International Journal of Cyber Criminology
Vol 4 Issue 1&2 January - July 2010 / July - December 2010

The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation

Nancy E. Marion[1]
University of Akron, USA

Abstract

In this paper, the Council of Europe's Convention on Cyber crime is analyzed in terms of its symbolic components. This article describes how the Convention contains the elements of symbolic policy: reassuring the public that action is being taken to thwart the arms of cyber crime, educating the public about cyber crime, acting as a model for state, and acting as a deterrent for those who are considering acts of cyber crime. The analysis raise questions about the effectiveness of CoE Treaty and other policies toward preventing international cyber crime and law enforcement's ability to fight this problem. Some suggestions for a better policy for addressing cyber crime are made.

Keywords: Cyber crime, Council of Europe, Symbolic Policy.

Introduction

In recent years, computers and the internet have evolved into a world-wide phenomenon. Technology now links populations around the world in ways never before possible. The interconnection of many computers, called "cyberspace," allows for citizens in different nations to communicate with ease. Unfortunately, as cyberspace has developed and evolved, so have cyber crimes of all forms. New technology opens opportunities for new crimes, and there has been a tremendous increase in the number of cyber crimes that are reported to officials (Wang, 2007; Nuth, 2008, Walden, 2004). There is, at this point, no accurate data on the incidence of cyber crime against individuals (Moitra, 2005) because many offenses go unreported and/or unrecorded (Williams, 2006). However, it has been reported that there has been a dramatic, yet continual, increase in the number of reported computer intrusions in the past few years (Schell & Martin, 2004, p. 50).

Despite the increase in these crimes, law enforcement has not been able to respond effectively to the threats posed by those who use computers to commit crimes (Kellermann, 2010). It has been said that there is "an apparent lack of effective legislation against cyber crime" (Schell & Martin, 2004, p. 104). There have been many calls for law enforcement to do more to stop the harms from cyber crime, yet police are hampered from acting because of jurisdictional issues or issues inherent in investigating cyber crime.

Another problem for law enforcement is the different cultural standards between nations (Shapiro, 1999). At times, there can be conflict between the moral, political or constitutional differences among nations (Swire, 2005). An act that is considered illegal in

[1] Professor of Political Science, University of Akron, Olin Hall 204 Akron, OH 44325-1904, United States of America. Email: NMarion@uakron.edu

one country is permissible in another. For example, many forms of pornography are legal in the US and are protected under the First Amendment of the Constitution ("Developments in the Law"; Swire, 2005). However, such material is clearly not allowed in other nations. Another cultural difference relates to speech. Speech that is permitted to some in some countries is not permitted in other countries (Lessig & Resnick, 1999). These cultural differences can create problems when trying to control content within cyberspace.

Consequently, content that is legally posted online by a person in one location may be violating the law in a second location where it is being viewed. In these situations, the laws at the location where the Internet activity was launched conflict with the rules at the place where the activity was received (Reidenberg, 2005). Questions then arise as to whether the person in the receiving location can be subject to punishment, or if the person who originally posted the content must modify their activities so they conform to the laws of the more restrictive country. Some have questioned if online activity is sufficient to make a person "present" in a different jurisdiction (Berman, 2002).

This often results in complex jurisdictional issues associated with cyber crimes (Swire, 2005). Traditional law is based on physical geography and boundaries, but cyber crimes easily intersect and cross national borders. Laws that govern cyber crime are often based on territory, so that they apply only within the country where the law was passed (Brenner & Schwerha, 2004). There are often questions about what country or agency has the responsibility to investigate, prosecute or even punish offenders, or what laws should apply (Kohl, 2002).

Many countries do not have adequate laws to criminalize cyber crimes. This became evident after it was discovered that a man from the Philippines unleashed the fatal "I Love You" virus. At the time, there was no Philippine law that specifically addressed computer crimes and the offender went free. About a month later, the Electronic Commerce Law was passed by the Philippine Congress. Those countries that have passed laws against cyber crimes find that the laws are obsolete, inconsistent or conflict with other laws (Gercke, 2009). For instance, the UK Computer Misuse Act of 1990 was criticized because the concepts were outdated and it did not cover new forms of computer crimes (Coleman, 2003). It has been noted that less than one in five countries have amended their laws to include new forms of cyber crimes ("Cyber crime laws," 2001). Most often, however, nations have adopted different legal rules. This means that when a cyber crime is committed, there is the possibility that many laws will apply, or that none will (Swire, 2005). To make matters worse, it is difficult for legislators to keep up with cyber criminals who are always devising new ways to use the computer to commit crime (Sinrod & Reilly, 2000)

Another problem for law enforcement is that cyber crimes are extremely difficult to investigate, prosecute and punish. There is often poor cooperation from web hosts when crimes are being investigated ("Wired Society," 2002), and it is sometimes difficult to gather evidence of an electronic crime so that the offender might be brought to justice. The acquisition and preservation of evidence that will prove an offender's identity and possible crimes is difficult to collect. Countries vary widely in their ability to investigate and punish cyber crime, and they vary in how technological savvy they are. At the same time, determining the intent of the offender is also a challenge. Hackers sometime illegally enter networks for fun rather than with criminal intent ("Wired Society," 2002).

