CYBER CRIME CONVENTION AND TRANS BORDER CRIMINALITY

by

MRINALINI SINGH & SHIVAM SINGH

Computers: A Device for Perpetrating Crimes [1]

While computers themselves do not commit crimes; they along with the Internet have given birth to an altogether new generation of crimes where the role of the human hand is only to start the criminal activity while the automated machines carry on the major activities.[1] The Internet with its unique advantage of anonymity and speed is a double edged sword. While it promotes free expression, it also provides a haven for the commission of several kinds of cyber crimes. The majority of what are termed cyber crimes are crimes of the digital age and really violations of long standing criminal law, perpetrated through the use of computers or information networks. On the one hand, it is believed that the problems of crime using computers will rarely require the creation of new substantive criminal law; rather, they suggest need for better and effective enforcement of existing laws through international cooperation.[2] It is suggested that crimes in cyberspace should be regulated the same way as those in real space as computer is merely an instrument.[3] On the other hand, it is believed that marked differences exist between cyber crimes and conventional crime. Cyber crimes are grossly under-detected and under-reported. The laws in the area are complicated,

---

1 Fatima Talat. (2005). Cyber Crimes: Challenging the Paradigms of Traditional Criminal Law. *Corporate Law Cases (3)*, 475.

2 (2000). World Information Technology and Services Alliance (WITSA) Statement on the Council of Europe Draft Convention on Cyber Crime. Retrieved October 25, 2006, from http://www.witsa.org/papers/COEstmt.pdf.

3 Katyal Neil Kumar. (2001). Criminal Law in Cyberspace. *University of Pennsylvania Law Review (149)*, 1005.

and are evolving at a different rate from the underlying technology.[4] As a result, responding to attacks against computers and information systems, such as malicious hacking, dissemination of viruses, and denial of service attacks poses serious problems. This view therefore requires addressing the issue of cyber crimes by evolving specific legislations and conventions.

Transnational Character of Cyber Crimes and Existing Inadequacies [2]

In principle, computer crimes can be perpetrated from anywhere and against any user in the world. Therefore, effective investigation and prosecution of cyber crime often requires that criminal activity be traced through several national borders. A number of Internet service providers spread over different jurisdictions may be involved in the course of investigation.

However, the national level scene in various countries is conspicuous by the absence of a computer crime focus. Despite the efforts of international and supranational organizations, various national laws world-wide show remarkable differences. This dilemma is reflected in the case of hate speech. While such speech is banned in many countries, particularly in Europe, the same hate speech in many instances is in fact protected by the First Amendment to the U.S. Constitution. Thus, for the United States, law enforcement cooperation with other countries' investigations of hate speech cases can be problematic. [5]

Considerable differences also exist with respect to the coercive powers of investigative agencies (especially with respect to encrypted data and investigations in international networks), the range of jurisdiction in criminal matters, and with respect to the liability of intermediary service providers on the one hand and content providers on the other hand.[6]

Moreover, lack of internationally agreed standards for criminalizing such harmful conduct is the prime cause of such abysmal number of convictions

---

[4] Mitchell Steven D. & Banker Elizabeth A.. (1998). Private Intrusion Response. *Harvard Journal of Law and Technology, (11)*, 708. Retrieved October 21, 2006, from http://jolt.law.harvard.edu/articles/pdf/v11/11HarvJLTech699.pdf.

[5] Goldstone David & Shave Betty Ellen. (1999). International Dimensions of Crimes in Cyberspace. *Fordham International Law Journal, 22*, 1935.

of the perpetrators. The defiance and audacity with which the cyber criminals operate only highlights the inadequacies of the existing system that seeks to tackle the issues of cyber criminality. Only some attackers are nailed, that too after lengthy and exorbitantly priced investigations. A large portion of these attackers still go unpunished.

