Cybercrime Convention: A Positive Beginning to a Long Road Ahead

I. INTRODUCTION

Information technology has developed rapidly throughout the past decade.[1] Such rapid progress has achieved significant advances in processing and transmitting data through use of computers and computer networks.[2] Some refer to this era as the "Information Revolution," in effect a second "Industrial Revolution."[3] Today, computers affect all aspects of our lives, from medical treatment to air traffic control, online banking and electronic messages ("e-mail").[4] The Internet[5] provides substantial benefits to society, including the ability to communicate with others real-time, access a library of information

1. *See* Doe v. 2Themart.com Inc., 140 F. Supp. 2d 1088, 1091 (W.D. Wash. 2001) (describing the Internet as a "revolutionary advance in communication technology"). Some suggest the Internet is the *greatest* innovation since the printing press. *See* Raymond Shih Ray Ku, *Open Internet Access and Freedom of Speech: A First Amendment Catch-22*, 75 TUL. L. REV. 87, 88 (2000) (analogizing the invention of the Internet to the invention of the printing press); *see also* United Nations Commission on Crime Prevention and Criminal Justice, *International Review of Criminal Policy - United Nations Manual on the Prevention and Control of Computer Crime*, 8th Cong. ¶ 2 (Vienna, April 27 – May 6, 1999), *available at* http://www.uncjin.org/Documents/EighthCongress.html (stressing that today, the Internet touches all aspects of life, irrespective of geographical location) [hereinafter *U.N. Manual*]; Robin Weisman, *U.S. Endorses European Cybercrime Proposal*, NEWSFACTOR NETWORK, Dec. 5, 2000, *at* http://www.newsfactor.com/perl/story/5709.html (recognizing that the U.S., as a whole, has become heavily dependant upon computer networks); Council of Europe, Committee of Experts on Crime in Cyber-Space, Explanatory Memorandum to the Convention on Cybercrime, Europ. T.S. No. 185 ¶ 1 (May 25, 2001), *available at* http://www.conventions.coe.int/Convention/en/Reports/HTML185.htm (asserting the Internet has in one way or another, affected every aspect of human activities) [hereinafter Explanatory Memorandum].

2. *See Doe*, 140 F. Supp. 2d at 1091 (recognizing the significant advances in communication achieved from the Internet).

3. *U.N. Manual*, *supra* note 1, at ¶ 1 (referring to the development of the Internet as the "Information Revolution").

4. *See* Explanatory Memorandum, *supra* note 1, at ¶ 1 (recognizing computer and information technology touch every aspect of our lives).

5. U.S. DEP'T OF JUSTICE, A REPORT OF THE PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET: THE ELECTRONIC FRONTIER n.2 (March 2000), *at* http://www.usdoj.gov:80/criminal/cybercrime/unlawful.pdf (defining the Internet as "collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected worldwide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire or radio.") [hereinafter ELECTRONIC FRONTIER].

and transmit data instantly without leaving home.[6] In addition to these benefits, Internet expansion has fostered new kinds of crimes, additional means to commit existing crimes and increased complexities of prosecuting crimes.[7]

It seems that today, computer crimes affect everyone.[8] A common example is credit card theft whereby a perpetrator illegally obtains the victim's personal information by "hacking"[9] into a website where the victim maintains an account or makes purchases.[10] The perpetrator may steal or charge thousands of dollars to the victim's credit card before he is apprehended, if ever.[11] The problem persists because a perpetrator can easily remain anonymous by instantaneously manipulating or deleting data.[12]

The consequences of crimes committed over the Internet reach farther than traditional methods of committing crimes because there are no geographical border restrictions.[13] Current criminal laws are unable to respond quickly to the

---

6. *See* Explanatory Memorandum, *supra* note 1, at ¶¶ 1-4 (recognizing the ease of accessing and searching information on computer systems regardless of geographic limits); Janet Reno, Speech Before the High Technology Crime Investigations Association 1999 International Training Conference (Sept. 20, 1999), *available at* http://www.cybercrime.gov/agsandie.htm (acknowledging that a man in his kitchen in St. Petersburg, Russia could use his computer to steal from a bank in New York).

7. *See* Jacqueline Klosek, *Convention on Cybercrime Raises Concerns About Data Privacy*, 6 CYBERSPACE LAWYER 2 (2002) (recognizing that although computer networks confer numerous benefits, they also create new opportunities for criminals); *cf.* Ulrick Sieber, *Legal Aspects of Computer-Related Crime in the Information Society*, COMCRIME Study Prepared for the European Commission 19 (Jan. 1998), *available at* http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc (stating that when cyber crimes first emerged, offenses consisted of computer manipulation, sabotage, espionage and illegal use of computer systems). *But see* Marc D. Goodman & Susan Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 2002 UCLA J.L. & TECH. 3, 134 (2002) (reporting that the existence of computer crimes was not widely accepted in the early 1960's because such reports were based on newspaper clippings).

8. *See, e.g.*, Jennifer Lee, *Identity Theft Complaints Double in '02*, NEW YORK TIMES, Jan. 22, 2003, *at* http://www.nytimes.com/2003/01/23/politics/23THEF.html (reporting identity theft increased from 86,000 cases in 2001 to 162,000 in 2002).

9. *See* REVELATION LOA—ASH, THE ULTIMATE BEGINNER'S GUIDE TO HACKING AND PHREAKING, PROAC MANIAC CLUB § I (Aug. 4, 1996), *at* http://www.proac.com/crack/hack/files/starthak.txt (defining hacking as "the act of penetrating computer systems to gain knowledge about the systems and how it works.").

10. *See Internet Fraud Grew in 2002, FTC Says*, REUTERS, Jan. 22, 2003, *at* http:www.siliconvalley.com/mld/siliconviallye/news/editorial/5006038.htm (reporting that consumers lost more than $343 million in 2002 to identity thieves); J.A. HITCHCOCK, NET CRIME & MISDEMEANORS 102 (Loraine Page ed., CyberAge Books 2002) (recognizing the Internet is a prime place for credit card fraud). It is difficult to apprehend the perpetrator because there are no witnesses in Internet crimes and the perpetrator does not have to show the credit card or sign the receipt. *Id.; see also, e.g.*, Press Release, U.S. Dep't. of Justice, *Russian Computer Hacker Sentenced to Three Years in Prison* (Oct. 4, 2002) (on file with author) (reporting Russian hacker sentenced to thirty-six months in prison for, amongst other crimes, stealing from banks).

11. *See, e.g.*, HITCHCOCK, *supra* note 10.

12. *See* Explanatory Memorandum, *supra* note 1, at ¶ 133 (acknowledging the difficulties in identifying the perpetrator of Internet crimes and assessing the harm because data is easily altered or destroyed).

13. *See* Explanatory Memorandum, *supra* note 1, at ¶ 6 (acknowledging that criminals are often located in places other than where the harm occurred); Michael L. Rustad, *Private Enforcement of Cybercrime on the Electronic Frontier*, 11 S. CAL. INTERDISC. L.J. 63, 98 (2001) (discussing the difficulties in prosecuting Internet crimes because there are no geographical borders and thus, no "traditional crime scene"). Internet crimes leave few "digital footprints," thus traditional methods of evidence gathering such as DNA evidence and fingerprints are useless. *Id.*; *see also* Goodman & Brenner, *supra* note 7, at 19 (acknowledging that the perpetrator of an Internet crime does not have to be at the crime scene when the crime is committed); Council

rapid changes in Internet technology.[14] When Congress enacts a statute, perpetrators of cyber crimes find new technology to bypass an essential element of the crime or impede investigations.[15] For example, prior to enacting the *No Electronic Theft Act of 1997* (NET),[16] the United States could not prosecute an individual who hosted a computer bulletin board that enabled anyone to download software at no cost.[17] Authorities were unable to show that the perpetrator received a financial gain from illegal copying, which the law required for criminal wire fraud liability.[18] Similarly, the Philippines Department of Justice dropped charges against the creator of the "ILOVEYOU" virus because existing criminal laws in the Philippines did not apply to computer hacking.[19]

Internet investigations are inherently difficult to conduct because a maze of interconnected computer networks can transmit information instantaneously.[20] Criminals can delete or alter data as quickly as they create it.[21] The ability to destroy or alter data quickly makes it difficult to obtain evidence and perform investigative procedures.[22] For example, perpetrators of crimes can easily

---

of Europe, *Riding the Web – Over 350 Million Surfers*, *at* http://www.coe.int/T/E/Communication_and_Research/Press/Theme_Files/Cybercrime/e_village (noting that Internet users do not need a passport to travel around the world).