Because of these problems, it became clear that current criminal laws to deter cyber crimes are not sufficient or specific enough. Each country has its own laws regarding cyber crimes (Ross, 2010) and there is no consistency amongst them. Law enforcement actions to prevent cyber crime have been lacking and those agencies have not adequately responded to the harms caused by cyber crimes (Katyal, 2001). Most law enforcement has not focused on the long-term threats from cyber crime to businesses, governments, and individuals (Speer, 2000).

Consequently, there have been more calls for increased regulation and governance of internet activity. However, even though all the nations agree that cyber crimes pose a significant problem, there is little consensus about how to solve that problem (Goodman & Brenner, 2002). One group that reacted to the calls was the Council of Europe. One significant policy that was drafted to address the problem is the Council of Europe's Convention on Cyber crime. The Convention calls on member states and observer nations to create new laws that address different crimes on the internet, and forces increased cooperation between law enforcement agencies of different countries in order to sustain more effective investigations of criminal offenders.

In this paper, the Council of Europe's Convention on Cyber crime is analyzed in terms of its symbolic components. This article describes how the Convention serves to reassure the public that action is being taken to thwart the arms of cyber crime, educate the public about cyber crime, act as a model for state, and act as a deterrent for those who are considering acts of cyber crime. This analysis raise questions about the effectiveness of CoE Treaty and other policies toward preventing cyber crime and law enforcement's ability to fight this problem. Some suggestions for a better policy for addressing cyber crime are made.

Convention on Cyber Crime Treaty

In 1997, the Council of Europe (CoE), an organization of 47 European countries, appointed a Committee of Experts on Crime in Cyberspace to identify and define new crimes, jurisdictional rights and criminal liabilities concerning the Internet. Canada, Japan, South Africa and the U.S. were also invited to participate in the discussions as observer nations. The goal was to create a set of standard laws concerning cyber crimes for the global community and create a common criminal policy to protect against cyber crimes. The country representatives sought to make it easier for law enforcement to cooperate in collecting evidence in investigating computer crimes (Furnell, 2002).

The resulting Convention on Cyber crime of the CoE was passed in June 2001 and is currently the only global document on this issue (CoE, 2001). The document attempts to define cyber crimes and to develop policies to prevent particular crimes committed with use of the internet. The treaty includes provisions geared toward fighting terrorism, child sexual exploitation, organized crime, copyright infringement, hacking, and internet fraud. The Convention also acts as a framework for international cooperation between countries in investigating and prosecuting possible cyber crimes. Other portions of the treaty include descriptions of extradition procedures.

If countries agree to the treaty, they must agree to pass legislation to address particular computer crimes (Gold, 2000; Yam, 2001). They also agree to provide international cooperation to other parties in the fight against computer-related crime by providing a contact for countries that need immediate help in investigating a computer crime (Boni, 2001). The treaty gives police agencies expanded powers to investigate and prosecute

computer crimes when the offense crosses national borders ("US Ratifies," 2006). On November 7, 2002, the Council of Ministers adopted an additional protocol, separate from the main Cyber crime Convention, which addresses racist and xenophobic materials committed through computer networks (CoE, 2001).

After the CoE finalized the proposed treaty, it was signed by twenty-six member states in Budapest, Hungary. The countries who enjoyed "observer status" (the U.S., Mexico, Japan, and Canada) had the option to sign it. It was then sent to countries for ratification (Hancock, 2000). The treaty came into effect when five states, including at least three CoE member states, ratified it ("Convention on Cyber crime Update," 2002). The Convention entered into force on July 1, 2004. To date, the Convention has been ratified by twenty-four countries; twenty-three of whom have also signed it but not ratified it (Kirk, 2009a; Kirk, 2009b). The last country to ratify the treaty was Germany, which did so on March 9, 2009. The U.S. Senate ratified the treaty on August 3, 2006. Although it appears to be a significant policy to attack cyber criminals, when examined closely, it is clear that the treaty has many elements of symbolism in it.

The Treaty is organized into four chapters. Each chapter includes different sections, which are then broken down into articles. Each chapter discusses a different aspect of the treaty, with specifics given in the articles. In all, there are 48 articles in the treaty. The treaty with complete description of the chapters, titles and articles is available at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (CoE, 2001).