Further the system is often not equipped to bear the onslaught of the cyber criminals. While new methods of attack have been accurately predicted by experts and some large attacks have been detected in early stages, efforts to prevent or deter them have been largely unsuccessful, with increasingly damaging consequences. Information necessary to combat attacks has not been timely shared. Investigations have been slow and difficult to coordinate.[7] In February 2000 attacks on CNN, eBay, Yahoo!, Amazon.com, online investment firms and others were launched by cyber criminals. These servers could almost not sell their products any more for the next few days. They claimed to have globally endured more than $1 billion in damages. Despite being able to anticipate attacks of this type on the basis of observations of public hacker exchanges that shared attack strategies and software to implement those strategies, law enforcement personnel were unable to prevent them, and security personnel employed by the targeted cyber systems were unable to defend against them. These troubling failures stem from serious weaknesses in the capacities of states to protect valuable cyber systems from attacks that pose a rapidly escalating danger.[8]

Further, very often, the attackers exploit the transnational character of the information infrastructure by avoiding prosecution or complicating investigations by initiating attack packets from countries with inadequate laws, and routing them through countries with different laws and practices, and no structures for cooperation.[9] Often the attacks are from nations lacking adequate laws governing criminalization of harmful conduct. Therefore,

---

[6] (2001). Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime", Communication from the Commission of the European Communities to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions. Retrieved November 3, 2006, from http://www.europa.eu.int/information_society

[7] Sofaer Abraham D. et al. (2000). A Proposal for an International Convention on Cyber Crime and Terrorism. Retrieved November 5, 2006, from http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm

[8] Ibid.

[9] Ibid.

when one country's laws criminalize certain activities on computers and another country's laws do not, cooperation in solving a crime and prosecuting the perpetrator may become difficult. Thus, when a criminal weaves his communications through three, four, or five countries before reaching his intended victims, inadequate laws in just one of those countries can, in effect, shield that criminal from law enforcement around the world.[10] Therefore, within the framework of international cooperation, the imperfections and inadequacies of national legislations are obviously a big obstacle in combating transnational computer crime. Clearly criminal sanctions on national and international level do not ensure good protection from computer crime, because of absence of precise clarification of computer crime in the national laws or because subsequently, the difficulty of interpretation and application of these laws restricts the law enforcement activity.[11]

Dual criminality is another issue of concern. This concept implies that extradition will not be permitted unless an act constitutes a crime under the laws of both the state requesting extradition and the state from which extradition is requested. This can often serve as a loophole in the system when the perpetrator's country does not have specific legislations concerning cyber crime, but the victim's country does. In such situations, application of a nation's domestic laws fails.[12]

The intangible nature of evidence is yet another challenge during cyber investigation and one which is capable of exploitation at the hands of cyber criminals. Paper, which is the most reliable medium of evidence, has almost no role to play in cyber investigation. Intangible and transient nature of data and the technical nature of evidence and investigation give the defense claims of error thereby making the case of the prosecution weak.[13] Investigation proceedings can suffer a setback due to the ability to destroy or alter data quickly, thus creating difficulties in obtaining valuable evidence.[14]

---

[10] DiGregory Kevin. (2000). Fighting Cybercrime - What are the Challenges facing Europe? Meeting Before the European Parliament. Retrieved November 7, 2006 from http://www.usdoj.gov/criminal/cybercrime/intl.html#Vd4

[11] Golubev Vladimir. (2005). International Cooperation in Fighting Cyber Crime. Retrieved October 1, 2006 from, http://www.crime-research.org/articles/Golubev0405/.

[12] Steele Howard L, (1997). The Web That Binds Us All: The Future Legal Environment of the Internet. *Houston Journal of International Law, (19)*, 501.

[13] *Supra* note 1, 478.

[14] Hoppkins Shannon L. (2003). Cyber Crime Convention: A Positive Beginning to a Long Road Ahead. *Journal of High Technology Law, (2)*, 102.

Further, conducting of the investigation measures related to search, seizure and arresting the computer machinery has certain peculiarities. First, the presence of specially trained and skilled personnel able to duly conduct these actions is required. Second, upon the arrest of information, the possibility of its modification and termination should be looked to and subsequently excluded. These actions should be conducted within minimum period of time, taking into account the speed of receiving the information. Third, careful analysis of the records about connections to Internet of the computer system should be made prior to arrest of this system. This is necessary for full procedure of conducting the measures on arrest and seizure of evidences.[15]

Finally, it has been suggested that even the development of international law in the area is currently ineffective.[16] "*To be held responsible under principles of international law, that person must commit a defined offense under customary international principles, as established by international treaties or norms.*"[17] Due to the relative novelty of computer crimes on the Internet, no such international norms presently exist.