14. *See U.N. Manual*, *supra* note 1, at ¶ 5 (explaining that existing criminal laws, the criminal justice systems and international cooperation have not kept up with technological changes); Rustad, *supra* note 13, at 97 (noting that criminal law, by its nature, lags behind technology); *Police Admit They Can't Keep Up With Cyber Criminals*, REUTERS, Nov. 1, 2002, *at* http://www.siliconvalle.com/mld/siliconvalley/news/editorial/4421571.htm (conceding, that law enforcement have lost the cyber crime battle before the fight began). Moreover, law enforcement in the U.K compiled evidence supporting the fact that organized criminal groups are continually using new technologies to commit crimes. *Id.*

15. *See* Rustad, *supra* note 13, at 96 (acknowledging that existing criminal laws are slow to react to changes in technology); *National Security Forum on Cyber Crime Examines Threats To Computer Systems*, HOOVER INSTITUTION, Executive Summary (2000), *at* http://www.hoover.stanford.edu/pubaffairs/newsletter/00winter/crime.html (communicating that States lack adequate laws to combat cyber attacks).

16. 17 U.S.C. § 506(a) (2000).

17. *See* Rustad, *supra* note 13, at 96-7 (discussing that before the NET, a copyright infringer must obtain a financial gain to be liable for computer wire fraud).

18. *See* United States v. LaMacchia, 871 F. Supp. 535 (D. Mass. 1994) (dismissing computer wire fraud charge because the perpetrator had not received a financial gain).

19. *See* Shannon C. Sprinkel, *Note, Global Internet Regulation: The Residual Effects of the "ILOVEYOU" Computer Virus and the Draft Convention on Cyber-Crime*, 25 SUFFOLK TRANSNAT'L L. REV. 491, 492-93 (2002) (noting that the Philippine President enacted the Electronic Commerce Act in response to the inability to punish the perpetrator of the ILOVEYOU virus). The ILOVEYOU virus caused billions of dollars in damages worldwide. *Id.; see also infra* note 76 (discussing further the case of the ILOVEYOU virus).

20. *See* Explanatory Memorandum, *supra* note 1, at ¶ 133 (recognizing the speed at which a perpetrator may alter or delete information on computers and computer systems); *supra* note 12 and accompanying text (identifying the difficulties in investigating internet crimes); Rustad, *supra* note 13 and accompanying text (discussing difficulties in apprehending cyber criminals because there are no territorial borders).

21. *See supra* note 20 and accompanying text (discussing the ease of altering or deleting information on the Internet).

22. *See* Explanatory Memorandum, *supra* note 1, at ¶ 133 (acknowledging the difficulties in identifying

change the sender of an e-mail so the receiver cannot identify the e-mail's origin.[23] Likewise, a criminal could use a computer system to erase data subject to criminal investigations, thus, destroying valuable evidence.[24]

These factors make it difficult to prosecute cyber criminals and create an exigent need for international cooperation.[25] The Council of Europe (CoE) [26] attempted to address these concerns in the Cybercrime Convention.[27] The Cybercrime Convention is an international treaty designed to police cyber crime through international cooperation.[28]

Section II of this note will discuss the purpose and history of the Convention. It will then address why we need a Convention and lastly, where cyber crime is currently most prevalent. Section III will discuss the detailed provisions of the Convention. Finally, the last section of this note will argue that the Convention presents a good starting point for addressing international cyber crime issues, but in reality, is merely aspirational.

The Convention requires additional substantive guidance because it requires parties to prohibit the crimes contained therein, but does not explain how to do so.[29] This note argues that it would be more beneficial if the Convention itself contained the crime elements instead of requiring the parties to create their own. This approach would also be consistent with traditional criminal law principles, which define crime elements at the outset and would also provide consistent application of substantive law principles across nations.[30]

---

the perpetrator of Internet crimes and assessing the harm because data is easily altered or destroyed).

23. *See* Fergusun v. Friendfinders, 94 Cal. App. 4th 1255 (2002) (accusing defendant of violating a state statute because the defendant altered the headers of the e-mail intending to "mask the identity of the sender"), *petition for review denied*, No. A092653, 2002 Cal. LEXIS 2378, at *1 (Cal. Apr. 10, 2002).

24. *See* Explanatory Memorandum, *supra* note 1, at ¶ 133 (recognizing that data is easily altered, moved or deleted instantaneously).

25. *See supra* notes 12, 13 and accompanying text (discussing the difficulty of apprehending and prosecuting perpetrators of Internet crimes).

26. *See About the CoE*, *at* http://www.coe.int/T/E/Communication_and_Research/Contacts_with_the_public/About. The Council of Europe is an intergovernmental organization aimed at protecting human rights; promoting awareness and encouraging development of Europe's culture, identity and diversity; solving problems such as discrimination, AIDS and organized crime and helping to stabilize democracy by supporting political, legislative and constitutional reform. *Id.* At the outset of World War II, ten Western European countries established the CoE, which is based in Stratsbourg, France. *Id.* Today, there are forty-four members of the CoE whose purpose is to strengthen democracy, protect human rights and oversee the law throughout the member states. *Id.* The CoE should not be confused with the European Union. *Id.* Since existence, the CoE adopted twenty conventions and more than eighty recommendations in the criminal law area. *See About the CoE*, *at* http://www.coe.int/T/E/Communication_and_Research/Contacts_with_the_public/About.

27. Council of Europe, Committee of Experts on Crime in Cyber-Space, European Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185 [hereinafter Convention], *available at* http://conventions/coe/int/Treaty/ENprojects/FinalCybercrim.htm.

28. *Id.*

29. *See infra* Section IV.B and accompanying text (advocating the Convention must provide additional substantive guidance).

30. *See National Security Forum on Cyber Crime Examines Threats To Computer Systems*, *supra* note 15 (explaining that due to the "speed and technical complexity" of the Internet, we need prearranged, agreed upon

II. BACKGROUND

A. Purpose of the Convention

The primary purpose of the Convention is to harmonize domestic substantive criminal law offenses and investigative procedures.[31] The Convention drafters' principal concerns were two-fold.[32] First, they wanted to ensure crime definitions were flexible enough to adapt to new crimes and methods of committing existing crimes as they evolve.[33] Second, the drafters wanted the Convention to remain sensitive to the legal regimes of domestic states.[34]

These concerns were especially challenging in the human rights area because states have different moral and cultural values.[35] For example, European nations have a much higher degree of privacy protection than the United States.[36] The United States, on the other hand, has stronger speech protection than other nations.[37] To further its purpose, the Convention also empowers parties to restrict or eliminate criminalization of certain offenses and limit investigative procedures by reservation.[38] The Convention's drafters,

---

procedures for investigating and prosecuting cyber crimes).

31. *See* Convention, *supra* note 27, Preamble (recognizing the need to ensure a proper balance between human rights and law enforcements needs); Explanatory Memorandum, *supra* note 1, at ¶¶ 6, 31, 145 (articulating the need to balance human rights with individual privacy in defining crimes and implementing investigative procedures); U.S. Senate Committee on Commerce, *Hearing on Security Risks in Electronic Commerce*, in FDHC Political Transcripts (July 16, 2001) (statement of U.S. Senator Ron Wyden (D-OR) Chairman) (discussing the Convention and stating, "we're trying to balance security versus liberty").

32. *See, e.g.*, Explanatory Memorandum, *supra* note 1, at ¶ 36 (articulating the Convention's purpose in using technology neutral language is to accommodate for both current and future technology); *supra* note 31 (discussing the need to balance human rights with law enforcement needs).

33. *See* Explanatory Memorandum, *supra* note 1, at ¶ 36 (stating that the Convention uses "technology-neutral" language to adapt to future technology).

34. *See supra* note 31 and accompanying text; *see also, e.g.*, Explanatory Memorandum, *supra* note 1, at ¶ 122 (allowing signatories to make certain reservations to gain the widest ratification possible).

35. *See* Explanatory Memorandum, *supra* note 1, at ¶ 145 (recognizing the Convention applies to parties of many different legal systems and cultures).

36. *See* Robert R. Schriver, *Note, You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2778 (2002) (explaining that the U.S. and Europeans view privacy in "fundamentally different ways"). U.S. Companies tend to reject higher international privacy standards. *Id.*; *see also* Tamara Loomis, *A Few Companies Have Complied With EU Law*, N.Y. L.J., Aug. 30, 2001, at 5 (finding U.S. companies do not see privacy as a "normal cost of doing business").