Cyber Crime Treaty as Symbolic Legislation

While the Convention on Cyber crime is a genuine attempt at addressing the problems of international cyber crime, the treaty remains largely a symbolic policy and thus will have a limited effect on cyber crime in the long-term. It clearly has elements of the four functions of symbolic policies. Symbolic policies were first defined by Edelman (1964), who recognized that some policies are created to make the public feel as if something is being done to solve problem when in actuality the policies do not make any real or significant change, nor do they get to the bottom of the specific issue at hand.

1. Function of reassuring public

Symbolic policies have many functions (Stolz, 1983). The first is to serve a reassurance function to the public that the lawmakers are "getting tough" on a problem (Zimring & Hawkins, 1973). Symbolic policies serve to reassure the public that something can be done to solve a problem quickly and easily when that may not be the case (Scheingold, 1984; Marion, 1997). The CoE cyber crime treaty clearly has elements of serving to reassure the public that action is being taken against cyber crime. The treaty itself proves to the public that the Council of Europe and other nations prepared a plan to halt the damage caused by cyber crimes, and the ratification by the states shows the same thing. Thus, there has been action by many different government units to solve the problem. The members of those bodies are demonstrating that they, like citizens, are clearly worried about cyber crime and they passed a new policy to address it.

However, questions arise as to if the treaty will be effective in solving the problem. It is not clear that the provisions in the treaty will be fully implemented, and therefore the treaty will not solve the problem at hand. To begin with, almost ten years after the original treaty was passed, only about half of the member states have ratified it in their home legislatures. The treaty was originally passed in 2001, and as of early 2010, only

twenty-four of forty-seven member states have ratified it. Although it has been "ceremonially signed" by many countries, it has not been concretely accepted" (Hilley, 2005). In fact, formal adoption of harmonized legal rules has not been especially widespread (Swire, 2005). This is indicative of being symbolic policy because although the treaty was "ceremonially signed," no further action was taken to ratify or enact the provisions of the treaty in many countries. Therefore, to the public, it appears as if the CoE members created new policies to deal with internet crime, but the provisions of the treaty are not being implemented in about half of the member states let alone non-member states.

a. Problems related to Countries

Many countries have not formally agreed to the treaty, and therefore are not required to enforce the treaty. Further, even for those countries that have ratified the treaty, the provisions may not be carried out fully. There are many objections to the treaty that will hamper full enforcement of it. Further, there are too many inconsistencies from one country to another, making cooperative efforts between countries difficult. Countries will, more than likely, enforce the laws differently if at all.

Further, even if a country ratified the treaty, it does not mean that they will implement the laws. There are problems with enforcement of the treaty as there are no international police to enforce the provisions. The treaty relies on international cooperation in investigating and punishing cyber criminals. The case could easily be made that some countries will investigate with more vigor than other countries, or will investigate some offenses more than others. Plus, there are some counties that do not have the resources to implement the law. Since treaty is not legally binding on the states and harmonizing measures will have only limited effect (Walden, 2004). Although such cooperation between governments sounds effective in theory, it is very difficult to achieve in practice (Katyal, 2001, p. 1096).

Differences exist between countries when it comes to investigating cyber-offenses. Some lack adequate resources, the necessary training with the appropriate level of sophistication, or even the desire to understand the nature of cyber crimes. In some cases, some countries may feel they do not have the jurisdiction over these offenses, thus leaving it to another agency to investigate allegations. Although some countries have established agencies to coordinate cyber crime investigations, others have not. For example, the European Union created a high-tech organization referred to as ENISA, which is responsible for coordinating cyber crime investigations within member countries (Ross, 2010). But not all countries have such an organization and have no plans to do so.

Differences also exist concerning the collection, preservation and analysis of evidence. Countries have varying standards for searches and seizures. In the United States, the requirements for obtaining a search warrant for telecommunications are quite stringent. Sometimes law enforcement officials overlook the regulations concerning warrants, but in those cases where investigators are found to have violated the law, the charges against the offender may be dropped and he or she leaves the criminal justice system. Some countries do not allow for online investigations of possible offenders, because they are deemed to be an excessive use of police power. Because of the differences in search and seizure policies, provisions of the CoE treaty may not be enforced equally or consistently (Grabosky, 2007).

Some critics of the Convention argued that the signatory countries are not the "problem" countries (Schell & Martin, 2004). Many countries do not share the urgency to combat cyber-crime. They have different values or have more pressing problems that need attention. These countries will give cyber criminals a safe haven to operate (Sinrod & Reilly, 2000). They will continue to do this, even if the treaty is ratified by more countries.

