International computer crimes

General report

érès | *Revue internationale de droit pénal*

2001/3 - Vol. 72

pages 813 à 829

ISSN 0223-5404

Article disponible en ligne à l'adresse:

http://www.cairn.info/revue-internationale-de-droit-penal-2001-3-page-813.htm

Pour citer cet article :

"International computer crimes" General report, *Revue internationale de droit pénal*, 2001/3 Vol. 72, p. 813-829.

Distribution électronique Cairn.info pour érès.

© érès. Tous droits réservés pour tous pays.

La reproduction ou représentation de cet article, notamment par photocopie, n'est autorisée que dans les limites des conditions générales d'utilisation du site ou, le cas échéant, des conditions générales de la licence souscrite par votre établissement. Toute autre reproduction ou représentation, en tout ou partie, sous quelque forme et de quelque manière que ce soit, est interdite sauf accord préalable et écrit de l'éditeur, en dehors des cas prévus par la législation en vigueur en France. Il est précisé que son stockage dans une base de données est également interdit.

SECTION II

INTERNATIONAL COMPUTER CRIMES

Matthew R. ZAKARAS,[*]

General Report

Introduction

Individuals and organizations with access to network technology are able to share information with each other from anywhere on the planet. These electronic exchanges have energized businesses and facilitated communication exponentially; however, they have also made this same information susceptible to a myriad of criminal activity. The activity that has arisen because of the developments in the use of network technology is novel both in its breadth and scope. A rash of criminal activity has occurred which has caused billions of dollars of damage to governments and private industry. In addition, network technology has spawned new types of criminals, who do not see tampering with computer systems as a nefarious act because of the spatial and emotional distance to its victims.

Miscreants using computers will not limit their crimes to the regions of the world which have thus far enjoyed the fruits of network technology. Criminals will also victimize individuals and organizations of developing societies and emerging democracies. These societies are particularly vulnerable because their institutions are in their infancy, thus offering criminals a greater opportunity to victimize individuals and organizations. In addition, these governments, organizations, and individuals in developing societies do not have the resources and technology to protect themselves

Since the nature of network technology creates opportunities for criminals to remotely victimize anyone on the planet, a response to computer crime needs to be international in nature. Accordingly, this Article describes the nature of

[*] B.A., 1998, Marquette University; J.D., 2001, DePaul University College of Law. Mr. Zakaras is an associate at the law firm of Levenfeld Pearlstein, Chicago, Illinois. The author would like to thank Professor M. Cherif Bassiouni for his comments and encouragement while writing this Article.

computer crimes and addresses issues and problems which will effect the international community. Part I is the Background. It describes how network technology has created a new type of criminal and criminal enterprise that uses unique techniques to victimize individuals and organizations. It also describes how these crimes are detected by investigators. Part II addresses international efforts to deal with computer crimes, including initiatives by the G-8, the Council of Europe and individual states. Part III addresses substantive, procedural and other issues that need to be examined by the international legal community. Part IV is the conclusion.

I. Background

A. A New Type of Criminal

The term "hacker" is a generic term to describe people who are adept at manipulating and attacking computers and networks.[1] When most people think of this term, images of kids staying up late into the night using their computer skills to bring down wealthy corporations often come to mind.[2] However, these miscreants are often more sophisticated and dangerous. The U.S. Federal Bureau of Investigation and the Computer Security Institute, in a survey of Fortune 500 companies, found that financial losses from computer crimes exceeded $360 million from 1997 to 1999.[3] Of those responding to the survey, 62% reported computer security breaches within the last year.[4]

The nature of a computer crime, and its effects on the international legal system can be seen by the May 2000 computer virus bearing the name "I Love You" which spread through businesses in Asia, the United States, and the rest of the world.[5] It affected thousands of corporate sites in the United States and the rest of the world, forcing many of them to shut down their email systems.[6] Systems that were affected included the Department of Defense, the Federal

[1] See DOROTHY DENNING,. INFORMATION WARFARE AND SECURITY (Addison-Wesley 1998); JEFF GOODELL, THE CYBER THIEF AND THE SAMURAI (Dell Publishing 1996); JONATHAN LITTMAN, THE FUGITIVE GAME: ONLINE WITH KEVIN MITNICK, (Little Brown & Company 1995); DONN B. PARKER, FIGHTING COMPUTER CRIME: A NEW FRAMEWORK FOR PROTECTING INFORMATION (John Wiley & Sons, Inc. 1998).

