1-1-2004

Cybercrime: National, Transnational, or International?

Ellen S. Podgor
Georgia State University College of Law

CYBERCRIME: NATIONAL, TRANSNATIONAL, OR INTERNATIONAL?

ELLEN S. PODGOR[†]

Table of Contents

I. INTRODUCTION

Determining which country has jurisdiction for purposes of a criminal prosecution may establish whether conduct will be a crime, how the crime will be defined, and how it will punished.[1] Issues of jurisdiction are particularly problematic in the context of cybercrime as the crime itself has unique extraterritorial qualities.[2] The interconnected nature of the global networks allows criminal acts in one country to pass easily into another country. As stated by Former Attorney General Janet Reno, "a hacker needs no passport and passes no checkpoints."[3]

[†]Professor of Law, Georgia State University College of Law.

This piece is dedicated to the late Edward M. Wise, who was an incredible mentor to me in the writing of our book, INTERNATIONAL CRIMINAL LAW: CASES AND MATERIALS (2000). The author thanks Professor Roger Clark for his comments on a draft of this article, and thanks Professor Peter Henning for organizing this wonderful conference.

1. *See* Ellen S. Podgor, *Cybercrime-Cyberterrorism*, 19 NOUVELLES ÉTUDES PÉNALE (2003).

2. *See generally* Ellen S. Podgor, *International Computer Fraud: A Paradigm for Limiting National Jurisdiction*, 35 U.C. DAVIS L. REV. 267 (2002).

3. U.S. Attorney General Janet Reno, Keynote Address at the Meeting of the P-8 Senior Experts' Group on Transnational Organized Crime, discussing High-tech and Computer Crime, at 5 (Jan. 21, 1997). The same metaphor was also used in a report of one of the Presidents working groups. *See* THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET, A REPORT OF THE PRESIDENT'S WORKING GROUP ON

Professor Edward M. Wise warned of countries becoming "computer crime havens."[4] He stated that "it seems futile to have laws restricting use of certain kinds of information if their provisions can be circumvented simply by moving the information to a jurisdiction with more lenient rules."[5] Since the writing of this article, countries throughout the world have passed laws to punish computer crimes. What now remains to be determined is whether the criminality is best approached in the national, transnational, or international sphere.

This essay looks at cybercrime jurisdiction in an attempt to determine if there is an appropriate forum for its prosecution.[6] It examines the unique aspects of cybercrime that make the jurisdiction question *sui generis*.[7] It then looks to various ways to approach cybercrime, namely from a national, transnational, or international perspective.[8] Finally it examines Article 22, the Jurisdiction Section, of the Council of Europe's Cybercrime Convention noting deficiencies in the approach taken in this document.[9] This essay advocates formulating clear rules of cybercrime jurisdiction.

II. THE PROBLEM

Worms, viruses, and other forms of cybercrime have caused significant worldwide damage. Individuals have caused havoc in the online world with viruses such as "I Love You," "Melissa, " "Nimda," "Code Red," "Sircam,"

UNLAWFUL CONDUCT ON THE INTERNET 22 (Mar. 2000), *available at* http://www.usdoj.gov (accessed by selecting Search on the top right and entering the terms "President's Working Group on Unlawful Conduct on the Internet") (last visited Mar. 16, 2004).

4. *See* Edward M. Wise, *Computer Crimes and Other Crimes Against Information Technology in the United States*, 64 INT'L REV. OF PENAL LAW 647, 668-69 (1993).

5. *Id.* at 668.

6. Others have examined jurisdiction issues in cyberspace with varying results. *See, e.g.*, Paul Schiff Berman, *The Globalization of Jurisdiction*, 151 U. PA. L. REV. 311 (2002) (discussing Internet jurisdiction); Bruce P. Keller, *The Game's the Same: Why Gambling in Cyberspace Violates Federal Law*, 108 YALE L.J. 1569 (1999); Darrel Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 MICH. TELECOMM. & TECH. L. REV. 69 (1998), *available at* http://www.mttlr.org (accessed by selecting Archive on the top left of homepage, then by selecting "Volume 4," and finally by selecting Jurisdiction in Cyberspace: Theory of International Spaces.) (last visited Mar. 16, 2004) (discussing use of international space law as jurisdiction base in cyberspace); Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet?*, 50 FED. COMM. L.J. 117 (1997) (discussing the regulation of cyberspace by states).