Many people have concerns about other aspects of the treaty, also prohibiting full enforcement. First is that there is no dual criminality provision. This means that the U.S. must compel a search and seizure against a person in the U.S. at the demand of a foreign government when the person's activity is a crime in that foreign country but legal in the US. In other words, the act can be legal in America, but illegal in another country, and the person carrying out that activity can be investigated by U.S. officials at the request of another country. For example, this might include hate speech which is protected in the US but illegal in Germany ("Senate Ratified Convention," 2006). More than likely, U.S. law enforcement will hesitate to investigate activity against a citizen if the behavior was legal (Magnin, 2001).

Some countries may even provide a safe haven for cyber criminals who will continue to perpetrate harm on unsuspecting victims by using technology. Cyber criminals will go to those countries with poor law enforcement that have little armory to defend against cyber crime ("Schneier," 2007; Katyal, 2001: 1029). For example, there is no legislation in North Korea against cyber crimes, and offenders are relatively safe from prosecution there (Archik, 2002). Even if laws are passed in those countries that currently have no laws or do not enforce them, there will always be havens for those trying to steal or peddle data (Sharma, 2005). Generally speaking, even if the provisions of the treaty are all carried out, chances are that cyber criminals will adapt and find ways around the new laws and will find ways to evade law enforcement to escape prosecution.

Along those lines, it is often the case with cyber crime that these types of offenses come to the attention of the authorities while they are in progress, or more than likely, after the offense has been carried out and the harm done. In both cases, it is difficult to determine who the offender really was or their exact location (Grabosky, 2007). Investigating these offenses and finding and punishing offenders requires multiple resources in terms of money and personnel for investigation and prosecuting the crimes. That means that many cyber criminals will simply go free.

b. Problems related to Internet Service Providers

Since the treaty requires signatory states to have broad powers of surveillance and interception, as well as powers to require the assistance of service providers (Coleman, 2003), it makes it appear as if the provisions of the treaty will be helpful for reducing cyber crime. Some critics argue instead that it is really a way to increase the powers of the police. By increasing the investigatory powers of law enforcement, governments are also enhancing their control of the Internet and promoting surveillance in the name of preventing "cyber-crimes," "information warfare" or protecting "critical infrastructures" (Privacy International ; "Hearing Before the Committee on Foreign Relations," 2004). This leads to a potential danger that the treaty could be used by some countries to conduct surveillance on each other's citizens—even if they are suspected of actions which are not a crime in their home country (ZDNet UK).

Privacy concerns resulting from the increased investigatory responsibilities are another concern that may prohibit the law from becoming fully implemented. Under the provisions of the treaty, Internet Service Providers (ISPs) will be required to retain records regarding the activities of their customers. Some argue that this poses a significant risk to the privacy and human rights of Internet users (Magnin, 2001). The treaty imposes liability on ISPs for third party content that places an unreasonable burden on providers of new network services and may encourage inappropriate monitoring of private communications. Further, ISPs may be held criminally liable for failing to monitor customer or user content, or for the criminal actions of their employees (Magnin, 2001). European critics of the treaty are concerned about the right to transfer European citizens' personal data outside of Europe to non-European authorities (Yam, 2001).

There are many concerns about the lack of consideration given to personal data protection issues by the provisions (Hilley, 2005). Many civil rights organizations have indicated their concerns about the treaty, primarily because it broadened the powers of government around the world. Civil liberties groups pointed out that the Convention undermines privacy rights and granted too much surveillance power to authorities. Different American organizations point out that the Convention allows for conducting surveillance and searches that would not be permitted by US law (Schell & Martin, 2004). The Global Internet Liberty Campaign wrote a letter with their concerns (Wales, 2000).

c. Inconsistencies of the CoE Treaty

Although the treaty tried to define terms and create some sort of consistency, critics of the treaty say that its provisions lack clarity and are unclear (Yam, 2001) and provide only very vague definitions of some of the terms (Perera, 2001; Walden, 2004). For example, the definition of "Illegal Devices" 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 (Magnin, 2001). As another example, the term "service provider" is defined in the treaty as any public or private entity that provides a service via the computer or any entity that stores data for such an online service. Critics say that under this definition, a pizza delivery operation could be considered a service provider (Yam, 2001). Because the terms are so broad, the treaty will be difficult to enforce.

Even though the treaty outlines specific laws that need to be passed in order for a country to be part of the treaty, there will be no consistency in how those laws are written from country to country. The definitions and interpretations of key terms will vary greatly from nation to nation. The parties can take a wide approach to their legislation, and there will be many differences in the legislation they pass. For example, the concepts of fraud vary greatly from nation to nation, as do the definition of pornographic material. Some countries are prohibited constitutionally from passing certain laws. Additionally, Congress cannot impose restraints on free speech over the internet (Simon, 1998). This also leads to inconsistencies and difficulties with enforcement.