37. *See* Draft Hate Speech Protocol to the Convention ¶ 8 (Sept. 5, 2002), *available at* http://assembly.coe.int//Documents/WorkingDocs/doc02/EDOC9538.htm (recognizing existence of greater speech protection because of differing views in the U.S. as compared to Europe) [hereinafter Draft Hate Speech Protocol]; *see also, e.g.*, Elissa A. Okoniewski, *Yahoo!, Inc. v. LICRA: The French Challenge to Free Expression on the Internet*, 18 AM. U. INT'L L. REV. 295, 296 (2002) (explaining France's freedom of speech laws are not as broad as the U.S.); Brandenburg v. Ohio, 395 U.S. 444 (1969) (holding that hate speech is only punishable if there is an imminent threat of physical harm).

38. *See, e.g.*, Convention, *supra* note 27, at Ch. 2, Art. 6 (allowing a party to restrict offenses related to "misuse of devices"); Convention, *supra* note 27, at Art. 10 (permitting countries to make a reservation not to

thus, attempted to balance crime definitions and the investigative needs of law enforcement with individual rights.[39]

B. Evolution of the Cybercrime Convention

There are three multilateral organizations[40] that focused on international cyber crime policy: the CoE,[41] the European Union (EU)[42] and the G-8.[43] The Organization for Economic Cooperation and Development (OECD)[44] and the United Nations (UN)[45] also participated, but to a lesser extent.[46]

In response to the increase in cyber crime the CoE's Committee of Ministers[47] adopted Recommendation No. R. (89) 9 ("R89") [48] in 1989, which required that member states consider computer crimes when reviewing old and enacting new legislation.[49] In 1995, the CoE adopted Recommendation No.

---

impose copyright infringement liability if other remedies are available); Convention, *supra* note 27, at Art. 11 (authorizing parties to restrict or eliminate aiding and abetting liability); Convention, *supra* note 27, at Ch. 4, Art. 42 (outlining procedure for parties to make a reservation).

39. *See supra* note 31 and accompanying text.

40. *See* Michael Sussman, *The Critical Challenges From International High-Tech and Computer Related Crime at the Millennium*, 9 DUKE J. COMP. & INT'L L. 451, 476 (1999) (defining multilateral organizations as groups with multiple-national membership).

41. *See About the CoE*, *supra* note 26 and accompanying text (describing the CoE); Sussmann, *supra* note 40, at 476 (discussing the extent of the CoE's past involvement in addressing cyber crime).

42. *See European Union at a Glance*, *at* http://europa.eu.int/abc-en.htm. The EU has fifteen member states, which are also members of the CoE. *Id.* Principles of democracy and rules of law govern the EU. *Id.* Its principle objectives are to establish European citizenship (fundamental rights, freedom of movement and political rights); ensure freedom, security and justice; promote economic and social progress and assert Europe's role in the world. *Id*

43. *See What is G8*?, *at* http://birmingham.g8summit.gov.uk/brief0398/what.is.g8.shtml. The G-8 originated in 1975 at an Economic Summit convened by President Valery Giscard d'Estaing of France. *Id.* Membership includes the United States, Canada, France, Germany, Italy, Japan, Russia and the United Kingdom. *Id.* These countries are the world's most powerful democracies because they are global leaders economically, technologically, legally, and politically. *Id.* At their 1998 Summit, the G-8 adopted a comprehensive plan to fight high-tech and computer-related crime. *Id.* Unlike the COE and EU, the G-8 is not governed by international convention or constrained by a convention-created bureaucracy. *See What is G8*?, *at* http://birmingham.g8summit.gov.uk/brief0398/what.is.g8.shtml. It can therefore move faster and address new and emerging areas as the will of its leaders dictates. *Id.*

44. *See About the OECD*, *at* http://www.oecd.org/about/general/index.htm. The OECD consists of 30 member countries organized for the purpose of developing economic and social policy. *Id.* The members consist of the twenty countries in Europe and North America, Japan, Australia, New Zealand, Finland, Mexico, Hungary, Poland, Korea, the Czech Republic and Slovack Republic. *Id.*

45. *See About the United Nations*, *at* http://www.un.org/aboutun/index/html.

46. *See* Sussmann, *supra* note 40, at 476 (noting that the U.N. and OECD participated in efforts to combat cyber crime but to a lesser extent than the CoE).

47. *See About the CoE*, *supra* note 26 and accompanying text (discussing functions of the CoE). The Committee of Ministers is the decision-making organ of the CoE, which consists of members from each of the member states. *Id.* According to the CoE, a European Foreign Minister is equivalent in rank to a Secretary of State. *Id.*

48. *See* Recommendation No. R. (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime (1989), *available at* http://www.cm.coe.int/ta/rec/1989/89r9.htm [hereinafter Recommendation No. 89].

49. *Id.; see also* Sussmann, *supra* note 40, at 478 (discussing the provisions of Recommendation No. 89).

(95) 13 ("R95")[50] establishing procedures for applying R89.[51] Investigations were still slow and difficult to coordinate, resulting in the untimely information retrieval necessary to combat cyber attacks.[52] Moreover, many countries lacked criminal cyber law statutes.[53] Countries with such laws found their laws were outdated.[54]

In 1997, the CoE formed a Committee of Experts on Crime in Cyber-space ("PC-CY") in response to prior failed efforts to prevent and deter cyber attacks or address the damaging consequences of such acts.[55] The United States Department of Justice (DOJ) also significantly participated in this effort.[56] The CoE finalized the Convention on November 8, 2001 and opened it for signature on November 23, 2001.[57] Twenty-six of the forty-three European member states signed the Convention, along with four non-members states, Canada, Japan, South Africa and the United States.[58] The Convention will become effective when at least five states ratify it, three of which must be European member states.[59]

C. Why the Need for a Cybercrime Convention?

Financial gain motivates many cyber criminals.[60] Financial experts agree that cybercrime is most prevalent in the United States because of its financial wealth and the volume of commercial transactions occurring within its

50. *See* Recommendation No. R. (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected With Information Technology (1995), *available at* http://www.coe.fr/cm/ta/rec/1995/95r13.htm [hereinafter Recommendation No. 95].

51. *Id.*

52. *See, e.g.*, ABRAHAM D. SOFAER, ET AL., *A PROPOSAL FOR AN INTERNATIONAL CONVENTION ON CYBER CRIME AND TERRORISM*, HOOVER INSTITUTION, ET AL., *at* http://oas.org.juridico/english/monograph.htm (Aug. 2000) (noting many nations have outdated criminal computer laws unequipped to deal with changing technology making investigations slow and difficult).

53. *See id.*

54. *See id.*; *supra* note 14 and accompanying text (explaining current criminal laws lag behind technology).

55. *See* Ryan M. F. Baron, *A Critique of the International Cybercrime Convention*, 10 COMMLAW CONSPECTUS 263, 269 (2002) (discussing the formation of the PC-CY).

56. Dep't of Justice, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime (Draft24REV2)*, *at* http://www.usdoj.gov/criminal/cybercreim/newCOEFAQs.html (July 10, 2001) (acknowledging that the DOJ participated as an active "observer" in the development of the convention).

57. *See generally* Convention, *supra* note 27 (noting the CoE opened the Convention for signature on November 23, 2001 in Budapest).

58. *See generally* Convention, *supra* note 27.

59. *See generally* Convention, *supra* note 27. Presently, Albania and Croatia are the only states to ratify the Convention. *Id.; see also* Center for Democracy and Technology, *International Issues: Cybercrime* (visited Oct. 21, 2002) http://www.cdt.org.international/cybercrime (recognizing the Convention has no legally binding force until ratified by national governments).

60. *See* Rustad, *supra* note 13, at 72-3 (recognizing that the majority of innovators are motivated by financial gain); Jon Swartz, *Hackers Evolve From Pranksters Into Profiteers*, USA TODAY, March 16, 2003, *at* http://www.usatoday.com/tech/news/computersecurity/2003-03-16-hacking_x.htm (finding internet related theft complaints tripled in 2002).

borders.[61] Criminals also target the U.S. because of its strong First Amendment protections.[62] Indeed, the U.S. is known amongst the western world as a "haven" for racial and hate speech.[63]

Globally, cyber crimes constitute more than $15 billion in damages every year.[64] Most organizations do not report cyber crimes because they fear exposure would make them vulnerable to future attacks by copycats or cause a loss of public confidence.[65] The cost and difficulty associated with investigations also hinders a company's willingness to report crimes.[66] Experts predict that developing nations will need to experience significant technological growth over the next decade to be "self-sufficient and more competitive" in an international economy.[67] Developing countries could thus eventually direct more cyber crimes to the United States, although financial constraints will most likely hinder such growth.[68]

---

61. *See The Threat of International Crime and Global Terrorism and the International Law Enforcement Programs of the Federal Bureau of Investigation: Before the House of Int'l Relations Comm.*, 105th Cong. (1997) (statement of Louis J. Freeh, Director of the Federal Bureau of Investigation), *available at* http://www.fbi.gov/pressrm/congress/congress97/intiatives-int.htm (recognizing cyber crimes are most prevalent in the U.S.); Matt Rosen, *The US-EU Convention on Cybercrime*, 2002 UCLA J.L. & TECH. NOTES 19 (2002) (recognizing the U.S. is regarded as the center of the Internet).