7. *See generally* Podgor, *supra* note 1.

8. *See infra* notes 25-40 and accompanying text.

9. *See infra* notes 41-50 and accompanying text.

"Klez Worm," "Blaster," and "SoBig."[10] Computer wrongdoing has resulted in billions of dollars of financial damage.[11] The ease with which computer criminality can occur also serves as an alert to the possible damage that can be caused if the next target becomes the critical infrastructure of a society.[12]

Cybercrime is not unique to the United States, as its pains have been felt worldwide. To meet this new challenge, various international initiatives have focused on curtailing cybercrime. At the forefront of these initiatives is the Council of Europe's Convention on Cybercrime. Additionally, there have been extensive discussions related to cybercrime in both the G-8[13] and the United Nations.[14] Think tanks in the United States have also produced reports related to cybercrime jurisdiction.[15]

---

10. *See, e.g.*, Jon Swartz, *Cops Take a Bite, or Maybe a Nibble, Out of Cybercrime; Despite Blaster Arrest, There's a Long Way to Go*, USA TODAY, Sept. 2, 2003, at B01 (describing the financial damage caused by various computer viruses and worms).

11. *See, e.g.*, Bria Murray, *Beware the Evils That Stalk Computers*, PITTS POST, Aug. 2, 2001, at A1 (discussing the damage caused by viruses and worms); *Bush Advisor: Cybercrime Costs us Billions*, REUTERS, Oct. 14, 2002, *available at* http://www.cnn.com /2002/TECH/biztech/10/14/crime.cyberspace.reut/index.html(last visited Jun. 2, 2004).

12. *Nunn Warns of Attacks from Techo-Terrorists*, ATL. J. CONST., Apr. 20, 1997, at G7. The Draft Action Plan on Cybercrime and Information Security for the Asia-Pacific region states, "[t]hreats to critical infrastructure and national interests arising from the use of the Internet for criminal activity are a growing concern." *Draft Action Plan on Cybercrime and Information Security for the Asia-Pacific Region*, United Nations Economic and Social Commission for Asia and the Pacific (2002) *available at* http://www.unescap.org/icstd (accessed by selecting Resolutions/Strategy/Declarations/Action Plans on the left side of the homepage, then by selecting Cybercime Action Plan.doc under the Action Plan Leading) (last visited Mar. 16, 2004).

13. Computer Crime and Intellectual Property Section (CCIPS), INTERNATIONAL ASPECTS OF COMPUTER CRIME, Meeting of the Justice and Interior Members of The Eight, (Dec. 9-10, 1997) *available at* www.usdoj.gov (accessed by selecting Alphabetical List of Components then selecting Criminal Division, next selecting Computer Crime and Intellectual Property then selecting International Aspects of Computer Crime and finally selecting Meeting of the Justice and Interior Ministers of the Eight, which is item number six under subsection (in re table of contents) (last visited Mar. 16, 2004).

14. *See* INTERNATIONAL REVIEW OF CRIMINAL POLICY -UNITED NATIONS MANUAL ON THE PREVENTION AND CONTROL OF COMPUTER-RELATED CRIME, UNCJIN, 8th U.N. Congress, Nos. 43 & 44, at 4 (1999), *available at* http://www.uncjin.org (accessed by selecting Documents in the menu on the left side of the homepage and then selecting International Review of Criminal Policy pdf version under the subheading Publication Series, Journals and Newsletters) (last visited Mar. 17, 2004).

15. A report, "*A Proposal for an International Convention on Cybercrime and Terrorism*" by the Hoover Institution, The Consortium for Research on Information Security & Policy (CRISP) and the Center for International Security and Cooperation (CISAC). This report is also termed the Stanford Draft, as the conference was held at Stanford University. *See* Abraham D.