Nations are also permitted to opt out of certain provisions of the treaty, leading to inconsistencies from one country to another. When the US Senate was considering the treaty, they chose to opt out of some provisions. The U.S. reserved the right not to apply certain paragraphs of the treaty, and reserved the right to impose other remedies in lieu of criminal liability as suggested in the treaty ("Executive Report of Committee," 2005). This also leads to inconsistencies in the cyber crime legislation between countries.

More inconsistencies result from the fact there the final treaty contains many provisions that were not agreed upon by the member states. There are clear divisions among council members and observers on what constitutes certain criminal acts under the proposal ("Convention on Cyber crime Update," 2002). Under the treaty, cyber crimes will continue to be difficult to trace and prosecute. Computer data is highly volatile, so a few keystrokes or by operation of automatic programs, it can delete key information, rendering it impossible to trace a crime to its perpetrator or destroying critical proof or guilt. Cyber criminals have discovered that it is easy to commit a crime in one jurisdiction and then hide behind the jurisdiction of another, especially developing and poor countries (Sinrod & Reilly, 2000). In fact, cyber crime is rampant in developing countries because there is a lack of law enforcement to tackle the issue. Computer criminals now and in the future can easily to move from one place to another, seeking haven in countries that do not ratify the treaty or those who choose not to enforce it. They will route their attacks through countries where there is no comparable legislation and they are relatively safe from prosecution (Yam, 2001; Archick, 2006).

2) Moral educative function

There are other functions of symbolic legislation that are apparent in the cyber crime treaty as well. One is to serve a moral educative function. The treaty is serving to educate people in all countries about what is right and wrong behavior concerning the internet. Since the Internet is a new phenomenon, some people are unsure as to what is "appropriate" and "inappropriate" behavior, and need to have a more defined understanding of acceptable and unacceptable behavior related to it. By reading the treaty, one would understand more about the problem of cyber crime. The treaty is also helping to create a "moral consensus" both within a country and internationally about criminal behavior on the internet and provide definitions of offenses.

Although no punishments are set in the cyber crime treaty, they are set in the legislation created in individual countries. This is serving to help citizens' associate negative consequences with the crimes, reinforcing the idea that the behavior is bad or wrong. The laws also serve to reassure those who do not commit cyber crime that they are acting appropriately and distinguish them from those who choose to commit criminal acts. The treaty is also effectively educating the public about the problem of cyber crime and possible solutions. It is providing people with a better understanding of the issues at hand and the potential policy options for solving the problem.

3) Function as model for other states

The third purpose of symbolic legislation is to serve as a model for the states. The CoE treaty is obviously fulfilling this role. For those countries that had no previous laws pertaining to cyber crime, or that had outdated laws, the treaty is acting as a model for the state legislatures to emulate—it is providing some suggestions for possible laws. They provisions of the treaty delineate very specifically what laws each nation must pass in order to effectively fight cyber crime. Thus, the Council of Europe is modeling what laws should be passed in order to fight cyber crime effectively. It serves as a guideline for any country that is developing legislation to prevent against cyber crime (Silver, 2001; Coleman, 2003).

Legislation against cyber criminals passed in the United States Congress in 2002 as part of the Homeland Security Act was called the Cyber Security Enhancement Act. It requires

stricter penalties for computer-related crimes such as life in prison for offenses that result in bodily harm or death. In 2003, the U.K. introduced legislation requiring people to "opt in" to unsolicited e-mails. This was called the Privacy and Electronic Communications Regulations. This law outlawed "spam" e-mail without the prior consent of the recipient. In the U.S., Congress passed The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, or the CAN-SPAM Act that came into effect on January 1, 2004. This required senders to provide an opt-out option for recipients (Kigerl, 2009). Like the law in the U.K., this legislation imposed limits and criminal penalties for the transmission of unsolicited electronic mail.

Other countries already had laws that prohibited cyber crimes. For example, many laws in many countries criminalize the traditional production and physical distribution of child pornography. For those countries, the treaty forced the legislative body to re-examine their current laws and possible update it. This happed during the ratification process in the US, it was decided that there were already sufficient laws on the books that were in compliance with the Convention, so no new legislation was required ("Senate Ratifies Convention," 2006; "Hearing Before the Committee,"). Nonetheless, it forced the Senate to examine the current laws and determine if they were up to date.

4) Function as deterrent to future criminal behavior

The final element of a symbolic policy is to serve as a deterrent to future criminal behavior. The role of the treaty as a deterrent is in question. The Convention did not set any level of sanction for the offenses they outlined. Instead, each country was allowed to set that in accordance with their penalty structure. This is something that has been perceived as a weakness of the treaty (Coleman, 2003). The deterrent, then, would be based on the punishment as set by an individual nation rather than an international body. Nonetheless, people in those countries that have developed punishments for cyber crimes may be deterred from committing cyber crime because of the potential for punishment.