62. *See* Draft Hate Speech Protocol, *supra* note 37, at ¶ 8 (admitting that perpetrators frequently place racist messages on American servers to avoid prosecution).

63. *See* Draft Hate Speech Protocol, *supra* note 37, at ¶ 8 (discussing the first racial website appeared in the 1990's). Since then, the number of racist websites has increased dramatically. Draft Hate Speech Protocol, *supra* note 37, at ¶ 8. There are now 4,000 racist web cites, including 2,500 in the United States whereas in 1995 there were only 160 such websites. *Id.*

64. Steve Gold, *Security Breaches Cost $ 15 Bil. Yearly*, NEWSBYTES, Nov. 15, 2000, *at* http://www.newsbytes.com/news/00/158197.html.

65. *See* Steve Range, *Renewed Calls To Fight Cybercrime*, PC WORLD (United Kingdom), Feb. 15, 2002, *at* http://www.pcw.co.uk/Analysis/1129289 (explaining companies fail to report cyber crimes because they do not want to admit weak security or attract other criminals); Bob Tedeschi, *Crime is Soaring in Cyberspace, But Many Companies Keep it Quiet*, NEW YORK TIMES, Jan. 27, 2003, at 4 (noting that companies are reluctant to report cyber attacks for fear of losing confidence from customers and shareholders, inviting other attacks or facing ridicule from competitors). Companies would rather lose money to hackers than initiate an investigation. *Id.*

66. *See, e.g.*, Andy McCue, *UK Law Lets Hackers Get Away With It*, PC WORLD (United Kingdom), June 11, 2001, *at* http://www.pcw.co.uk/News/1126671 (claiming some U.K. companies are prepared to write off 50,000 pounds because of difficulties in getting a conviction). A survey conducted by the American Bar Association reported that companies who were victims of computer crime suffered economic losses ranging from $145 million to $730 million. *U.N. Manual*, *supra* note 1, at ¶ 29; *see also* Computer Crime and Security Survey Conducted by the Computer Security Group and the FBI Computer Intrusion Squad – *Financial Losses Due to Internet Intrusion, Trade Secrete Theft and Other Cyber Crimes Soar*, *at* http://www.gocsi.com/prelea_000321_htm (Mar. 12, 2001) (reporting the amount of damages from computer crimes has increased from $110 million in 1997 to $378 million in 2001).

67. *See U.N. Manual*, *supra* note 1, at ¶ 13 (requiring developing nations to experience "significant growth" if they intend to become "economically self-sufficient" and compete in world markets); *Internet Users to Reach 655 Million by Year-end*, SIDNEY MORNING HERALD, Nov. 19, 2002, *at* http://www.smh.com/au/articles/2002/11/19/1037599406943.html (explaining that poor countries ability to adapt to current commerce depends on their capacity to integrate into "regional and global supply chains").

68. *See Internet Users Reach 655 Million By Year-end*, *supra* note 67.

Cyber criminals range in both age and skill level.[69] Studies show, however, that employees are the largest threat.[70] Ostensibly, ex-employees, as corporate insiders, can easily exploit their knowledge of a company's computer network.[71] For example, an employee may steal a company's source code by entering the corporate network remotely through unauthorized access using confidential passwords.[72] Companies could prevent or at least mitigate computer fraud if they focus more on security through password controls, employee training and background checks.[73]

Many states have enacted cyber crime laws.[74] Those laws, however, were confined to a specific territory and were frequently outdated.[75] Perpetrators of crimes have thus gone unpunished.[76] Until we are able to cope with the fast-paced changes of the Internet, new kinds of crimes may continue to go unpunished.[77] Those countries that actually have computer crime legislation will continue to operate under a conglomeration of varied and often disjointed

---

69. *See U.N. Manual*, *supra* note 1, at ¶ 34 (noting that criminal behavior reaches across a wide spectrum of society of all different ages and demographics).

70. *See, e.g.*, Xenia Ley Parker, *Understanding Risk*, 2001 INTERNAL AUDITOR, at 61 (arguing that insiders are a corporation's biggest security threat, comprising between seventy-five and eighty percent of security violations); *U.N. Manual*, *supra* note 1, at ¶ 35 (declaring employees are the biggest threat, estimating ninety-percent of computer crimes are committed by insiders); McCue, *supra* note 66 (predicting an explosion of cybercrime from ex-employees who use their knowledge of the corporate networks to commit crimes).

71. *See, e.g.*, Parker, *supra* note 70, at 86 and accompanying text.

72. *See* Rustad, *supra* note 13, at 75 (noting that hackers can steal a company's source code remotely and gain access to a wealth of information).

73. *See* Rustad, *supra* note 13, at 86 (advocating better training, password protection and screening would mitigate computer fraud).

74. *See* s*upra* notes 14, 52 and accompanying text (avering many states have cyber crime laws, but those laws are largely outdated).

75. *See* s*upra* notes 14, 52 and accompanying text; *see also* Explanatory Memorandum, *supra* note 1, at ¶ 6 (declaring the need for an international Convention because domestic criminal laws are generally confined to a specific territory); *Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information*, MCCONNELL INTERNATIONAL, Dec. 2000, *at* http://www.mcconnellinternational.com/services/cygercrime.htm (finding most countries have not clearly encompassed provisions within their existing criminal law statutes to prohibit cyber crimes); Joe Ticehurst, *Cybercrimanls Are Getting Away With It*, VUNet.com (United Kingdom), Aug. 12, 2000, *at* www.vunet.com/News/1115223 (reporting nine of the fifty-two countries at the time had extended existing criminal laws to cyber crimes). Thirty-five of those surveyed have not updated their laws to address *any* type of cybercrime. *Id. (*emphasis added*)*.

76. *See, e.g.*, Sprinkel, *supra* note 19, at 92-3 (responding to the crippling effect of the "ILOVEYOU" virus, the Philippine President outlawed computer crimes and enacted the Electronic Commerce Act ("ECA") on June 14, 2000). Unfortunately, it was too late to prosecute the creator of the "ILOVEYOU" virus because the ECA was not retroactive. Sprinkel, *supra* note 19, at 92-3. Thus, billions of dollars in damages went unpunished due to "gaps" in the criminal laws of countries that did not foresee the need to account for these crimes in the context of computers and the Internet. *Id.*; *see also supra* note 18 and accompanying text (discussing the *Lamachia* debacle); Range, *supra* note 65 (urging the United Kingdom to rewrite the Computer Misuse Act, implemented twelve years ago to be more consistent with the "harsh realities of the Internet age"). The U.K. enacted this law prior to when most users were surfing the Internet or when corporate systems could access the global network. Range, *supra* note 65. The Act addressed computer fraud in the context of "trespass." *Id.* Security experts say the lawmakers should rewrite the statute to focus on "fraud." *Id.*

77. *See, e.g.*, *supra* note 76 and accompanying text.

laws.[78] The CoE adopted the Convention in response to the need for harmonization.[79] The Convention is a welcome and necessary advance to international criminal laws. It is, however, largely "aspirational" and fails to provide substantive guidance for defining precisely what conduct constitutes a cyber crime. The Convention also does not identify what specific legal procedures states should apply when investigating and prosecuting cyber crimes.

III. THE CYBERCRIME CONVENTION PROVISIONS

The Convention consists of four chapters.[80] The first chapter enunciates key definitions applicable throughout the document.[81] Chapter Two includes three sections.[82] The first section articulates the crimes included in the Convention and requires signatories to enact legislation to establish those crimes as domestic criminal offenses.[83] Section Two establishes "powers and procedures" that signatories must follow in investigating and prosecuting criminal offenses, including expedited preservation of data, production and order, search and seizure and collection of evidence.[84] The last section establishes guidelines for asserting jurisdiction over criminals.[85]

Chapter Three of the Convention establishes general and specific principles for international cooperation and mutual assistance for investigating and prosecuting cyber crimes.[86] Chapter Three empowers a party to compel another party to provide information under their control through search and seizure, real-time collection and data interception procedures.[87] The final chapter encompasses all other miscellaneous provisions, including but not limited to signature, amendments and settlement of disputes.[88]

IV. THE CONVENTION DOES NOT PROVIDE SUBSTANTIVE LAWMAKING

78. *See supra* notes 14, 52 and accompanying text (criticizing countries that lack computer crime laws or because such laws are outdated).