[2] P. TAYLOR, THE HAWKS AND THE DOVES—ENEMIES AND FRIENDS (Routledge 1999); DONN B. PARKER, FIGHTING COMPUTER CRIME: A NEW FRAMEWORK FOR PROTECTING INFORMATION (John Wiley & Sons, Inc. 1998); WINN SCHWARTAU, INFORMATION WARFARE (Thunder Mouth Press 1994).

[3] Speech by U.S. Attorney General Janet Reno to the National Association of Attorneys General, Jan. 10, 2000. http://www.usdoj.gov/ag/speeches/2000/011000naagfinalspeech.htm

[4] Id.

[5] Paul Festa and Joe Wilcox, EXPERTS ESTIMATE DAMAGES IN THE BILLIONS FOR BUG, CNET News.com May 5, 2000, 12:55 p.m. PT

[6] Id.

Reserve, Britain's parliament, Ford, Lucent and Daimler Chrysler.[7] Although businesses had been struck by computer viruses in the past (i.e., Melissa and SATAN), the "I Love You" virus was particularly damaging and infectious. The rogue program spread quickly because of its ability to send copies of itself to email addresses contained on victimized computers. It then used a program placed on its server to steal passwords stored in computers.[8] In this process, the virus destroyed data on infected computers. Experts have estimated that the cost to governments and businesses was upwards of $10 billion.[9]

Within days of it being sent out, the National Bureau of Investigation, with assistance of a local Internet provider and caller ID, was able to trace the origin of the virus to an apartment in a Manila neighborhood where a young college drop-out named Onel A. de Guzman acknowledged that he may have accidentally unleashed the virus. [10] Even though there was talk of bringing charges against de Guzman in the United States,[11] he was charged in the Philippines under a law dealing with illegal use of passwords for credit card and bank transactions.[12] On August 21, 2000, all charges were dropped against de Guzmun because his actions did not fall under the purview of his charged-crimes.[13]

The psychological profile of a hacker includes the following traits: not career orientated; show an aptitude with computers and other electronic equipment; families are usually dysfunctional, characterized by single-parent households.[14] According to Tim Jordan and Paul Taylor in *Sociology of Hackers*, hackers are motivated by six common threads. First, hackers have an addiction to computers and computer networks. Second, they are curious as to what can be found on the world wide web. Third, hackers often claim that their life offline is boring compared to their online exploits. Fourth, they are attracted to getting into

[7] Id.

[8] SP TRACKS "LOVE" BUG THROUGH CALLER ID, The Associated Press, Special to CNET News.com, May 15, 2000, 8:45 a.m. PT

[9] Paul Festa and Joe Wilcox, EXPERTS ESTIMATE DAMAGES IN THE BILLIONS FOR BUG, CNET News.com May 5, 2000, 12:55 p.m. PT

[10] SP TRACKS "LOVE" BUG THROUGH CALLER ID, The Associated Press, Special to CNET News.com, May 15, 2000, 8:45 a.m. PT

[11] SETH MYDIANS, OFFICIALS TRACE COMPUTER VIRUS IN PHILIPPINES, NEW YORK TIMES (May 9, 2000, Section A, Page 1, Column 2, Business/Financial Desk); see also ATTORNEY JANET RENO'S WEEKLY MEDIA AVAILABILITY WITH MICHAEL VATIS, NATIONAL INFRASTRUCTURE PROTECTION CENTER TO DISCUSS NEW E-MAIL VIRUS, JUSTICE DEPARTMENT, WASHINGTON, D.C. (May 19, 2000, 9:33 A.M. EDT Friday) ("Q: Is there any thought, either Ms. Reno or Mike [Vatis],…[t]o filing U.S. charges against any suspects in the Philippines…. [A]TTY GEN. RENO: I think that while the investigation is pending, we really shouldn't comment.").

[12] PHILIPPINES DROPS CHARGES IN 'ILOVEYOU' VIRUS CASE, August 21, 2000, Web posted at: 11:40 AM EDT (1540 GMT) MANILA, Philippines (Reuters)

[13] Id.