Cyber Crimes and International Cooperation [3]

The Internet is not a single entity; no government, company, or individual owns it. As a result, "*nations' borders are just speed bumps on the information superhighwa*y".[18]

Therefore, the transnational character of cyber crimes makes jurisdictional issues an important area of concern. The players are multiple states and it is imperative that agreements on jurisdiction and enforcement need to be strongly enforced as the law enforcement agency of one state may require the mutual assistance of another state for the purposes of extraditing a criminal to its own territory in order to enable effective prosecution. Therefore, international cooperation is imperative for any fight against cyber crime to be effective.

---

[15] *Supra* note 11.

[16] Coffield Grant E. (2001). Love Hurts: How to Stop the Next 'Love Bug' From Taking a Bite Out of Commerce. *Journal of Law and Commerce, (20)*, 254.

[17] *Supra* note 12, 495.

[18] Selin Sean. (1997). Governing Cyberspace: The Need for an International Solution. *Gonz. Law Rev*iew, *(32)*,376.

One form of this said international cooperation is by having investigators and prosecutors with expertise in the field to be available 24 hours a day so that appropriate steps can be taken in a fast breaking high tech case. This is largely because of the unique feature of computer crime which requires immediate action to locate and identify criminals. The trail of a criminal may be impossible to trace once a communication link is terminated, because the carrier may not keep (or is not required by law to keep) records concerning each individual communication. When a carrier does not collect traffic data, a suspect's trail may evaporate as soon as communication terminates.[19]

While the criminals will recognize no boundaries on the Internet, the law enforcement agencies must respect the sovereignty of other nations. Therefore, once again, dependence on foreign law enforcement agencies and inter- State cooperation for the purposes of fighting cyber crime assumes vital significance as it is difficult for investigations to be carried on in a foreign country without obtaining sanction from the country's authorities.

The involvement of law enforcement officials is much desired in order to prevent the commission of cyber crimes. Interpol, which is a long-established, solid institution promoting cooperation between police force plays an important role here.[20] It has a network of national central bureaus in its member States which render timely assistance to it whenever a request for international cooperation is forwarded. Its I-24/7 network, as the name suggests functions 24 hours a day; it builds up a strong network of law enforcement and communications carriers who can work together on investigations, and improving the legal agreements by which cooperation can be extended in time-sensitive situations. Due to the technical nature of computer crime, several countries had set up special law enforcement units responsible for taking urgent action at the national level when information about computer related crime is circulated internationally. This is an early warning system and is useful as information exchanged through Interpol channels reaches these special units with the least possible delay.

Steps towards combating cyber crime have also been undertaken by the G-8, or group of eight, formed in 1975. The G-8 in 1997 adopted an Action Plan to combat high tech crime. It delineated four areas where action by the

[19] Lim Yee Fen. (2002). *Cyberspace Law*. Melbourne: OUP, 264.

[20] Retrieved October 8, 2006, from http://www.interpol.int

international community was essential to tackle cyber criminals. The areas require, first, enactment of sufficient laws to appropriately criminalize computer and telecommunications abuses; second, commitment of personnel and resources to combating high-tech and computer-related crime; third, improvement in global abilities to locate and identify those who abuse information technologies; and fourth, development of an improved regime for collecting and sharing evidence of these crimes, so that those responsible can be brought to justice.[21]

Need for a Convention [4]

Therefore, given the evolving information age and the challenges faced in combating cyber crime, there is a pressing need to regulate the Internet, (especially in the criminal realm), which otherwise thrives in an environment where there is free exchange of information.