79. *See generally* Convention, *supra* note 27.

80. *See generally* Convention, *supra* note 27.

81. *See* Convention, *supra* note 27, at Ch. 1 (articulating the definitions included in the convention are: what constitutes a "computer system," what qualifies as "computer data" who is considered an Internet "service provider" and what is included within the parameters of "traffic data").

82. *See* Convention, *supra* note 27, at Ch. 2.

83. *See* Convention, *supra* note 27, at Ch. 2, § 1. These criminal offenses include: offences against confidentiality, data integrity and availability such as access and misuse of devices; computer related offences for forgery and fraud; content offences related to child pornography; copyright infringement and ancillary liability for aiding and abetting. Convention, *supra* note 27.

84. *See* Convention, *supra* note 27, at Ch. 2, § 2 (defining procedural law requirements of the Convention).

85. *See* Convention, *supra* note 27, at Ch. 2, § 3 (discussing jurisdictional requirements under the Convention).

86. *See* Convention, *supra* note 27, at Ch. 3 (encompassing standards for international cooperation).

87. *See* Convention, *supra* note 27, at Ch. 3.

88. *See* Convention, *supra* note 27, at Ch. 4 (containing the final Convention provisions).

GUIDANCE

The CoE was the first organization to develop an international cyber crime Convention.[89] Although seemingly aspirational, the Convention presents a noble effort towards the harmonization of international law and procedure. Its provisions are not detailed enough to provide substantive rules and procedures for combating cyber crime.

A. The Convention's Key Definitions Are Too Broad

Chapter One of the Convention identifies key definitions critical to interpreting the Convention's provisions.[90] The definitions are overly broad and unclear about what conduct falls within the definitions.[91] The Convention definitions should not, however, be so narrow that they disable the Convention's ability to adapt with technological changes.[92] Instead, these Convention definitions should include only computer and Internet related transactions.[93]

For example, the Convention defines a computer as "any device or a group of interconnected or related devices one or more of which, pursuant to a

89. *See About the* CoE, *supra* note 26 and accompanying text (discussing the purpose and function of the CoE).

90. *See* Convention, *supra* note 27, at Ch. 1 (defining terms of the Convention).

91. *See* U.S. Attorney General Janet Reno, Keynote Address to the Meeting of the G-8 Senior Experts' Group on Transnational Organized Crime, Chantilly, VA (Jan. 21, 1997), *available at* http://www.usdog.gov/criminal/cybercrime/agfranc.htm (stating "countries need to reach a consensus as to which computer and technology-related activities should be criminalized, and then commit to taking appropriate domestic actions."); Center for Democracy and Technology, *Comments on Council of Europe Draft "Convention on Cyber-crime" (Draft No. 25)* (visited Oct. 2, 2002) http://www.cdt.org/international/cybercrime/010206cdt.shtml (recognizing that the Convention raises concerns about what conduct falls within its broad definitions) [hereinafter *CDT Comments*]; David Banisar & Gus Hosein, *A Commentary on the Council of Europe Cybercrime Convention*, Section by Section Analysis - Art. 1 - Definitions (Oct. 2000) (manuscript on file with the author) (finding the definitions in the Convention "problematic" because they are either too far-reaching, ambiguous or lack support); Abraham Sofaer, *National Security Forum on cyber Crime Examines Threats to Computer Systems*, Hoover Institution Newsletter (2000), *at* http://www-hoover.standford.edu/pubafairs/newsletter/00winer/crime.html (finding the lack of uniformity amongst countries challenging because, for example, each country defines "unauthorized access" differently); David R. Johnson & David Post, *Surveying Law and Borders: Law And Borders – The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996) (recognizing that an individual country cannot satisfactorily govern the Internet).

92. *See* Explanatory Memorandum, *supra* note 1, at ¶ 36 (discussing the purpose of the Convention is to promote adaptability to new crimes or different ways of committing existing crimes).

93. *See* Thomas Claburn, *Fear of Hacked Planet – A New Cure for Cybercrime May Be Worse Than the Disease; Government Activity*, ZIFF DAVIS SMART BUSINESS FOR THE NEW ECONOMY, May 1, 2002, at 39 (advocating that the Convention's definitions should be narrower and only apply to a few specific crimes); *U.N. Manual*, *supra* note 1, at ¶ 7 (identifying lack of global consensus on the legal definitions of criminal conduct as one of the problems surrounding international cooperation); *CDT Comments*, *supra* note 91 (justifying a Convention that deals with harmonizing laws around a "core set of offenses"). Terms that are more narrowly defined will help avoid unanticipated future lawsuits for conduct the Convention was not meant to address. *CDT Comments*, *supra* note 91.

program, performs automatic processing of data."[94] The definition 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.[95] Moreover, it is difficult to tell whether the definition of computer data[96] includes items such as bar codes used to scan groceries at the supermarket.[97]

The Convention's broad definition of a service provider could conceivably encompass any Internet user who maintains a website, thus potentially imposing a huge cost and labor burden on a large user group.[98] Furthermore, it is not clear whether the Convention's ambiguous definition of traffic data[99] includes things such as hyperlinks[100] and http requests.[101] If the definition of traffic data does include hyperlinks and http requests, the definition may be far more invasive on communication than the drafters intended.[102]

Finally, it is unclear whether the term communication used in defining traffic data includes surfing the Internet, which is traditionally both a communication and a transaction.[103] Arguably, the act of reading e-mail by connecting through an ISP to a web mail provider is a transaction rather than

---

94. Convention, *supra* note 27, at Ch. 1, Art. 1(a).

95. *See* Banisar & Hosein, *supra* note 91.

96. *See* Convention, *supra* note 27, at Ch. 1, Art. 1(b) (defining computer data as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.").

97. *See* Banisar & Hosein, *supra* note 91 (questioning whether items such as barcodes are included within the definition of a computer system).

98. *See* Convention, *supra* note 27, at Ch. 1, Art. 1(c) (defining a service provider as (a) "any public or private entity that provides to users of its service the ability to communicate by means of a computer system and (b) any other entity that processes or stores computer data on behalf of such communication service or users of such service."); *see also* Paul Meller, *Hate Crime Footnote Added to Council of Europe Cybercrime Convention*, INFOWORLD DAILY NEWS, Nov. 9, 2001 (reporting ISPs dissatisfaction with the Convention because they fear they will not be reimbursed for expenses incurred to meet law enforcement requests); Mike Godwin, *International Convention on Cybercrime Poses Burden on High-Tech Companies*, IP WORLDWIDE, Apr. 4, 2001 (expressing concern that massive compliance orders will disrupt business); Donovan Stelzner, *The Draft Convention on Cybercrime: What Every Internet Service Provider Should Know*, 2001 INTERNET L. J. (Feb. 5, 2001), *available at* http://www.tilj.com/content/webarticle02050103.htm (suggesting a clearer definition of ISP may limit those who are providing services to the public).

99. *See* Convention, *supra* note 27, at Ch. 1, Art. 1(d) (defining traffic data as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communications' origin, destination, route, time, date, size, duration, or type of underlying service.").

100. *See Webopedia*, *at* http://www.webopedia.com (defining hyperlinks as "an element in an electronic document that links to another place in the same document or to an entirely differently document.") (last visited Mar. 24, 2003).

101. *See* HITCHCOCK, *supra* note 10, at 321 (defining http requests as "a set of instructions for communication between a server and a site.").

102. Banisar & Hosein, *supra* note 91 (expressing concerns over the Convention's broad definition of traffic data).

103. Banisar & Hosein, *supra* note 91 (questioning what types of conduct the term communication, within the definition of traffic data, encompasses).

communication.[104] Finally, denial of service attacks ("DDOS")[105] could be construed as a communication even though they also include a transactional aspect.[106]

B. The Convention, Not the Individual Signatories Should Define the Elements of the Crimes

The Convention encompasses a finite list of crimes, some of which currently are crimes in one signatory country but are not in another.[107] Convention signatories agree to criminalize offenses included therein, in their domestic laws.[108] The Convention does not, however, include guidance detailing the elements required for those offenses.[109] In the case of countries that do have legislation, lack of guidance will still likely result in different conduct establishing guilt for the same crimes.[110]

For example, the U.S. may want to prosecute a citizen from France for the crime of illegal access. France's criminal cyber statute may not include access to a computer system connected to another computer system within the definition of illegal access. Thus, the U.S. could not prosecute a French citizen who accessed a computer connected to another computer. In contrast, if the U.S. and France were both signatories to a Convention codifying the elements of the crime, the U.S. could prosecute a French citizen because both countries would recognize the requisite criminal elements.