[14] JEFF GOODELL, THE CYBER THIEF AND THE SAMURAI (Dell Publishing 1996).

computer systems because these areas are restricted. Fifth, recognition from peers who are also online is a goal and reward for many hackers. Finally, hackers see their activities as a service to future computer users because of the loopholes that they find in computer networks.[15] Most hackers do not intend to hurt people, but rather compare themselves to Robin Hood who stole money from the elite part of society and gave it to those who are less fortunate.[16] Similarly, the motivation of hackers is to make programs and information available to others for free.[17]

Network technology has created an environment where citizens who would not ordinarily be involved in criminal enterprises, get involved because they do not have a spatial or emotional connection to their victims. Computer hackers whose only objective is intellectual curiosity are hired by criminal enterprises who have profit-making intentions. These computer hackers may have other legitimate jobs and break into computers only for fun. When the skills of these hackers are combined with the profit-making, and often violent, activities of organized criminal enterprises, the effects can be damaging.

Techniques of Hacking

In order to understand how states should deal with crimes related to the activity of hacking, the techniques and methods used by hackers must be explored. Examining these techniques and methods illustrates the magnitude of the problem that hacking presents and the activity's diverse, unique, and adaptive nature. Hacking has been divided into eight general categories:[18] (1) Eavesdropping: Using Packet Sniffers to Observe Patterns of Traffic; (2) Snooping: Downloading Data; (3) Tampering or Data Diddling; (4) Spoofing; (5) Jamming and Flooding; (6) Injecting Malicious Code; (7) Exploiting Flaws in Design, Implementation or Operation; and (8) Cracking Passwords, Codes, and Keys. These categories are not mutually exclusive and hackers often use more than one technique in a given attack.

[15] TIM JORDAN AND PAUL TAYLOR, SOCIOLOGY OF HACKERS, at http://www.comms.uab.es/inet99/inet98/2d/2d_1.htm

[16] Id.

[17] Id.

[18] See Dorothy E. Denning, Cyberspace Attacks and Countermeasures, in INTERNET BESIEGED: COUNTERING CYBERSPACE SCOFFLAWS 29, 32-41 (Dorothy E. Denning & Peter J. Denning eds., 1997).

Eavesdropping: Using Packet Sniffers to Observe Patterns of Traffic

One method of attacking computer networks is eavesdropping or the "passive interception of network traffic."[19] The eavesdropper observes patterns of traffic (i.e., sources and destinations) on a network using a "packet sniffer" in order to determine the relationships among organizations and individuals. In this process, the information is only observed, not changed. A "packet sniffer" is a program that monitors network packets flowing through a computer. These sniffers are placed in workstations on local area networks, in Internet gateways, on router machines, or any other place which directs and relays Internet traffic. Packet sniffers have been used to capture login IDs and passwords from users logging into remote sites. Typically, these passwords are transmitted in the clear and can be ascertained by a hacker without recourse to other methods.

Eavesdropping where the hacker uses packet sniffers to observe patterns of network traffic can be seen in a recent case which was the first federal hacking trial in the Southern District of New York.[20] In *United States v. Oquendo*, Jesus Oquendo, an employee of an Internet start-up company which shared office space and a network with one of its investors, altered the start-up commands of the investor company's network so that its password file was automatically sent to an e-mail account which he controlled.[21] Although the company for which he worked failed, he used his access to the investor company to install a network "sniffer" which intercepted and recorded network traffic on the investor company's network.[22] By means of this "sniffer," he was able to obtain the password to a third company which sold computer equipment at retail locations.[23] Using this password to gain access to this third company's accounts, he erased one of their databases, causing $60,000 in damage.[24]

Snooping: Downloading Data

In this method, the attacker browses through documents, e-mail messages, information stored on disks, etc. and downloads information from these sources to his computer without altering its content.[25] Snooping is performed for many

[19] DENNING, supra note 18, at 32-33.

[20] New York Computer Security Expert Convicted by Jury of Computer Hacking and Electronic Eavesdropping, PRESS RELEASE (U.S. Department of Justice, Southern District of New York), March 7, 2001, at 1 [hereinafter Eavesdropping] (United States v. Oquendo, (S.D. NY)).

[21] Eavesdropping, supra note 20, at 1.