Several arguments have been advanced to achieve this said regulation by way of a multilateral convention. Not only do cyber criminals exploit weaknesses in the laws and enforcement practices of States, exposing all other States to dangers that are beyond their capacity to respond, but the speed and technical complexity of cyber activities requires prearranged, agreed procedures for cooperation in investigating and responding to threats and attacks. Therefore, a multilateral convention will ensure that all States will adopt laws making dangerous cyber activities criminal, enforce those laws or extradite criminals for prosecution by other States, cooperate in investigating criminal activities and in providing usable evidence for prosecutions and participate in formulating and agreeing to adopt and implement standards and practices that enhance safety and security.[22]

The Internet also creates new issues stemming from the potential for criminal misuse and because cyber crimes increasingly have an international element, national measures need to be supplemented by international cooperation based on global measures, coordinated

[21] Sussmann Michael A. (1999). The Critical Challenges From International High-Tech and Computer-Related Crime at the Millennium. *Duke Journal of Comparative and International Law (9)*, 458.

[22] *Supra* note 7.

international work and binding minimum standards.[23] For any convention to be successful in achieving its desired goal and to have the largest number of nations ratify it, only the offenses that have generally been prohibited by a consensus of nations should be included. The Select Committee of Experts on Computer-Related Crime of the Council of Europe deliberated upon this issue. It created a minimum list of certain computer-related abuses that should be dealt with via criminal law legislation. This list represented a consensus for the major computerized nations of the world.[24]

The role of a convention also assumes importance as the objective is to have an instrument which applies world-wide so that "digital havens" or "Internet havens" can be denied to anyone wanting to engage in shady activities and hoping to find all the facilities they need, including financial ones, for laundering the product of their crimes. It must not be forgotten that the Internet is a global system and that no country can isolate itself from the rules under which it has to operate.[25]

It has been suggested that first, at a minimum, a model code for substantive computer offenses should be brought about so that uniformity in cyber crime laws is achieved. Further, apart from creating a unified body of cyber law, this offers advantages to those countries with archaic laws, who can now get assistance in updating them. As a result of this subsequent uniformity of offenses, the requirement of dual criminality in extradition and mutual assistance treaties would also be met.[26]

Finally, any Convention on Cyber Crime must also deal with the exercise of jurisdiction over an alleged cyber criminal by a nation. In cyber crime, unlike most other crime, the criminal can commit the offense in multiple nations simultaneously. Therefore, obtaining jurisdiction over criminals outside of the nation is an issue that merits examination.

The Eighth United Nations Congress has recommended that agreements on jurisdiction over computer criminals should address the issue of

[23] Goueff Stefan Le. The Draft Cyber Crime Convention: Creating an International Law Enforcement Standard. Retrieved October 15, 2006 from http://www.vocats.com/vocats/LeGoueff.nsf/0/884C04CE4BF47EFBC1256B1100528446/$File/The_Draft_Cyber_Crime_Convention.htm?Open

[24] *Supra* note 12, 507.

[25] Chevenement Jean Pierre. (2000). G-8 Conference on Cyber Crime. Retrieved November 7, 2006 from http://www.ambafrance-us.org/news/statmnts/2000/cyber2.asp

[26] *Supra* note 12, 507.

cooperation in the investigation, prosecution and punishment of international computer offences, including the admissibility of evidence lawfully gathered in the other countries, and the recognition of punishment effectively served in other jurisdictions.[27]

There are several traditional extraterritoriality principles to exercise jurisdiction when the criminal has not committed a crime within its boundaries. Nations have used the active nationality principle, the passive personality principle, the protective principle, and the universality principle. However, the varied rationale of these theories often results in concurrent jurisdiction and the possibility of double jeopardy. Consequently, a single, unified jurisdictional framework governing the nations of the world is needed to overcome the limitations of jurisdiction.[28]

Council of Europe's Convention on Cyber Crime [4.1]

One of the most serious steps taken to regulate this problem was the adoption of the Convention on Cyber Crime by European Council on 23 November 2001, the first international agreement on juridical and procedural aspects of investigating and prosecuting cyber crimes.[29] It specifies efforts coordinated at the national and international level and aims at preventing illegal intervention into the work of computer systems. The Convention stipulates actions targeted at national and inter-governmental level, directed to prevent unlawful infringement of computer system functions.[30] Four kinds of cyber crimes are dealt with in the Convention:

---

[27] (1994). U.N. Manual on the Prevention and Control of Computer-Related Crime. 4 U.N. Doc. ST/ESA/SER.M/43-44, U.N. Sales No. E.94.IV.5

[28] *Supra* note 12, 507.