Furthermore, if signatories do not agree upon the elements of each crime, we could face a similar debacle as was confronted in *Yahoo, Inc. v. La Ligue*

---

104. Banisar & Hosein, *supra* note 91 (arguing that reading e-mail is a transaction rather than a communication).

105. *See* Center for Democracy & Technology, *Testimony on Denial of Service Attacks and the Federal Response* (visited Feb. 29, 2000) http://www.cdt.org/security/dos (defining denial of service attack as attacks where a hacker floods the computer or network with enormous data requests causing it to cease functioning). Denial of service attacks can impact a company's business and prevent legitimate customers from transacting business with that company. *Id.; see also* Brian Krebs & David McGuire, *More Than One Internet Attack Occurred*, WASHINGTONPOST.COM, Oct. 23, 2002, *at* http://www.commoncriteria.org/news/newsarchive/Oct2002/oct17.htm (noting the F.B.I. is investigating two simultaneous DDOS attacks on 13 computer servers). The White House Press Secretary Ari Fleischer expressed difficulty in discovering the identity of DDOS hackers because they use computers, which often belong to third parties and either manually or remotely program the computer to carry out the attacks. *Id.*

106. *See* Krebs & McGuire, *supra* note 105.

107. *See* Convention, *supra* note 27, at Ch. 1; *supra* notes 74, 75, 78 and accompanying text (identifying that some states do have laws in place dealing with electronic crimes).

108. *See* Convention, *supra* note 27, at Ch. 2 (requiring that "Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law . . . .").

109. *See* Baron, *supra* note 55 (identifying the most controversial debate relative to the Convention is what type of laws countries should enact domestically). There is great concern because the Convention requires countries to enact new criminal legislation, but does not provide countries with any guidance. Baron, *supra* note 55. The Convention leaves open how these domestic laws, once enacted, will impact the Convention and the other signatories. *Id.*

110. *See, e.g.*,Convention, *supra* note 27 (allowing parties to criminalize conduct within the Convention according to that country's own interpretations, morals and political views).

Contre Le Racism Et L'Antisemitisme [111] recently. In the *Yahoo* debacle, the French Government found *Yahoo* violated French law because *Yahoo*'s auction website permitted the sale of Nazi memorabilia.[112] The Convention would not require the U.S. to cooperate with French authorities if the crime is political.[113] Authorities found this problematic because the U.S. considered the sale of Nazi memorabilia a political offense but France considered it a crime against humanity.[114]

Crime standardization could, however, pose some difficulties for regulators because countries may be reluctant to sign the Convention if it infringes upon domestic legal regimes and cultures.[115] Specifically, the CoE may face resistance in attempting to harmonize content related crimes, such as hate speech, because states established these types of crimes according to their own cultural values.[116] For example, the CoE has recently approved a hate speech provision banning hate speech on the Internet.[117] This ban includes hyperlinks to other web cite pages containing offensive content.[118] The United States vehemently opposes the hate speech provision because it abridges the First Amendment.[119] Accordingly, the U.S. is unlikely to ratify the Convention.[120] Critics believe a ban on hate speech in the Convention would encourage hate groups to solely target the U.S.[121]

The Convention drafters purposely empowered signatories to enact crime legislation out of concern that if the Convention retained too much power,

---

111. 169 F. Supp. 1181 (N.D. Cal. 2001).

112. *Id.* at 1184 (noting the sale of Nazi memorabilia was legal in the U.S. but not in France).

113. *See* Convention, *supra* note 27, at Ch. 3, Art. 27 ¶ 4(a) (permitting a requested party to refuse to assist the requesting party if the requested party considers the offense political).

114. Yahoo, Inc. v. La Ligue Contre Le Racism Et L'Antisemitisme, 169 F. Supp. 1181 (N.D. Cal. 2001).

115. *See* Explanatory Memorandum, *supra* note 1, at ¶ 145 (recognizing the sensitivity in respecting parties' existing legal regimes).

116. *See* Rustad, *supra* note 13, at 96 (recognizing that balancing privacy against law enforcement needs will be more difficult because of the "radically different fundamental rights and freedoms" between countries).

117. *See* Draft Hate Speech Protocol, *supra* note 37 (banning "any written material, any image or any other representation of ideas or theories, which advocates, promotes or invites hatred, discrimination or violence against any individual or group of individuals, based on race, color, descent or national or ethnic origin, as well as religion if used as a pretext for these factors."); *see also* Julia Scheeres, *Europeans Outlaw Net Hate Speech*, WIRED NEWS, Nov. 9, 2002, *at* http://www.wired.com/news/business/0,1367,56294,00.html (announcing the Council of Europe has adopted measures criminalizing Internet hate speech).

118. *See* Draft Hate Speech Protocol, *supra* note 37.

119. *See* Declan McCullagh, *U.S. Won't Support Net "Hate Speech" Ban*, CNET News.com, Nov. 15, 2002, *at* http://www.news.com/2100-1023-965983.html (declaring that the U.S. can't be a party to any treaty that abridges the U.S. constitution). The First Amendment protects hate speech, notwithstanding a few very narrow exceptions that allow the Government to ban speech that would constitute a breach of the peace or speech directed at an individual intended to "provoke imminent lawless conduct." *Id.* The hate speech ban, however, is not tied to the Convention itself and thus, does not require signatories to adopt it. *Id.* Civil Liberties Unions praised the U.S. for taking this position on the new hate speech protocol. *Id*

120. McCullagh, *supra* note 119. *But see* Paul Meller, *Europe Moving Toward Ban on Internet Hate Speech*, NEW YORK TIMES, Nov. 10, 2001, at 3 (considering United States constitutional protections in drafting the hate speech protocol as a "side agreement," which the U.S. can choose not to sign).

121. Draft Hate Speech Protocol, *supra* note 37 and accompanying text.

members would be reluctant to ratify it.[122] The drafters believed this was a better solution than if only a few countries ratified the Convention.[123] Based on these examples, however, the Convention would be more valuable if it also included the elements of the crimes rather than leaving this decision to the signatories.[124]

C. The Convention Must Specify Consistent Procedures for Investigating and Prosecuting Cyber Crimes

The Convention requires signatories to enact procedures domestically for evidence gathering, including expedited searches, seizures and data collection.[125] Again, the Convention requires the parties to determine how to implement those procedures.[126] In doing so, the drafters intended to respect distinctions in cultures and legal systems by recognizing, for example, disparities amongst parties in levels of privacy protection or speech protection.[127]

Specifically, the Convention requires that the country from where the crime originates, must, at the request of the harmed country, preserve and disclose data to the requesting party.[128] The provision does not, however, specify what law enforcement must demonstrate before accessing potentially private information.[129] Parties with different human rights protections could thus encounter conflicts pertaining to what data must be disclosed.[130] For example, many states do not consider the interception of content data and the collection of traffic data equivalent privacy interests because data collection, without more, does not disclose the communication's actual content.[131] Consequently,

122. *See* Explanatory Memorandum, *supra* note 1, at ¶ 145 (articulating the Convention's purpose is to strike a balance between harmonizing international law and the sanctity of the sovereign).

123. *See* Explanatory Memorandum, *supra* note 1, at ¶ 122 (seeking the widest ratification possible).

124. *See U.N. Manual*, *supra* note 1, at ¶ 276 (advocating the need to legislate substantive criminal law in each State consistently to avoid loopholes or conflicting interpretations of the laws).

125. *See* Convention, *supra* note 27, at Ch. 2, Art. 16-17 (defining requirements for expedited preservation and storage of computer data and expedited preservation and partial disclosure of traffic data).

126. *See* Convention, *supra* note 27; *see also* Explanatory Memorandum, *supra* note 1, at ¶ 145 (leaving the implementation of procedures up to the individual countries in accordance with their domestic laws and procedures); Baron, *supra* note 55, at 273 (noting the Convention mandates nations to enact specific procedural provisions, but provides no guidance on how to draft or enact them).

127. *See* Explanatory Memorandum, *supra* note 1, at ¶¶ 145-48 (recognizing the Convention applies to parties of many different legal regimes and cultures in requiring parties to implement their own procedures to adhere to those differences); *supra* notes 36, 37 and accompanying text (describing differences in speech an privacy protections in the U.S. as compared to Europe).

128. *See generally* Convention, *supra* note 27, at Ch. 2.

129. *See* Baron, *supra* note 55 (declaring the Convention should encompass human rights standards included in other CoE Treaties); *see also generally* Convention, *supra* note 27.