Further, because the treaty was not signed by all countries, it is clear that there are a significant number of countries not passing or enforcing the laws against cyber crime. For it to be a deterrent, more states will have to sign the Convention and abide by its mandates (Archick, 2006).

Suggestions

Unfortunately, the internet is difficult to regulate because it is world-wide and does not regard boundaries. Because no one body of law has precedence over the entire internet, cyber crimes are not offenses that can be solved through government action (Coleman, 2003). New treaties are not enough. Comprehensive policies need to be enacted on many fronts in order to have a complete and effective fight against cyber crimes. A serious fight against cyber crimes also needs to be addressed on many levels. On a large scale, relevant laws need to be passed, and on a more local level, better management practices should be adopted to control these new crimes (Backhouse & Dhillon, 1995). The following are some of the suggestions for better policy on cyber crimes.

1. First, business and organizations must take an active role in fighting cyber crimes. In many cases, security breaches are often the result of poorly implemented internal processes, a lack of staff awareness or lax control. Therefore, businesses need to implement their own crackdown on cyber crimes (Lawrie, 2002). Businesses and organizations should take responsibility for identifying potential

security issues within their computer systems and for creating and implementing plans to deal with those risks. Overall, security must be improved within the organization itself (Coleman, 2003). It has even been suggested that companies sponsor a "hack-in" contest where people can try to hack into sites as a game or security exercise in order to identify potential holes in a sight and create a more security network. Obviously, all sensitive information would be removed prior to the contest (Wible, 2003).

2. All industries related to computer technology should be encouraged to produce new and more secure technologies to protect against further cyber crimes. These should be constantly evolving as cyber criminals devise new ways to commit crimes on the internet, or as new crimes evolve.
3. System owners and users must be made aware of the threats and vulnerabilities of the internet (Coleman, 2003). They need to be conscious of the potential offenses and take precautions when possible. They should also report threats or harms when they occur.
4. The existing laws need to be regularly updated laws as new technologies are developed and new crimes are devised or as cyber criminals come up with new ways to evade the police.
5. Qualified and knowledgeable private and or government investigators should be trained who can keep abreast of advances in technology and who establish specialized knowledge in investigating computer crimes (Chung et al Archick, Kristin, 2006, 2004). They could look for electronic vulnerabilities and identify potential areas of concern which could then be address before harm could be done (Wible, 2003).
6. Investigations need to be based on cooperation among police from all countries involved. Interpol is one agency that can provide an exchange of information and cooperation at the international level, but law cooperation from all law enforcement is essential in implementing future cyber crime laws (Brenner & Schwerha, 2004). At the same time, the US needs to engage its diplomatic, economic, military and informational stems to pursue global partnerships that can assist in providing a more secure cyberspace (Kellermann, 2010).
7. ISPs may prevent crime as well. The internet gives a criminal the ability to commit a crime cheaply and easily, have access to millions of potential victims, and the ability to end the activity instantaneously. They can hide their actions by using systems in several countries. ISPs can randomly monitor web traffic to look for suspicious activity, especially with regards to critically important sites such as military computers or power grids. They can scan web sites hosted to their networks for illegal programs, scan e-mails for viruses, and even build software and hardware constraints into their systems. ISPs can assist in developing profiles of hackers, and can, if need be, bounce certain subscribers from the network. The ISPs can report instances of potential computer offenses and make it easier for law enforcement to investigate cyber crime (Katyal, 2001, pp. 1095-7).
8. Finally, the need for global international regulation of the internet is clear. The involvement of groups such as the United Nations or other geographic communities, such as the European Union, is key to effective laws pertaining to cyber crime, and enforcement thereof. Because of the global aspects of the

internet, no single law in a single country will effectively reduce the harm caused by internet criminals.

Conclusion

There is no doubt that cyber crimes are potentially damaging offenses, with potentially serious ramifications. Since computer-related crimes affect practically all nations (Backhouse & Dhillon, 1995), there is no question of a need for updated, harmonized laws that involve international cooperation to fight crime in cyberspace (Walden, 2004). The international community cannot choose to ignore cyber crimes, as that would only encourage the attackers' greed and more serious criminal behaviors will result (Wang, 2007). The CoE treaty is an important step in the right direction (Boni, 2001) and is the most significant treaty to address computer crimes (Walden, 2004). Although an international perspective in fighting cyber crimes is vital, it is, at the same time, difficult. In making the treaty, the CoE Convention convened representatives from many nations, both from their members and outside nations, to discuss and debate the definition of certain acts committed on the internet and then define what the most appropriate actions would be to institute a fair, yet effective, fight against cyber crimes. They recognized the need for a consistent international approach to fighting cyber crimes that included cooperation between law enforcement agencies to investigate offenses.