[29] In particular, the following European Recommendations have influenced widely the Council of Europe Convention on Cyber-crime;

1. Recommendation N° R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications,

2. Recommendation N° R (88) 2 on piracy in the field of copyright and neighboring rights, the Recommendation N° R (87) 15 regulating the use of personal data in the police sector,

3. The Recommendation N° R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services,

4. Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and

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

[30] *Supra* note 11.

hacking of computer systems, fraud, forbidden content (racist websites and child porn content) and breaking copyright laws. The Convention also defines the offences which all States would have to recognize. It also proposes extradition procedures. The countries involved include some major countries outside the Council of Europe and that, once signed, this Convention is open for signature by all States wishing to accede to it.

Mutual Legal Assistance [5]

MLATs and Letters Rogatory [5.1]

International cooperation in cyber crime investigation in the form of mutual legal assistance requires an international agreement or other similar arrangement such as reciprocal legislation. Such provisions, whether multilateral or bilateral, oblige the authorities of a contracting party to respond to a request for mutual legal assistance in the agreed cases. Such assistance generally refers to specific coercive powers concerning the investigation of cyber crime. Apart from requests for traditional help, such as interviewing witnesses, the purpose is to obtain certain data stored in a computer system that is located in the territory of another state or being transferred electronically through a network and capable of being monitored or intercepted in the territory of that state.

Existing legal instruments available for obtaining cooperation between States include Mutual Legal Assistance in Criminal Matters Treaties (MLATs) and letters rogatory. MLATs permit a victim's government to go into the criminal's country and seek assistance in gathering information.[31] Further, very often, MLATs can only be used to coordinate an investigation and prosecution if the requirements of dual criminality are satisfied.[32] The case of Onel de Guzman, is one of the commonly cited examples, where Guzman, the author of the Love Bug virus could not be prosecuted despite effective international cooperation between the law enforcement agencies of Philippines and other affected countries. The concept of dual criminality came to his rescue, where authoring and unleashing a computer virus was at the concerned time not an offense in Philippines! MLATs also fail with

[31] *Supra* note 12, 501.
[32] *Supra* note 16, 253, 254.

respect to the speedy and urgent preservation of evidence which is synonymous with cyber crime investigation.[33] Investigators need to be able to contact their counterparts in other countries immediately in order to ensure that the necessary evidence should not be lost. This speedy coordination cannot be guaranteed by the MLATs which are fraught with procedural and bureaucratic delays. In addition, MLATs can often restrict the scope of offenses under investigation.[34] Finally, the bilateral nature of MLATs severely hinders their usefulness. Cyber attacks are often routed through several states and hence the number of bilateral treaties required to achieve near- universal coverage is untenable.[35] It is however the worst when many nations do not have MLATs or extradition treaties.[36]

Letters rogatory, which are a customary method of obtaining assistance from abroad in the absence of a treaty or an executive agreement are once again inappropriate because they are extremely time consuming.[37]

24/7 Network [5.2]

Even the Convention on Cyber Crime stresses greatly on provisions dealing with mutual legal assistance. Article 35 deals with ways to speed up international cooperation, taking up the concept of national contact points. Since cyber crimes transcend national and international borders, cooperation of different legal systems is essential in successful investigation and prosecution. The transient nature of evidence makes it imperative for investigators to call upon their counterparts in other States for the preservation of the same. Article 35 outlines the concept of the 24/ 7 network which is an important tool in dealing with the issue of cyber crimes.

Effective combating of cyber crimes and effective collection of evidence in electronic form requires rapid and immediate response. Across multiple countries, cyber crime operations can be set up, then reconfigured in milliseconds. Therefore, existing *police* cooperation and modes of mutual assistance require supplementary channels to address the challenges of the

---

[33] Ozment Andy. (2003). The Need for a Near Universal, Multilateral, International Legal Regime to Combat Cyber Crime. *WG Paper 5, 2nd U.K Student Pugwash Conference*, 2.

[34] *Supra* note 12, 501.

[35] *Supra* note 33, 2.

[36] *Supra* note 16, 254.