130. *See Freedom v. Rules Bring Cybercrime Convention Clashes*, REUTERS, Mar. 6, 2001, *at* http://www.cyberrights.org/cybercrime (discussing critic's complaints that the Convention lacks balance and gives too much power to the law enforcement community at the expense of civil liberties); *see also* Baron, *supra* note 55, at 274 (criticizing the Convention for not clearly articulating which privacy rights it includes).

131. *See, e.g.*, Explanatory Memorandum, *supra* note 1, at ¶ 143.

the Convention allows parties to limit certain procedures through reservation to enable broader applications of powers and procedures for collection of real-time and traffic data.[132]

Another conflict arises when a requested party's domestic laws permit the requesting party to gather more information from the requested party than the requesting party's own laws would permit.[133] A dilemma exists over whether or not the requested party should supply only as much information as the requesting party is willing to provide.[134] A third conflict arises because parties can decide whether or not to require notice before permitting a search rather than require such notice by law.[135] Moreover, the Convention allows party's to individually determine the degree of severity required before they require interception or collection of content data.[136] These procedures, however, could be crucial in investigating criminal offenses.[137] Nevertheless, in recognizing the sensitivities surrounding the collection of data, the Convention permits the states themselves to determine the scope of these procedures.[138]

Additionally, the Convention does not address payment of costs associated with data interception, storage and surveillance.[139] Conceivably, such costs could be enormous and impose significant burdens on those required to comply.[140] Critics believe that this could place a heavy burden on service providers to retain data and perform additional record-keeping functions.[141] Furthermore, this provision may inundate ISPs with data requests from law enforcement, thereby disrupting core business operations.[142] The Convention

---

132. *See* Explanatory Memorandum, *supra* note 1, at ¶ 143.

133. *See* Banisar & Hosein, *supra* note 91 (expressing concern where one party's laws permit greater investigative authority than another's).

134. *See* Banisar & Hosein, *supra* note 91, at Art. 24 (advocating that a requested party must comply with the legal regime of the requesting party).

135. *See* Explanatory Memorandum, *supra* note 1, at ¶ 204 (recognizing that some countries consider notification of a search essential when distinguishing between searches of stored data and interception of flowing data).

136. *See* Explanatory Memorandum, *supra* note 1, at ¶ 214 (noting that some countries may not consider certain offenses serious enough to permit interception of content data or the collection of traffic data).

137. *See* Sussman, *supra* note 40 and accompanying text (explaining certain procedures are critical because the source of the intrusion must be detected quickly).

138. *See* Explanatory Memorandum, *supra* note 1, at ¶ 214 (remaining sensitive to the domestic nation's law by leaving the scope of certain investigative procedures up to the individual states); Convention, *supra* note 27 at Ch. 2.

139. *See* Tinabeth Burton, *Global Internet Group Calls for Council of Europe to Extend Deadline of Draft Convention on Cyber Crime*, Global Internet Group, Nov. 7, 2000, *at* http://www.gip.org/publications/papers/11-17-00b.asp; Barry Steinhardt, *ACLU/EPIC Comments on CoE Cybercrime Convention*, PUBLIC INTEREST LAW NETWORK, July 7, 2001, *at* http://www.pili.org/lists/piln/archives/msg00777.html (finding it troublesome that the Convention does not require countries requesting information to pay the costs imposed on third parties).

140. *See* Steinhardt, *supra* note 139 and accompanying text.

141. *See* Steinhardt, *supra* note 139 and accompanying text.

142. *See* Godwin, *supra* 98 (expressing concerns over the potential burden on ISPs posed by the Convention's data retention and storage requirements).

should include a provision to apportion payment of investigative costs.[143]

Furthermore, the Convention also requires that each signatory provide for conditions and safeguards to balance investigative procedures with the need to protect human rights, but does not articulate those safeguards.[144] The Convention does not clearly define those safeguards or require that signatories harmonize these safeguards with other international instruments, such as the United Nations Convention on Civil Rights.[145] Even if the Convention required harmonization, existing directives such as the European Convention for the Protection of Human Rights and Fundamental Freedoms are outdated.[146] For example, the United Nations Convention on Civil Rights, adopted in 1950, does not adequately respond to communication privacy issues in the digital age.[147] Although countries currently have different procedures to investigate crimes, and admittedly will continue to after parties ratify the Convention, unless lawmakers harmonize these procedures, they will find it difficult to achieve the Convention's goals.[148]

D. Jurisdiction

The Internet has changed the way law enforcement is able to prosecute crimes due to the lack of geographical boundaries.[149] Jurisdictional issues are as critical as the substantive law itself because countries must share information quickly before it disappears.[150] The Convention drafters included broad jurisdictional provisions to provide flexibility for states to decide jurisdictional issues in the event of a dispute.[151] Investigators would lose valuable time

143. *See* Godwin, *supra* 98.

144. *See* Convention, *supra* note 27, at Ch. 2, Art. 15 (requiring each party to ensure that "the establishment, implementation and application of the powers and procedures provided for . . . are subject to conditions and safeguards . . which provide for the adequate protection of human rights and liberties . . . ."); *but see* Yaman Akdeniz, *Anonymity, Democracy, and Cyberspace; Part V: Democratic Process and Nonpublic Politics*, 69 SOCIAL RESEARCH 223 (2002) (articulating that the Convention seems incompatible with the European Convention on Human Rights and Fundamental Freedoms and its safeguards and conditions "are not clearly defined").

145. *See* Akdeniz, *supra* note 144 (noting that the Convention requires signatories to consider other human rights instruments but does not require that they harmonize procedures with those instruments).

146. *See supra* note 14 and accompanying text (asserting existing laws are outdated).

147. *See CDT Comments*, *supra* note 91 (advocating updating existing cyber crime statutes).

148. *See* Steinhardt, *supra* note 139 (criticizing the Convention for vagueness because the procedural provisions are "unlikely to create any significant procedural protections"); *U.N. Manual*, *supra* note 1, at ¶ 7 (articulating one of the problems in combating cyber crimes is the lack of harmonization between different countries procedural laws); *Civil Liberties Groups Slam European Union*, CLUEBOT.COM, Oct.18, 2000, *at* http://www.cluebot.com/articles/00/10/17/1622228.shtml (stating now is the time to harmonize the inconsistent procedures amongst nations); Lawrence D. Casiraya, *Falling Behind Internet Security*, BUSINESSWORLD, Oct. 1, 2002 (acknowledging that some states have already adopted "uniform" anti-cybercrime policies and coordinated law enforcement efforts).

149. *See supra* note 13 and accompanying text (discussing the borderless nature of the Internet).

150. *See* Sussman, *supra* note 40, at 468 (stressing the need to share information quickly in conducting international computer crime investigations).

151. *See* Convention, *supra* note 27, at Ch. 2, Art. 22(5) (allowing the parties to determine the most

needed to gather information and identify the perpetrator if the Convention required law enforcement to obtain a search warrant from each jurisdiction through which an electronic signal passes.[152]

Under traditional common law jurisprudence, a court may exercise jurisdiction if it has both the authority over the area of law in controversy (e.g. subject matter jurisdiction) and personal jurisdiction over the defendant.[153] The Convention requires states to adopt legislation establishing jurisdiction over offenses committed within its territory, on board a ship flying that state's flag, on board an aircraft registered under the laws of that state or by one of its nationals if punishable by criminal law where committed.[154] In addition, the Convention requires that parties declining to extradite a national have laws in place to enable investigation and prosecution of that individual domestically.[155] Lastly, the Convention requires the parties to a jurisdictional dispute to determine amongst themselves the most appropriate forum.[156]

As drafted, the Convention does not contain a mechanism to deal with conflicts in jurisdiction, further supporting the necessity of clear jurisdictional guidelines.[157] For example, in a recent case, jurisdiction issues existed where a company incorporated in Vanuatu, operated its business from Australia, maintained its computer server in Denmark, maintained its source code in Estonia and the original developers resided in the Netherlands.[158] In that situation, the court had to determine whether jurisdiction was properly in the home state, in each state through which the Internet traffic traveled or where the harm occurred.[159]

A possible solution would establish a priority of jurisdiction.[160] For example, the Convention could establish a hierarchy where the nation that incurred the harm has jurisdictional priority over the nation where the crime was initiated.[161] As discussed, without clear jurisdictional guidelines in place, the Convention may yield unwieldy conflicts and inconsistent decisions.[162]

---

appropriate forum to prosecute a claim).

152. *See* Sussman, *supra* note 40, at 468.

153. *See* Pennoyer v. Neff, 95 U.S. 714 (1877); Int'l Shoe v. Washington, 326 U.S. 310 (1945).

154. *See* Convention, *supra* note 27, at Art. 22(1).