The cybercrime problem is exacerbated not only because of it being an international problem, but also because it presents unique problems to law enforcement. There are both substantive and procedural issues that make this criminality different from the typical crimes encountered by police and prosecutors. At the forefront of the complexities of this crime is the fact that (1) there is no clear definition of what constitutes a cybercrime;[16] (2) cybercrimes come in a variety of different forms;[17] (3) there can be questions as to whether the criminality should be in the civil or criminal sphere;[18] (4) constitutional issues such as privacy and the First Amendment make this area problematic in resolving a uniform worldwide plan to combat this criminality;[19] (5) locating the perpetrators of the crime can be difficult as identities can be masked;[20] (6) there

---

Sofaer et. al., *A Proposal for an International Convention on Cybercrime and Terrorism* (Aug. 2000), *available at* http://www.iwar.org.uk/law/resources/cybercime/stanford/cisac.draft.htm. *See also* Erez Kalir & Elliot E. Maxwell, *Rethinking Boundaries in Cyberspace: A Report of the Aspen Institute Internet Policy Project*, THE ASPEN INST. 2002, *available at* http://www.aspeninst.org (accessed by selecting Bookstore in the menu on the left side of the homepage, then typing "Erez Kalir" in the Author blank and clicking Search, finally selecting Download as a Free PDF, to access this book online) (last visited Mar. 17, 2004).

16. *See* Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 934 (1996) (discussing how a computer can be "target of the offense," "tool of the offense," or "incidental to the offense"); Joe D. Whitley & William H. Jordan, *Computer Crime*, ABA WHITE COLLAR CRIME INSTITUTE 2000 at E-1 (describing how a computer crime can be the "object, subject, or instrument of a crime"). *See also* Podgor, *supra* note 2, at 273; Ellen S. Podgor, *Computer Crime*, ENCYCLOPEDIA OF CRIME & JUSTICE (2001); Richard W. Aldrich, *Cyberterrorism and Computer Crimes: Issues Surrounding the Establishment of an International Regime, INSS Ocassional Paper #32* at 11-30 (April 2000), *at* http://www.usafa.af.mil/inss (accessed from home page by selecting Publications then selecting Occasional Papers then selecting Occasional Paper #32) (last visited Feb. 25, 2004) (USAF Institute for National Security Studies, USAF Academy) (discussing various international definitions of computer crimes). Both the United Nations Manual on the Prevention and Control of Computer-Related Crime and the Council of Europe's Cybercrime Convention describe various acts of computer crimes without providing an explicit definition of what constitutes computer crime. *See* Aldrich, *supra* note 16, at 19.

17. An endless number of crimes can involve computers. For example, a computer can be used to commit identity theft, fraud, extortion, or piracy. In some cases the crimes are unique to the computer, as with illegal computer accessing where the perpetrator illegally enters another computer without permission. *See* Charney & Alexander, *supra* note 16, at 932-33. In other cases, the crimes are traditional crimes with a new medium, such as cyberstalking, cyberpornography, and cyberterrorism. *See* THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET, *supra* note 3, at 19-22.

18. Podgor, *supra* note 2, at 307-08.

19. *Id.* at 309-10.

20. *Id.* at 310-11. *See also* George du Pont, *The Criminalization of True Anonymity in Cyberspace*, 7 MICH. TELECOMM. & TECH. L. REV. 2001, at 196, *available at*

are limited tools available for "gathering, analyzing, securing, and storing" computer evidence;[21] (7) securing evidence and perpetrators from other countries can be procedurally challenging;[22] (8) the law controlling these forms of crimes can vary among countries;[23] (9) the activities can be conspiracies involving perpetrators from several different countries;[24] and (10) legal protections have moved slowly in comparison to the speed of the technology.[25]

As such, the cybercrime problem entails enormous economic losses and the potential for even greater non-economic consequences.[26] It is a problem with both national and international implications. Finally, the issues it raises for law enforcement exceed those presented in cases of traditional crime.

