/KIM/

[6] See website http://www.forensic-institute.org/mission.html
[7] http://europa.eu.int/comm/justice_home/fsj/criminal/network/fsj_criminal_network_en.htm

opinions known to members of their governing bodies. The second one includes how IT professionals can become involved at the prosecution level as expert witnesses. Finally, the third focus is on the need to understand what is and is not against the law, as well as the differences between criminal and civil law, the international nature of the problem, the rights and privileges of the accused and the victim, penalty and law enforcement.

5.4 Victim cooperation

Without the cooperation of cyber crime victims, efforts to suppress these acts can be only partially effective. Reporting incidents to authorities is necessary to discover criminal behaviour. The accurate reporting of cyber crimes provides an additional benefit. The more information the law enforcement community has on new trends of cyber crimes, the better it can adapt existing methods of detection to fight against them. Reporting of crimes would definitely promote public confidence in the ability of the law enforcement and judicial communities to detect investigate and prevent cyber crimes.

5.5 Community

Familiarity with electronic complexity is slowly spreading among the general population. It is necessary to educate the users of computers and network systems. Law enforcement and IT professionals need to work more closely with the community to build a cyber-fighting team that has the skills, the means and the authority necessary to reduce the instances of crime on the Internet. Training in this area and familiarity with the concepts behind complex computer techniques are required before law enforces can operate adequately.

5.6 Informal Social Control

It is necessary to convince the community about the need to track down cyber criminals and expose the problems that these individuals pose to different sectors of the society under varying circumstances. If cyber criminals are shamed rather than admired, some will be less likely to engage in the criminal conduct. A number of potential cyber criminals are attracted by the idea of impressing not only people in their environments but also colleagues in the cyber community. Emphasizing on the fact that a crime in the cyberworld can be of the same high significance and have similar consequences as a crime in the physical world is still a major challenge. There is no doubt that some people will commit crimes regardless of peer pressure. However, this pressure is a valuable tool to reduce the level of cyber crime based on the “everyone does it” argument.

6. CONCLUSIONS AND FUTURE WORK

Cyber crime is a persisting international threat that transcends national boundaries in a manner that renders this form of organized crime a global concern. Cyber crime may take several forms including online fraud, theft and cyber terrorism. It has been seen that amongst the most important reasons that facilitate the perpetration of this crime is the globalization of technology and the revolutionary advancement of information technologies that have impacted on criminal activity. Broadband, wireless technologies, mobile computing and remote access, Internet applications and services, software and file transfer protocols are amongst the tools used by cyber criminals to commit their

crimes. The increasing proliferation in usage of technology assisted criminal activity and cyber crime merits further attention from the global community by enacting the necessary legislative provisions and implementing effective technological and enforcement tools that reduce IT-facilitated criminal activities.

The prevention and prosecution of computer related crime addresses the needs of all societies, with their emerging and still vulnerable information technology structures. Improving international cooperation requires: harmonization of substantive laws (agreement to common concepts of computer related crime), common set of investigative powers, adequate and flexible mutual legal assistance and extradition arrangements. It is admitted that cyber crime should be subject to a global principle of public policy that aims at combating and preventing this crime through raising global awareness and increasing literacy rates, coordinating legislative efforts on national, regional and global levels, and establishing a high level global network of cooperation between national, regional and international enforcement agencies and police forces.

As future work we propose the evaluation of law enforcement and prevention initiatives included in the international legal instruments in order to analyze their efficiency in each of the countries that have to fulfill them. At the same time, it should be of interest to visit the Directives and Laws of the different regions of the world and countries concerning cybercrime handling at all levels and how they would fit into applying better security, privacy handling of personal data while, at the same time, harmonizing the exercises in investigating cybercrime for computer forensic analysis of data for digital evidence presentation, etc. This would help in establishing procedures for better computer forensics handling using IT and designing more effective tools which are legally acceptable and binding. In this sense, closer collaboration among experts from Criminology, Law and Computer Science areas is necessary, though that collaboration must be mainly addressed by government agencies.

REFERENCES

COMPUTER LAW DIVISION OF THE SCIENCE & TECHNOLOGY LAW SECTION (2002), “International Cybercrime Project of the Aba Privacy and Computer Crime Committee”. Retrieved June 13, 2006 from http://www.abanet.org/scitech/computercrime/cybercrimeproject.html

COUNCIL OF EUROPE (1990), Computer-Related Crime: Recommendation No. R(89)9 on Computer-Related Crime and Final Report of the European Committee on Crime Problems, Strasbourg. Retrieved June 13, 2006 from http://cm.coe.int/ta/rec/1989/89r9.htm

COUNCIL OF EUROPE (1996), Problems of Criminal Procedural Law connected with Information Technology: Recommendation N0. R(95)13 and explanatory text, Strasbourg. Retrieved June 13, 2006 from http://cm.coe.int/ta/rec/1995/95r13.htm

COUNCIL OF EUROPE (2002), Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Communities L 201/37.

CHAWKI, M. (2005), "A Critical Look at the Regulation of Cybercrime". Retrieved June 13, 2006 from http://www.crime-research.org/articles/Critical

GOODMAN, M.D. and BRENNER, S. W. (2002): “The Emerging Consensus on Criminal Conduct in Cyberspace”, *International Journal of Law and Technology* 3.

MAO, W. (2003), “Modern Cryptography: Theory and Practice”, Prentice Hall.

OECD-ICCP (1986), “Computer Related Crime: Analysis of Legal Policy”, Information, Computer and Communication Policy, Series núm. 10, Paris. Retrieved June 13, 2006 from http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_1_1_1_1,00.html

OECD (1992), Recommendation of the Council concerning Guidelines for the Security of Information Systems, OECD/GD(92)10, Paris. Retrieved June 13, 2006 from http://www.oecd.org/document/19/0,2340,en_2649_34255_1815059_1_1_1_1,00.html

OECD (2002), Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. Retrieved June 13, 2006 from http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html

OPPLIGER, R. (2005), "Contemporary Cryptography", Artech House.

PIRAGOFF, D. K. (1998), "Investigation of Computer Network Crime", United Nations Expert Meeting

SIEBER, U. (1998) "Legal Aspects of Computer Related Crime (European Commission)"

UNITED NATIONS (1994): United Nations Manual on the Prevention and Control of Computer-Related Crime, New York.

TAYLOR, G. (2002) "The Council of Europe Cybercrime Convention A civil liberties perspective". Retrieved June 13, 2006 from http://www.crime-research.org/library/CoE_Cybercrime.html

WAINER, P. (2002) "Disappearing Cryptography - Information Hiding: Steganography and Watermarking", Morgan Kaufmann.