[22] Eavesdropping, supra note 20, at 2.

[23] Id.

[24] Id.

[25] DENNING, supra note 18, at 33.

purposes including espionage, acquiring software or documents without paying, and finding exploitable weaknesses in a system.

The snooping technique can be seen in the 1996 attack by a German hacker on a Miami Internet Service Provider (ISP).[26] The hacker gained access to the ISP and downloaded credit card information of the service's subscribers.[27] Using the downloaded data, he threatened to distribute the data unless the victims provided him with $30,000. After an investigation by the U.S. Secret Service, an Indonesian-born computer student was arrested when he tried to pick up money from a post office in Germany.

Tampering or Data Diddling

Tampering and data diddling occurs when the attacker makes an unauthorized modification to data or software on a system.[28] The threat from these types of attack is especially serious if the attacker obtains root access, with the capability to issue any command and retrieve, alter, or delete any data on the system. If such access is obtained, the attacker can crash the system or damage it to the extent that a systems administrator may have to shut down the system temporarily in order to check for and restore corrupted files. In extreme cases, attackers have replaced systems utility or application software with a Trojan horse--a program which appears to perform an intended function, but instead executes hidden malicious code. One type of Trojan horse program is a modified login program which appears to operate normally, but which stores copies of login IDs and root passwords in a hidden file. The attacker can later access this hidden file to obtain the password and login into the network.

The tampering and data diddling technique can be seen in the 1994 theft ring headed by a hacker in St. Petersburg, Russia named Vladimir Levin.[29] He broke into the Citibank electronic money transfer system and manipulated data so that $10 million was transferred in forty transactions to accounts in Finland, Russia, Germany, the Netherlands, the United States, Israel, and Switzerland.[30] Eventually, all of the transfers, with the exception of $400,000, were recovered by Citibank. Vladimir Levin was arrested in London, England and successfully extradited to the United States where he was sentenced to prison for three years and ordered to pay restitution in the amount of $240,000.

[26] David Goldstone and Betty-Ellen Shave, International Dimensions of Crimes in Cyberspace, 22 FORDHAM INT'L L.J. 1924, 1929 (1999)(citing Matthew McAllester, Feds Aid Miami Company in Global Hunt for Hacker, Newsday, June 8, 1997, at A41).

[27] Id.

[28] DENNING, supra note 18, at 33.

[29] Goldstone and Shave, supra note 26, at 1927 (citing Dean Starkman, Russian Hacker Enters Fraud Plea in Citibank Case, Wall St. J., Jan. 26, 1998, at A6).

[30] Id.

Spoofing

Using this method, the attacker impersonates a legitimate user and deceives him into disclosing security information. Oftentimes, the attacker will use one system as a springboard to log into another, and then use that to login to another, and so on.[31] This process, called looping, allows the attacker to keep his identity and location concealed. This process may include several legs that cross national boundaries. In another form of spoofing, called e-mail forgery, the attacker generates messages with a false Internet address in the "From" field in order to obtain security information.[32]

In 1986, the spoofing technique was used by a German hacker to obtain sensitive information, such as munitions information, information on weapons systems, and technical data from computer networks throughout the United States.[33] In order to obtain this information, he gained access to the Lawrence Berkeley Laboratory, in Berkeley, California. He used his access to the computer at the Lawrence Berkeley Laboratory to fool other computer networks into allowing him access.

Jamming and Flooding

If an attacker is jamming or flooding a computer system, he is disabling or tying up the system's resources.[34] This kind of attack is often referred to as "denial-of-service." Jamming or flooding occurs when an attacker consumers all available memory or disk space on a machine or when he floods a network with so much traffic that no one else can use it. In the past, Internet Service Provides (ISPs) have had their systems temporarily disabled through a SYN attack, which exploits the Internet's TCP protocol where requests for information are processed. The attacker floods the target machines with SYN messages, but instead of providing the sender with return IP addresses, the messages contain fake return addresses. The target machine returns the messages, but receives no replies, thus filling its storage buffers and leaving no room for legitimate connections.[35]

The jamming and flooding technique can be seen in the 1996 attack by a Swedish hacker on the Northern Florida Emergency 911 system.[36] The hacker obtained the direct telephone numbers that corresponded to the lines used to

[31] DENNING, supra note 18, at 35.