III. NATIONAL, TRANSNATIONAL, OR INTERNATIONAL

Although cybercrime clearly crosses borders, whether the criminality should be labeled national, transnational, or international is less certain. This dilemma is in part a function of whether cybercrime is approached in a "technologically neutral"[27] way or as a distinct form of criminality. If approached in a "technologically neutral" manner, as advocated by some scholars,[28] one merely looks to the underlying crime and determines jurisdiction based upon how jurisdiction would be approached if the crime did not involve a computer. Thus, if the crime were cyberpornography, then one would treat jurisdiction as one would treat the prosecution had this been a crime involving a hard copy of pornography.

This approach works well with rapes, robberies, and burglaries, as crimes

---

http://www.mttlr.org (accessed from homepage by selecting Archive, then selecting Volume 7) (last visited Feb. 25, 2004).

21. *See "Computer Forensic Tools" Introduced for War on Cybercrime*, 3 CYBERCRIME L. REP. 12 (Nov. 3, 2003) (discussing the European Commission's adoption of the "world's first set of 'computer forensic tools.'").

22. *See* Podgor, *supra* note 2, at 311-12.

23. *Id.* at 308-09.

24. *See Tokyo Police Arrest Brazilian Teen, Alleged Member of International Hacker Ring*, 3 CYBERCRIME L. REP. 13 (Nov. 17, 2003) (discussing how a juvenile collaborated with individuals in the United States, Brazil, and Portugal in "hacking into computer systems in as many as 1,032 government offices, public institutions, and private businesses in 33 countries.").

25. Although computer criminality existed prior to 1984, this was the year the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000), was enacted into law. Prosecutors had to use existing statutes prior to that date to proceed against activities involving computers. *See, e.g.*, 18 U.S.C. § 1343 (2000) (wire fraud statute).

26. Charney & Alexander, *supra* note 16, at 937.

27. Podgor, *supra* note 2, at 293.

28. Keller, *supra* note 6, at 1575.

committed without a computer usually occur in a set location. Territorial jurisdiction determines both the act and the resulting harm as the rape, robbery, or burglary, occurs where the perpetrator acts. This is not always the case, however, when the crime involves the use of the Internet. When the World Wide Web is a component of the criminal act, it can change the jurisdiction of the crime.

Using a classic approach to jurisdiction when the animal is cybercrime, can result in limitless jurisdiction. The act can occur where the perpetrator uses the keystroke, the location where the data initially passes, or the location where it may spread and cause damage. The resulting damage can provide a limitless number of jurisdictions that might never have been envisioned by the perpetrator of the crime. Thus, using a "technologically neutral" approach with cybercrime does not define the jurisdiction, but rather expands prosecutorial opportunities that may not exist with other forms of criminality. This expansion can result in jurisdictional conflicts, conflicts that only occur because of the involvement of a computer.

A more thoughtful approach to cybercrime, is to first determine if the activity is cybercrime.[29] Once designated as cyber activity, the conduct should be categorized among the many different forms of computer criminality. Using this approach would mean that jurisdiction for cyberterrorism would not be treated equivalent to jurisdiction for crimes involving cyberfraud. The cyber aspect would place it within a separate category and the specific form of cyber activity, whether it be terrorism or fraud, would then be used to determine the appropriate jurisdiction.

If this latter methodology is used, computer crimes as a whole cannot be designated as national, transnational, or international crime. Rather it would be necessary to consider the activity involved to determine where the specific type of cybercrime best belongs.

A. National

Although computer crime laws do not as of yet exist in all countries, and those countries with specific laws may have differing elements and focus, it is clear that computer crime laws have grown in national settings. For example, in the United States we find a clear recognition of computer criminality in the Computer Fraud and Abuse Act that criminalizes several different forms of

29. Podgor, *supra* note 1, at 2. Others have argued that cyberspace needs a distinct set of rules. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996), Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PA. L. REV. 1003 (2001).

computer conduct.[30] This statute prohibits activities such as computer espionage,[31] illegal access,[32] and interstate trafficking in passwords.[33] As a national crime, the jurisdiction defines the illegality, who prosecutes the crime, and who eventually punishes individuals who violate this national law.