However, because the Convention is largely symbolic, its long-term effectiveness must be brought into question. There are problems relating to the definitions of terms in the treaty, privacy issues, and the investigatory powers created in the document. Further, international laws requiring cooperation between nations are difficult to enforce. Overall, the treaty leaves too many holes in terms of the lack of definitions and inconsistencies, and has many gaps that will allow criminals to continue to commit criminal offenses. There are many ways for criminals to continue to exist and operate even after the treaty is in force. In order for the treaty to be effective, more countries will need to sign it and ratify it and turn it into national law (Schell & Martin, 2004, 103). Until then, cyber crimes will not be impacted by the treaty in any significant way.

References

Archick, K. (2006). Cyber crime: The Council of Europe Convention. *Congressional Research Service*, Report for Congress. September 2006. Retrieved on 15th April 2011 from http://www.fas.org/irp/crs/RS21208.pdf

Backhouse, J., & Dhillon G. (1995). Manager Computer Crime: A Research Outlook. *Computers and Security*, 14, 645-651.

Berman, P. S. (2002). The Globalization of Jurisdiction. *University of Pennsylvania Law Review,* 151(2), 311-545.

Boni, B. (2001). Creating a Global Consensus Against Cyber crime. *Network Security,* 2001 9, 18-19.

Brenner, S., & Schwerha, J. J. (2004). Introduction—Cyber crime: A Note on International Issues. *Information Systems Frontiers, 6*(2), 111-114.

Chung, W., Chen, H., Chang, W., & Chou, S. (2006). Fighting cyber crime: a review and the Taiwan Experience. *Decision Support Systems,* 41, 669-682.

Coleman, C. (2003). Security Cyberspace—New Laws and Developing Strategies. *Computer Law and Security Repor*t, *19*(2), 131-136.

Convention on Cyber crime Update. *Computer Fraud and Security,* (2002), 4, 4-5.

Council of Europe. (2001). Convention on Cyber Crime. Retrieved on 12th May 2011 from http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Cyber crime Laws Need Overhaul 2001. *Network Security* 1, 3.

Developments in the Law: The Law of Cyberspace. *Harvard Law Review*, *112*(7), 1574-1704.

Edelman, M. (1964). *The Symbolic Uses of Politics*. Chicago: University of Illinois Press.

Executive Report of Committee Congressional Record—Senate November 9, 2005.

Furnell, S. (2002). *Cyber crime: Vandalizing the Information Society*. Boston: Addison-Wesley.

Gercke, M. (2009). Europe's Legal Approaches to Cyber crime. *ERA Forum* 10: 409-420.

Gold, S. (2000). G8 Cyber crime Meeting Seeks Global Cooperation, *Newsbytes*, May 15.

Goodman, M., & Brenner, S. (2002). The emerging consensus on criminal conduct in cyberspace. *UCLA Journal of Law and Technology*, 3. Retrieved on 12th May 2011 from www.lawtechnournal.com/articles/2002/03_020625_goodmanbrenner.pdf.

Grabosky, P. (2007). *Electronic Crime*. Upper Saddle River, New Jersey: Pearson/Prentice Hall.

Hancock, B. (2000). US and Europe Cyber crime Agreement Problems. *Computers and Security, 19*(4), 306-7.

Hearing Before the Committee on Foreign Relations United States Senate. June 17, 2004, U.S. Government Printing Office.

Hilley, S. (2005). Pressure Mounts on US Senate to Pass Cyber crime Treaty. *Digital Investigation,* 2, 171-174.

Katyal, N. K. (2001). Criminal Law in Cyberspace. *University of Pennsylvania Law Review, 149*(4), 1003-1114.

Kellermann, T. (2010). Building a Foundation for Global Cybercrime law Enforcement. *Computer Fraud and Security,* May, 5.

Kigerl, A.C. (2009). CAN SPAM Act: An Empirical analysis. International *Journal of Cyber Criminology, 3*(2), 566-589.

Kirk, J. (2009a). Germany Ratifies Cyber crime Treaty. *PC World*, March 10. Retrieved on 1st April 2010 from http://www.pcworld.com/printable/article/id,160956/printable.html

Kirk, J. (2009b). Countries Move Forward on Cyber crime Treaty, *PC World*, March 11. Retrieved on 1st April 2010 from http://www.pcworld.com/printable/article/id,161067/printable.html

Kohl, U. (2002). Eggs, Jurisdiction and the Internet. *The International and Comparative Law Quarterly*, *51*(3), 555-582.