[32] Id.

[33] Goldstone and Shave, supra note 26, at 1927-8 (citing CLIFF STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989)).

[34] DENNING, supra note 18, at 36.

[35] Id.

[36] Goldstone and Shave, supra note 26, at 1930(citing 911 Lines Tied Up by Hacker—In Sweden, Orlando Sentinel, Mar. 8, 1997, at D4).

receive 911 calls from eleven Florida counties. Using these direct telephone numbers, he made multiple calls to the 911 systems which tied up their lines.

Injecting Malicious Code

In this method, the attacker injects malicious code using an external device like e-mail or another network protocol.[37] The malicious code can be transmitted with any message or data that contains code, including source code, machine code, command scripts, or macros. This code is activated when the file or data stream is opened or executed. Malicious code takes the form of self-replicating code, e.g., "viruses" or "worms." A "virus" consists of fragments of code that attach themselves to a host that is executable. Examples of executable hosts are the boot sector of a hard or floppy disk, an *.EXE file containing an application program, or a macro.[38] A "worm" is like a virus, but they spread themselves only through networks and do not attach themselves to particular programs.

Exploiting Flaws in Design, Implementation or Operation

Attackers also exploit security holes in computer networks to gain access to systems, files, accounts, or root privileges, or to sabotage a system or its files.[39] System vulnerabilities occur for many reasons, including software bugs, lack of attention to security, and poor configuration. These vulnerabilities are generally characterized as flaws in design, implementation, or operation. They arise during the all stages of a products development, including installation and maintenance. Even when these security holes are patched, new flaws arise, sometimes even the fix or security module. Attackers use many tools to assist them in finding and exploiting vulnerabilities on a system, including Trojan horse utility programs, attack scripts, packaged tools which help an attacker acquire root access, and network scanners such as SATAN and the Internet Security Scanner (ISS).

This method of attack can be seen in the September 2000 attack of Western Union's web server.[40] According to a security specialist with underground connections, the crackers obtain access to the network when a hole was opened during routine site maintenance.[41] Once the crackers were in the system, they

[37] DENNING, supra note 18, at 37.

[38] Id.

[39] Id.

[40] Counterpane Internet Security, September 11, 2000 (Western Union Cracked) at http://www.counterpane.com/incidents.html.

[41] Id.

copied nearly 16,000 customer credit and debit card numbers.[42] The site remained off-line for five days while repairs were conducted.[43]

Cracking Passwords, Codes, and Keys

This method of attack involves the attacker guessing or finding by brute force a password or encryption key.[44] It may also involve discovering secret methods which can be used to encrypt or copy-protect data. Guessing a password is sometimes easy because users maintain the default password that has not changed since the product was shipped or choose passwords like their first name or social security number. Attackers have also used more systematic attacks with the aid of a dictionary and a password cracking program. Additionally, the Internet has made it possible to assemble massive computing resources to crack a key by brute force.

C. Detecting Computer Crime

The techniques in Section I(B), *supra*, allow criminals to hide their identify and commit crimes remotely from almost anywhere in the world. In order to investigate computer crimes, electronic evidence is used which is highly perishable and can be easily deleted or modified. For this reason, success in identifying criminals is contingent upon quickly following a trail of communication from the victimized computer to a computer where the criminal is located. This often involves tracing the communication through a number of computers that could all be in different countries. In addition, technologies need to be in place to effectively generate and store traffic data so investigators can effectively use it.

Sometimes, this tracing occurs in "real time," meaning that the investigation occurs at the same time the criminal is communicating or committing the crime.[45] This tracing is very complicated because the communication often traverses a number of computers.[46] In many computers, technologies are not designed to facilitate such tracing because the Internet only receives the address of the computer directly connected to it, not the address of the source of the communication. Even if the originating source was identified, the address may be incorrect or temporarily hijacked. Because of these limitations, investigations

[42] Id

[43] Counterpane Internet Security, September 15, 2000 (Western Union Up and Running) at http://www.counterpane.com/incidents.html.

[44] Id.

[45] Fighting Cybercrime--What are the Challenges facing Europe?, Remarks of Kevin DiGregory on Fighting Cybercrime before the European Parliament, September 19, 2000. http://www.cybercrime.gov/Euremarks.htm, taken 5/12/2001.