National law, however, does not preclude a country from asserting international jurisdiction when it meets the extraterritorial allowances of the jurisdiction.[34] For example, computer crimes that occur within the United States can be acts of a perpetrator outside this country. Using the "objective territorial principle," an act that has effects within the United States can be subject to prosecution in this country.[35]

B. Transnational

Computer crimes are also listed as one of eighteen transnational crimes.[36] As stated by Professor Gerhard O.W. Mueller, the term "transnational crime" "did not have a juridical meaning" when initially used, and "does not have one now."[37] It is clear, however, that computer crimes, crimes that operate on the Internet, a worldwide network, can be crimes that "involve more than one country."[38]

Not all computer crimes are transnational in nature. Clearly individuals who engage in criminal acts on the World Wide Web, accessible to those throughout

---

30. 18 U.S.C. § 1030 (2000).

31. 18 U.S.C. § 1030(a)(1) (2000).

32. 18 U.S.C. § 1030(a)(2)(3)(4) (2000).

33. 18 U.S.C. § 1030(a)(6) (2000).

34. Likewise, transnational and international issues of extradition, luring, and production of evidence may surface despite the fact that the prosecution is premised upon a national statute. *See Bogus FBI Company Snares Russian Hackers; Indictments Follow in Connecticut, Washington, and California*, 1 CYBERCRIME L. REP. 7 (2001).

35. Objective territoriality includes "[a]cts done outside a jurisdiction, but intended to produce and producing detrimental effects within it." Strassheim v. Daily, 221 U.S. 280, 285 (1911). This principle is an extension of territoriality, one of five generally recognized bases of jurisdiction. Harvard Research in International Law, *Jurisdiction With Respect to Crime*, 29 AM. J. INT'L L. SUP 437 (1935).

36. Gerhard O.W. Mueller, *Transnational Crime: Definitions and Concepts*, *in* COMBATING TRANSNATIONAL CRIME 13 (Phil Williams & Dimitri Vlassis eds., 2001).

37. *Id.* at 13.

38. *Id.* at 14 (citing UNITED NATIONS, GENERAL ASSEMBLY *Fourth United Nations Survey of Crime Trends and Operations of Criminal Justice Systems*, A/CONF.169/15/ Add.1 (1995), *available at* http://www.uncjin.org (accessed by selecting Statistics, then United Nations Surveys of Crime Trends and Operations of Criminal Justice Systems, and then choosing Fourth Survey) (last visited Mar. 17, 2004).

the world, indicate the possibility of being involved in a transnational crime. Instances, however, of someone entering a specific computer for the purpose of retrieving confidential information from the hard drive does not rise to the level of a transnational crime. Thus, whether a national or transnational crime has been committed should not be dependant upon whether the crime fits within the computer crime rubric, but rather whether the specific conduct involves national or transnational activity. In the same vein, the line between transnational and international is not clear, as inter-state cooperation, such as treaties, may place the criminal activity in the transnational category. Absent cooperation however, the crime might be designed an international crime.

C. International

Computer crimes are clearly an "international concern."[39] A worm or virus placed by an individual in one country can travel to another country without the individual leaving home. Being an "international concern," however, does not automatically mean that the activity constitutes an international crime. Membership in the exclusive club of international crimes is limited.

Determining whether a crime is an "international crime" is a matter of scholarly debate. Professor Edward Wise stated that "[i]t is impossible to determine *a priori*, on the basis of its intrinsic characteristics, whether particular conduct constitutes an 'international crime' - just as it is not possible in domestic law to distinguish criminal from non-criminal conduct on the basis of the intrinsic qualitites of the conduct in question."[40] In delineating three types of international crimes he includes crimes that are "acts of private individuals which have been subjected to treaty prohibition because they involve international traffic or harm to a mutual or common interest of states requiring international cooperation for its effective suppression."[41] In contrast, Professor Cherif Bassiouni uses ten penal characteristics as a part of the process to determine if a crime is an

39. Professor Cherif Bassiouni notes that the "common denominator" between an international crime and international concern is "the preservation of certain interests which represent commonly shared values in the world." M. Cherif Bassiouni, *Introduction to Symposium on the Teaching of International Criminal Law*, 1 TOURO J. TRANSNAT'L L. 129, 130 (1988).