155. *See* Convention, *supra* note 27, at Art. 22(3).

156. *See* Convention, *supra* note 27, at Art. 22(5).

157. *See U.N. Manual*, *supra* note 1, at ¶¶ 245-47 (noting that where crimes involve multinational contact, conflicts of jurisdiction are sure to arise); *supra* note 13 and accompanying text (observing that these situations are more likely given the borderless Internet).

158. *See* Leiber v. Consumer Empowerment BV, No. 01-09923-SVW (C.D. Cal. 2003) (on file with the clerk of court) (discussing international Internet jurisdiction issues).

159. *Id.*

160. *See U.N. Manual*, *supra* note 1, at ¶ 254 (stressing that an international convention should establish an explicit priority of jurisdictional criteria).

161. *See U.N. Manual*, *supra* note 1, at ¶ 254.

162. *See U.N. Manual*, *supra* note 1, at ¶¶ 242-44.

E. Countries Must Cooperate to Successfully Combat Cyber Crime

The Convention requires signatories to provide mutual assistance to one another in cooperating with criminal investigations "to the widest extent possible."[163] The drafters recognized the need for a mechanism allowing law enforcement to investigate offenses and obtain evidence quickly and efficiently, while remaining cognizant of each nation's sovereignty and constitutional and human rights.[164]

As drafted, the Convention does not require "dual criminality" as a condition for mutual assistance consistently throughout the treaty.[165] Dual criminality exists if the offense is a crime under both the requestor and requesting party's laws.[166] If countries do not agree on what elements constitute a given crime, the perpetrator may go unpunished.[167] For example, if Country A requires elements one through four to constitute a given crime but Country B only requires elements one through three, Company A may not receive cooperation from Company B and a perpetrator who commits element number four may go free in Country B.[168] Critics expressed similar concerns because they believe a country does not have the right to interfere with the privacy of another country's citizens or impose "onerous requirements" to investigate crimes.[169]

Furthermore, the Convention does not require that parties implement investigative restraints to prohibit the requested party from using techniques or procedures that go beyond the power of the requesting party.[170] The language, as drafted, does not provide specific guidelines limiting a party's ability to avoid assisting in an investigation.[171] Opponents believe that signatories might use this open-ended language to justify a refusal to cooperate with crime investigations.[172] If countries refuse to cooperate, law enforcement may resort

---

163. *See generally* Convention, *supra* note 27, at Ch. 3, Art. 23-28.

164. *See* Commission of the European Communities, *Communication From the Commission to The Council, The European Parliament, The Economic and Social Committee and The Committee of the Regions*, eEurope, at 22 (2002) (recognizing the need for a mechanism allowing countries to investigate offense quickly and efficiently).

165. *See* Convention, *supra* note 27, at Ch. 3 (discussing provision for mutual assistance).

166. *See* ELECTRONIC FRONTIER, *supra* note 5, at 39 (expressing concern that lack of dual criminality could stymie the ability to solve crimes and prohibit extradition). "Because Internet access is available in over 200 countries, and because criminals can route their communications through any of these countries, law enforcement challenges must be addressed on as broad a basis as possible." ELECTRONIC FRONTIER, *supra* note 5, at 40.

167. *See U.N. Manual*, *supra* note 1, at ¶ 269 (recognizing the need for dual criminality amongst states); *see also, e.g.*, *supra* note 76 and accompanying text (noting that because Philippines' law did not require dual criminality, the creator of the ILOVEYOU virus went unpunished).

168. *See, e.g.*, Banisar & Hosein, *supra* note 91 (recommending extradition only apply where there is dual criminality citing it as a "key component" of the Convention).

169. *See* Steinhardt, *supra* note 139 (advocating the need for dual criminality to support the mutual cooperation provisions of the Convention).

170. *See* Convention, *supra* note 27, at Ch. 3 (discussing provisions for mutual assistance).

171. *See, e.g.*, Convention, *supra* note 27, at Ch. 3.

172. *See* Banisar & Hosein, *supra* note 91 (expressing concern that one party's laws will permit more protection than another's).

to methods of self-help and take matters into their own hands.[173]

For example, a federal court recently sentenced a Russian hacker, Vasiliy Gorshbikov to thirty-six months in prison for crimes resulting from illegal hacking.[174] Gorshbikov committed numerous computer crimes as well as fraud against various service providers, on-line banks and e-commerce networks in the United States.[175] In an undercover investigation to stop the hackers, the F.B.I. tricked Gorshbikov, and his accomplice Ivanov into entering U.S. territory.[176] The FBI used information obtained from Gorshbikov and Ivanov to hack into their computers located in Russia.[177] The FBI then copied data from their accounts, pursuant to a warrant issued by a U.S. Magistrate Judge and obtained sufficient evidence to convict the hackers.[178]

Lastly, Article twenty-seven of the Convention specifically allows a party to refuse extradition under certain circumstances, such as crimes constituting political offenses or those that may prejudice a nation's interests.[179] The provision, however, does not clarify what types of offenses qualify as "political" in nature or which they will consider prejudicial.[180] As seen in *Yahoo*, this provision, as written, will quickly run afoul simply from different interpretations of what constitutes a political offense.[181] Thus, the Convention needs to provide more detailed guidance as to what types of political offenses or prejudices will legitimately justify a refusal to cooperate and who will render that decision.[182] The Convention should also either provide additional guidance to signatories or set the standards itself to ensure timely and efficient criminal investigations through international cooperation.

---

173. *See infra* note 176 and accompanying text (discussing that the FBI resorted to self-help techniques through illegal hacking to gather evidence).

174. *See* Press Release, U.S. Dep't of Justice, Russian Computer Hacker Sentenced to Three Years in Prison, Oct. 4, 2002 (on file with author); *see also* Revelation Loa-Ash, *supra* note 9 (defining hacking).

175. *See* Russian Computer Hacker Sentenced to Three Years in Prison, *supra* note 174.

176. *See* Russian Computer Hacker Sentenced to Three Years in Prison, *supra* note 174. As part of an undercover operation, the F.B.I. set up a fake company called "Invita," posed as Invita personnel and communicated to Gorbishikov and Ivanov through e-mail and telephone. *See* Russian Computer Hacker Sentenced to Three Years in Prison, *supra* note 174. The two Russian suspects agreed to meet with the Invita executives (a.k.a. FBI agents) face-to-face in Seattle, WA. *Id.* Prior to the meeting, the FBI created a false computer network for the men to hack into, which they did successfully during the meeting. *Id.* The FBI also audio and videotaped the meeting, getting Gorbishikov bragging about various incidents where he hacked into other computers. *Id.*

177. *See* Russian Computer Hacker Sentenced to Three Years in Prison, *supra* note 174.

178. *See* Russian Computer Hacker Sentenced to Three Years in Prison, *supra* note 174.

179. *See* Convention, *supra* note 27, at Art. 27(4)(a) (allowing parties to refuse to extradite nationals if "the request concerns an offence, which the requested Party considers a political offence or an offence connected with a political offence, or it considers that execution of the request is likely to prejudice its sovereignty, security order public or other essential interests.").

180. Convention, *supra* note 27, at Art. 27(4)(a).

181. *See supra* notes 111-112 and accompanying text (discussing the *Yahoo* debacle).

182. *See* Steinhardt, *supra* note 139 (requiring the CoE to "explain with much greater specificity the situations and scenarios where parties are permitted to use the articulated reservations of political offenses and prejudicing . . .").

VI. CONCLUSION

The Convention is a welcome and long-overdue start towards addressing the exigent circumstances evolving from the Internet revolution. The CoE deserves much credit in accepting such a significant and valuable task. Computer crimes are difficult to solve due to the absence of geographical borders and the inherent ability to swiftly transfer and manipulate information instantly. Nevertheless, technological advances will continue to challenge law enforcement officials. As long as long signatories are permitted to codify cyber criminal laws domestically and countries remain unsubscribed to the Convention, authorities may be unable to obtain sufficient evidence to prosecute crimes.

We must reach a global consensus to harmonize not only the crimes themselves but also the investigative and prosecutorial procedures that will enable law enforcement to prevent and convict cyber crimes. Success will hinge upon the cooperation of all countries, both parties to the Convention and those that are not.[183]

Shannon L. Hopkins

183. *See* Godwin, *supra* note 98 (declaring that the Convention will not serve its purpose unless all countries are willing to adopt it); Gareth Morgan, *International Assault on Cybercrime Closer*, PC WORLD (United Kingdom), Dec. 11, 2001, *at* http://www.pcw.co.uk/News/1126786 (stating the key to the Convention's success is persuading countries to sign).

THIS PAGE INTENTIONALLY LEFT BLANK