[46] Id.

often involve contacts with each communication provider in the chain to determine the original source of the criminal activity.

Tracing in "real time" is difficult because investigations often are not started until the damage is complete and even when a criminal is caught in the act, the investigators often do not have enough resources to trace the communication through multiple computers. This is the reason why most investigation depend on historical transactional records which are stored on both source and destination computers.[47] Examples of these historical transactional records include log files and electronic email records. In order for the after-the-fact investigation to be successful, the information in regard to the criminal event needs to be obtained quickly before critical information is allowed to be deleted.[48] This includes getting information from different computers throughout the chain of computers used in the incident, including service providers.

D. Network Technology Facilitates an Organic Form of Criminal Organization

Criminal enterprise is flexible and adaptive. Historically, the organization of criminal enterprises has been limited to confraternal groups with hierarchical structures, resembling a syndicate; ethnic- or nationality-based which act as a network based on ethnic affiliations; and gang-type groups which are brought together by their violent money-making operations.[49] A criminal enterprise takes on one of these organizational forms based on social context, beneficial opportunities, and the pressures of the criminal justice system.

The rise of computer crimes has made criminal enterprises more organic, taking on the characteristics of networks with decentralized leadership and decision-making under the penumbra of shared ideological, strategic, or operational goals. Small groups of hackers in different locations can now utilize networks to aggregate their otherwise exiguous resources in pursuit of criminal enterprises. According to a RAND report entitled *Countering the New Terrorism*, criminal enterprises taking on a network form come in three forms:

Chain Network. Commonly seen in a smuggling chain where people, goods, and information move along a line of separated contacts. In this type of network, communication must travel through each intermediate node.

Star or Hub Network. Franchises and cartels are examples of this type of network organization where the actors are tied to a central node and must go through that node to communicate and coordinate.

[47] Id.

[48] Id.

[49] M. Cherif Bassiouni and Eduardo Vetere, Organized Crime and its Transactional Manifestations, in INTERNATIONAL CRIMINAL LAW, Second Ed. Vol. I. Crimes, Edited By M. Cherif Bassiouni (Transactional Publishers, Inc. New York 1999), 883, 885.

All-Channel Network. Collaborative network of small groups or nodes where every group is connected to each other.[50]

These three types of networks can be combined to form hybrids. For example, a criminal enterprise may have an all-channel network at its core, but use a star or chain form to conduct its operations. In addition, the more traditional forms of criminal enterprise, like confraternal or gang-like groups, may be at any one of these nodes.

All three forms of network enterprises are highly decentralized. In the past, decentralized organizations have been difficult to form because communication is difficult to maintain between diverse groups. However, the rise of network technology has facilitated the increase in communication between diverse criminal groups. The capacity of these enterprises to operate effectively will ultimately depend on shared principles, interests, or goals between the nodes. This collaboration can occur between individuals and enterprises from very different locations, cultures, and walks-of-life.

Networking among hackers can be seen in the case United States v. Torricelli where Raymond Torricelli, a/k/a "rolex" was arrested in New Rochelle, New York, for, inter alia, breaking into the National Aeuronautics and Space Administration's Jet Propulsion Laboratory and other computers and using those computers to host an Internet chat-room devoted to hacking.[51] According to the Complaint, Torricelli used the chat-room to enter into discussions with other members of a group which called itself "#conflict."[52] Among the things that the group talked about were (1) breaking into computers; (2) obtaining credit card numbers and making unauthorized purchases; and (3) using their computers electronically to alter the results of the annual MTV movie awards.[53]

II. Responses to International Computer Crime

The international community and countries within the community have seen the need to create legislation and policies to address the problem of crime using network technology.

A. G-8's Response

In 1997 and early 1998, the G-8 Justice and Interior Ministers adopted and endorsed 10 Principles and a 10-point Action Plan to fight cyber crime. This was

[50] John Arquilla, David Ronfeldt & Michele Zanini, Network, Netwar, and Information-Age Terrorism, Chapter 3, in RAND, Countering the New Terrorism 39, 47-52 (2000).