40. EDWARD M. WISE & ELLEN S. PODGOR, INTERNATIONAL CRIMINAL LAW: CASES AND MATERIALS 498-99 (2000).

41. Edward M. Wise, *International Crimes and Domestic Criminal Law*, 38 DEPAUL L. REV. 923, 937 (1989). *See also* Yoram Dinstein, *International Criminal Law*, 20 ISRAEL L. REV. 206, 221 (1985), *reprinted in* WISE & PODGOR, *supra* note 40, at 499 (stating that "[t]he practice of States is the conclusive determinant in the creation of international law (including international criminal law), and not the desirability of stamping our obnoxious patterns of human behavior.").

international crime.[42]

Irrespective of the approach taken to determine whether a crime should be designated an international crime, it is clear that some types of computer activity may rise to this level.[43] With the adoption of the Convention on Cybercrime of the Council of Europe and the possibility that computer crimes could damage the critical infrastructure of a nation, there are strong arguments that this form of criminality can rise into the category of being an "international crime." It is also apparent, however, that many specific types of computer crimes will never have the attributes comparable to crimes considered under the rubric of "international crimes."

D. Summary

Although the foregoing demonstrates that computer crimes as a group cannot be designated as national, transnational, or international, this does not mean that such designations should be ignored. Knowing the jurisdiction for particular categories of crimes can assist in promoting international cooperation and enforcement. Further, recognizing designations of jurisdiction avoids conflicts that can arise when one country trespasses on the jurisdiction of another nation.

---

42. Professor Ndiva Kofele-Kale synthesized these ten characteristics as:

> (1) [E]xplicit recognition of proscribed conduct as constituting an international crime, a crime under international law, or a crime; (2) implicit recognition of the penal nature of the act by establishing a duty to prohibit, prevent, prosecute and punish; (3) criminalization of the proscribed conduct; (4) duty or right to prosecute; (5) duty or right to punish the proscribed conduct; (6) duty or right to extradite; (7) duty or right to cooperate in prosecution, punishment (inclduing judicial assistance in penal proceedings); (8) establishment of a criminal jurisdictional basis (or theory of criminal jurisdiction or priority in criminal jurisdiction); (9) reference to the establishment of an international criminal court or international tribunal with penal characteristics (or prerogatives); and (10) elimination of the defense of superior orders.

Ndiva Kofele-Kale, *The Right to a Corruption-Free Society as an Individual and Collective Human Right: Elevating Official Corruption to a Crime Under International Law*, 34 INT'L L. 149 (2000) (citing from M. Cherif Bassiouni, *The Penal Characteristics of Conventional International Criminal Law*, 15 CASE W. RES. J. INT'L L. 27 (1983)).

43. Computer crimes are not directly listed as one of the four crimes covered by the Rome Statute for an International Criminal Court which includes the crimes of genocide, crimes against humanity, war crimes, and the crime of aggression. The Rome Statute for an International Criminal Court, Art. 5, *available at* http://www.un.org (accessed by selecting Welcome from the home page, then selecting International Law, next selecting International Criminal Court, and finally selecting Rome Statute of the International Criminal Court beneath the heading Documentation) (last visited Feb. 17, 2004). Arguably, certain forms of computer crimes could rise to a level of being one of the four crimes listed in the Rome Statute for an International Criminal Court.

Understood, however, is that in some instances jurisdiction will appropriately be in more than one sphere, with decisions being made on whether the international or transnational forum should have priority to prosecute the criminal conduct.