[37] *Supra* note 33, 2.

computer age effectively. The establishment of the 24/7 network is one of the most important means provided by the Convention of ensuring that nation states can effectively deal with the law enforcement challenges posed by computer crime.[38]

The Convention mandates that, each party designate a point of contact available, 24 hours a day, 7 days a week, in order to render timely assistance and cooperation in cyber crime investigations. States have the freedom to determine the location of their point of contact, whether with a central authority or with a specialized police unit. Each national 24/7 point of contact is responsible for taking urgent action at the national level upon information about cyber crimes being circulated internationally. This may involve either facilitating or directly carry out, inter alia, the providing of technical advice, preservation of data, collection of evidence, giving of legal information, and locating of suspects. If a party's 24/7 contact is part of a police unit, it must have the ability to coordinate with other relevant components within its government expeditiously, such as the central authority for international extradition or mutual legal assistance, in order that timely action may be undertaken. Moreover, 24/7 contacts must have the capacity to carry out fast communications with the other members of the network and must have proper equipment and trained personnel.[39]

The Convention makes it clear that international cooperation is to be provided among contracting states to the 'widest extent possible.'[40] Therefore, concerted international cooperation is a must for combating cyber crimes internationally. The commission of crimes in a global environment mandates assistance from other states during investigation. This includes both informal cooperation by law enforcement personnel and formal mutual legal assistance conducted through national authorities.

Concluding Remarks [6]

"*Giving birth to new technologies is the work of inventors and making use of those technologies for more advanced and drastic crimes is the craftwork of*

[38] In Conversation with Bernhard Otupal, Officer, Financial and High Tech Crime Unit, Interpol.

[39] Article 35, Convention on Cyber Crime.

[40] Article 24, Convention on Cyber Crime.

criminals."[41]

One of the more significant aspects of computer related crime is its global reach. While international offenses are not a unique phenomenon, the global nature of cyber space significantly enhances the ability of offenders to commit crimes in one state which will affect individuals in a variety of other countries. This poses great challenges for the detection, investigation and prosecution of offenders.

Therefore, cyber crime investigation is characterized by several challenges. The most daunting task that confronts law enforcement officials today is the transnational character of cyber crimes whereby geographical limits and international boundaries have become obliterated. Most Internet activities involve the simultaneous interactions of many connected computers dispersed all over the world. It is not possible for any one country to deal with these international developments. Close continuing cooperation is essential to discover the activity, gather evidence, and prosecute the perpetrators.

Therefore, it is imperative that there needs to be a substantial consensus with respect to what cyber activities should be considered criminal. Substantial benefits can only be derived from a multilateral arrangement where there are common standards for recognition of offenses and for investigation and cooperation. Here, we stand on opinion that there is a lacuna in the present Convention on Cyber Crime as there still remains a lack of clarity in the present definition of offenses. Certain key definitions essential to interpreting the Convention's provisions are overly broad.[42] However, the Convention cannot be categorized as a failure either. The transient nature of data and the absence of geographical boundaries make computer crimes inherently hard to detect. But the Convention does harmonize substantive criminal laws and procedures related to cyber crimes by setting up an international cooperation system among national

[41] Varma S.K & Mittal Raman. (2004). *Legal Dimensions of Cyberspace*. New Delhi: Indian Law Institute, 265.

[42] *Supra* note 14, 105. For instance, the Convention defines a computer as "any device or a group of interconnected or related devices one or more of which, pursuant to a program, performs automatic processing of data." This is problematic because it does not define or limit what constitutes a device, thus, potentially including devices such as children's toys, Palm Pilots or cable TV boxes. Moreover, it is difficult to tell whether the definition of computer data includes items such as bar codes used to scan groceries at the supermarket.

law enforcement agencies to fight the cyber criminals more efficiently and in real time. With its strong emphasis on developing a 24/7 network, there is definitely a commendable attempt at ensuring rapid and smooth overflow and exchange of information and assistance. This is particularly useful in tackling the otherwise complex issues of jurisdiction and bureaucratic hurdles posed by way of MLATs and letters rogatory.

Thus, the Convention is certainly a positive beginning to a long road ahead. The final destination should however harmonizing not just the crimes but also the investigative and prosecutorial procedures that will enable prevention as also conviction of cyber crimes and criminals.[43]

[43] *Ibid*, 108.