Lawrie, L. (2002). A Twin-Pronged Approach in the Fight Against Cyber crime. *The Scotsman*, May 8, 5.

Lessig, L., & Resnick, P. (1999). Zoning Speech on the Internet: A Legal and Technical Model. *Michigan Law Review, 98*(2), 395-431.

Magnin, C. J. (2001). The 2001 Council of Europe Convention on Cyber-Crime: An Efficient Tool to Fight Crime in Cyber space? LLM Dissertation.

Marion, N. E. (1997). Symbolic Policies in Clinton's Crime Control Agenda. *Buffalo Criminal Law Review,* 1, 67-108.

Moitra, S. (2005). Developing Policies for Cyber crime, *European Journal of Crime, Criminal Law and Criminal Justice, 13*(3), 435-464.

Nuth, M. S. (2008). Taking Advantage of New Technologies: For and Against Crime *Computer Law and Security Report,* 24, 437-446.

Perera, R. (2001). Cyber crime Treaty ready for signatures. CNN.com/Sci –Tech Retrieved on 1st April 2010 from http://www.archives.cnn.com/2001/TECH/internet/11/12/cybercrime.treaty.idg/index.html

Privacy International, Cyber crime. Retrieved on 1st April 2010 from http://www.privacyinternational.org/index.shtml?cmd[342][]=c-1-Cyber+Crime&als

Reidenberg, J. R. (2005). Technology and Internet Jurisdiction. *University of Pennsylvania Law Review, 153*(6), 1951-1974.

Ross, J. I. (2010). *Criminal Investigations: Cyber crime*. New York: Chelsea House.

Scheingold S. A. (1984). *The Politics of Law and Order: Street Crime and Public Policy*. New York: Longman Press.

Schneier: Cyber crime Lurks in Developing Countries, (2007). *Computer Fraud and Security*, March, 4.

Schell, B. H., & Martin, C. (2004). *Cyber crime: A Reference Handbook*. Santa Barbara, California: ABC-CLIO.

Senate Ratifies Convention on Cyber crime (2006). *Tech Law Journal*. Retrieved on 1st November 2010 from http://www.techlawjournal.com/topstories/2006/20060803b.asp

Shapiro, A. (1999). The Internet. *Foreign Policy,* 115, 14-27.

Sharma, A. (2005). World Seeks a Wider Web Role. *Congressional Quarterly Weekly Report* Nov 14, 2005, 3042.

Simon, G. E. (1998). Cyberporn and Censorship: Constitutional Barriers to Preventing Access to Internet Pornography by Minors. *The Journal of Criminal Law and Criminology, 88*(3), 1015-1048.

Silver, O. (2001). European Cyber crime Proposal Released. *Computer Fraud and Security,* 2001 (5), 5.

Sinrod, E. J., & Reilly, W. P. (2000). Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws. *Santa Clara Computer and High Technology Law Journal, 16*(2), 1-53.

Speer, D. L. (2000). Redefining Borders: The Challenges of Cyber crime Crime, *Law and Social Change,* 34, 259-273.

Stolz, B. A. (1983). Congress and Capital Punishment: An Exercise in Symbolic Politics. *Law and Policy Quarterly, 5*(2), 157-180.

Swire, P. P. (2005). Elephants and Mice Revisited: Law and Choice of Law on the Internet, *University of Pennsylvania Law Review*, *153*(6), 1975-2001.

U.S. Ratifies International Cyber crime Treaty, *Computer Fraud and Security*, November 2006, 2-3.

Walden, I. (2004). Harmonising Computer Crime Laws in Europe. *European Journal of Crime, Criminal Law and Criminal Justice, 12*(4), 321-336.

Wales, E. (2000). Draft Council of Europe Cyber crime Convention Upsets Civil Rights Bodies. *Computer Fraud and Security Issue,* 12, 7.

Wible, B. (2003). A Site Where Hackers are Welcome: Using Hack-In Contests to Shape Preferences and Deter Computer Crime. *The Yale Law Journal,* 112(6), 1577-1623.

Wang, S. (2007). Measures of Retaining Digital Evidence to Prosecute Computer-based Cyber-crimes, *Computer Standards and Interfaces*, 29, 216-223.

Williams, M. (2006). *Virtually Criminal*. New York: Routledge.
Wired Society, *The Nation*. May 4, 2002.
Yam, J. T. (2001). Cyber crime Treaty Under Way. *Business Word,* May 3, 9.
ZDNet UK, US joins European cyber crime convention, Retrieved on 1st November 2010 from http:www.zdnet.co.uk/misc/print/0,1000000169,39283761-39001093c,00.htm
Zimring, F., & Hawkins, G. (1973). *Deterrence: The Legal Threat in Crime Control*. Chicago: University of Chicago Press.