[51] Hacker Group Leader Arrested for Breaking into NASA Computers, NEWS RELEASE (U.S. Department of Justice, Southern District of New York), July 12, 2000, at 1 [hereinafter Hacker Group] (United States v. Torricelli (S.D. NY)).

[52] Hacker Group, see supra note 51, at 2.

[53] Id.

the first time that a group of Presidents and Prime Ministers agreed upon principles that should be used to fight computer crime. The G-8 is made up of the United States, the United Kingdom, Germany, Japan, Italy, Canada, France, and Russia In addition, the G-8 has set up a 24/7 Point-of-Contact network, which requires participating countries to establish a 24-hour, seven days a week, service to assist in the investigation of computer crime cases.

The G-8 agreed to endorse the following principles to combat high-tech crime:

I. There must be no safe havens for those who abuse information technologies.

II. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.

III. Law enforcement personnel must be trained and equipped to address high-tech crimes.

IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.

V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.

VII. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.

VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.

IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.

X. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.

In addition, each participating country agreed to direct its officials to do the following:

1. Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.
2. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.
3. Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.
4. Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.
5. 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.
6. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.
7. Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence.
8. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax, or e-mail, with written confirmation to follow where required.
9. Encourage internationally-recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.
10. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.

B. Council of Europe

The Council of Europe (hereinafter "COE") and the United States[54] are working toward a final draft of a treaty which has been in the drafting stage for

[54] PRESS RELEASE ON THE COUNCIL OF EUROPE DRAFT CONVENTION ON CYBERCRIME (April 27, 2000) ("The 41-nation Council of Europe has previously produced two recommendations on the

nearly three years.[55] The purpose of the treaty is "[t]o harmonize national legislation in this field, facilitate investigations and allow efficient levels of co-operation between the authorities of different States."[56] The draft calls on signatories to pass legislation to criminalize computer hacking, hacking devices, illegal interception of data and interference with computer systems, computer related fraud and forgery, on-line child pornography, and the reproduction and redistribution of copyrightable material.[57] The draft also deals with law enforcement issues and international co-operation.[58]

C. Domestic Responses

Many states have developed laws to proscribe computer crimes. Accordingly, the crime of unauthorized access to computer systems has emerged in many states as the threshold offense. Unauthorized access is a good starting point because most crime in regard to hacking involve some sort of entry into a computer system without the permission of the network's owner. States that have enacted such legislation include Australia, Austria, Belgium, Brazil, Canada, Peoples Republic of China, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Iceland, Israel, Italy, Japan, Luxembourg, The Netherlands, New Zealand, Norway, Poland, Portugal, Singapore, Sweden, Switzerland, Turkey, United Kingdom, and the United States.[59] Although many countries have developed legislation to proscribe unauthorized access to computer systems, many countries have not developed such legislation. Since computer crime can be committed remotely from almost any jurisdiction in the world, it is crucial that every jurisdiction enact such legislation.

III. Legal Issues in International Computer Crimes[60]

A. Substantive Laws

Substantive law refers to that part of law which creates, defines, and regulates rights and duties of parties.

question, in 1989 and in 1995….[G]iven the importance of the subject, non-member States, such as Canada, Japan, South-Africa and the United States, also actively participated in the negotiations.").

[55] EUROPEAN COMMITTEE ON CRIME PROBLEMS (CDPC), COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE (PC-CY), DRAFT CONVENTION ON CYBER-CRIME, (Draft # 22, December 22, 2000). See Appendix I

[56] Id.

[57] Id.

[58] Id.

[59] MOSS BYRETT, THE LEGAL FRAMEWORK—UNAUTHORIZED ACCESS TO COMPUTER SYSTEMS. Penal Legislation in 37 Countries (Last Updated February 22, 2001), by Stein Schjolberg, Chief Judge, Moss Byrett, Norway. http://www.mossbyrett.of.no/info/legal.html. See Appendix II.

[60] Some of the Issues Raised in this section were originally raised in Goldstone and Shave, supra note 26, at 1930-1941. Other issues were raised originally in HONG KONG SECURITY BUREAU, INTER-DEPARTMENTAL WORKING GROUP ON COMPUTER RELATED CRIME (September 2000).

Substantive Laws Need to be Enacted in Every State: Although many countries have developed such laws to prohibit crimes which are facilitated by computer networks, there are still many countries which have not drafted new legislation. Many of these countries are underdeveloped and have no reason to enact legislation to protect their computer networks because they do not have any. These countries create a safe-haven for criminals. This is particularly a problem which combating computer crime because criminals can commit their crimes in any country where they can hook up a computer to a network.

Dual Criminality. When seeking extradition, it is necessary that the substantive law of the country where the investigation takes place has a law which criminalized the alleged behavior. This requirement, called "dual criminality" is especially applicable in cases involving a computer crime because the its propensity to transverse national borders.

Differences in Substantive Laws. Even when substantive laws have been enacted to deal with computer crimes, these substantive laws may not proscribe precisely the same behavior. This is a problem when meeting the requirements of "dual criminality" because it requires that each nation must incorporate the precise crime particularly at issue.

B. Procedural Law

Jurisdiction. According to international law, jurisdiction can be asserted over a criminal based upon the locus of the crime (territorial jurisdiction); the nationality of the offender (nationality jurisdiction); the nationality of the victim (passive personality jurisdiction); the infringement on an important interest of the state (protective jurisdiction); or the violation of a fundamental human right (universal jurisdiction).[61] Because of the nature of network technology, more than one country will often be able to assert jurisdiction over a computer criminal. Standards need to be in place to ensure that a country's assertion of jurisdiction is reasonable, as compared to assertions by other countries.

Other Procedural Laws. Procedural laws facilitate investigations and provide guidance for the collection of evidence. In addition, they create powers and limitations. Clear procedural laws are essential in dealing with computer crimes because of the intrusive nature of many investigations. Increasingly, personal information of the citizens is on computer networks and procedural laws need to be in place in order to ensure the protection of these citizens' rights.

Differences in Procedural Laws. Variations in the procedural laws of states slows down investigations. Creating uniformity in these procedural laws is

[61] See Christopher L. Blakesley, Introduction: Brief Overview of the Traditional Bases of Jurisdiction over Extraterritorial Crime, 33, in M. CHERIF BASSIOUNI, INTERNATIONAL CRIMINAL LAW, PROCEDURAL AND ENFORCEMENT MECHANISMS (2nd Ed. 1999).

essential to effectively investigating computer crimes because of the electronic evidence is highly perishable.

Transborder Searches. The nature of computer crimes can create a scenario where a law enforcement official with a warrant to search a computer in his own country may breach the sovereignty of another country by remotely searching files which are located on a computer in a different country.

Remedies. Since the victims of computer crimes are often located in different countries, a problem arises because you can only extradite an alleged criminal to one country at a time. Additionally, the country that prosecutes and punishes the criminal may not adequately vindicate the rights of the victims.

C. Other Concerns

Training. Investigations of computer crimes require specialized skills. Countries need to allocate resources to training individuals in these specialized skills. Additionally, developed countries need to coordinate with countries where investigators are less knowledgeable.

Public Education. In order to effectively combat computer crime, public education is needed in order to raise security awareness and promote ethics. General computer users need to be taught how to protect their computer systems and administrators of networks need to observe good management practices.

Private Sector's Role. Although government computers are sometimes the targets of attack, the majority of attacks are targeted at private systems. Therefore, law enforcement agencies must effectively participate with and assist the private sector. This is critically important because the private sector has skills and resources that the public sector does not possess.

Language Barriers. Computer crimes often transverse different countries where law enforcement officials speak different languages. This language barrier is problematic, especially because effective investigation requires speed in gathering electronic data from many parts of the world.

Timeliness. The evidence from a computer crime is extremely perishable. This makes it important that investigations are efficient.

IV. Conclusion

In order to counter computer crimes, effective communication is needed between governments, organizations, and individuals. Governments will need to share resources and information with organizations and individuals in order to adequately educate the public of the vulnerabilities of network technology. Governments will also have to share information and resources with each other. This is especially important in combating computer crimes because these crimes can be committed remotely against anyone. This sharing of information and resources may involve developed countries giving information and resources to developing countries. In exchange, these developing countries may enact legislation that closes the loopholes that exist for computer criminals. In addition to communication by governments, private organizations will have to share their resources and expertise with governments in order to effectively catch and prosecute criminals. This communication by all sectors is essential to protecting the potential victims of the computer crimes and ensuring that our institutions operate effectively.