IV. ARTICLE 22 OF THE COUNCIL OF EUROPE'S CYBERCRIME CONVENTION

At the forefront of international documents focused on combating cybercrime is the Convention on Cybercrime of the Council of Europe. Its main objective, as noted in its summary statement is "to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation."[44] The Convention was opened for signature in Budapest on November 23, 2001 and entered into force on July 1, 2004.[45] The U.S. signed the Convention.[46]

Article 22 of the Convention is titled "Jurisdiction." This section, divided into five parts, provides the language that guides who should prosecute cybercrime and how jurisdictional conflicts should be resolved.[47]

Part One instructs countries to adopt cybercrime laws when the offense is committed "in its territory," "on board a ship flying the flag of that Party" "on board an aircraft registered under the laws of that Party" and when the crime is "by one of its nationals, if the offense is punishable under criminal law where it is committed or if the offense is committed outside the territorial jurisdiction of any State."[48] It is clear that this section includes acceptance of both a territorial and nationality approach to jurisdiction.[49]

---

44. Convention on Cybercrime, Council of Europe, *available at* http://conventions. coe.int (accessed by first selecting Full list under the heading Council of Europe Treaties on the home page, then selecting Convention on Cybercrime on the Full List page, and finally selecting Summary under the heading, What do you want to know about this treaty?, on the Convention on Cybercrime page) (last visited Feb. 17, 2004).

45. Department of Justice, *available at* http://www.usdoj.gov (accessed by selecting Organization Chart under the heading About DOJ on the home page, then selecting Criminal Division from the Organization Chart page, next selecting Computer Crime and Intellectual Property under the heading Topics of Special Interest on the Criminal Division page, and finally selecting International Aspects of Computer Crime under the heading Other Cybercrime Legal and Policy Issues) (last visited Feb. 17, 2004).

46. *Id.*

47. Convention on Cybercrime, Council of Europe, *supra* note 44.

48. *See* Explanatory Report to the Convention on Cybercrime, *available at* http://conventions.coe.int (accessed by first selecting Full list under the heading Council of Europe Treaties on the home page, then selecting Convention on Cybercrime on the Full List page, and finally selecting Explanatory Reports under the heading What do you want to know about this treaty? on the Convention on Cybercrime page) (last visited Feb. 17, 2004).

49. *Id.*

Part Two permits countries the right, through reservation, to disregard any of these bases of jurisdiction.[50] This Part expands or limits jurisdiction at the prerogative of the specific country.

If there is a refusal to extradite premised upon the nationality of the offender, Part Three requires the country to have the legal authority to proceed with a prosecution. Thus countries choosing to avoid extradition of a national are left to prosecute that individual within their own country.

Part Four of the Convention expands the jurisdiction base in that it provides that "[t]his Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law."[51] It is this last Part that makes jurisdiction limitless.[52]

Finally, Part Five, aimed at resolving conflict of law questions, provides that "when more than one Party claims jurisdiction over an alleged offense established in accordance with this Convention, the parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."[53] This final Part of the jurisdiction section of the Convention does not mandate that the parties resolve questions of jurisdiction.[54]

Although clearly Article 22 exudes international cooperation, it also fails to provide any clear lines of who will have jurisdiction to prosecute a computer crime. This is particularly true for the United States, a country that uses an objective territorial approach[55] to jurisdiction, an approach that permits prosecution when the conduct has an "effect" in the United States.[56] Because of the interconnected nature of networks, computer crimes are very likely to have some effect in this country. Thus, by including a section that incorporates the criminal jurisdiction used in domestic law, the document allows the United States to have nearly unlimited jurisdiction to prosecute computer crimes.[57] After all, it will be rare that a computer virus or worm put into the World Wide Web does not have an effect on the United States.

---

50. The explanatory text notes that no reservation is permitted for territorial jurisdiction or for "cases falling under the principle of 'aut dedere aut judicare' (extradite or prosecute)." *Id.* at ¶ 237.

51. *Id.*

52. *Id.*

53. *See id.* at ¶ 239.

54. *Id.*

55. *See supra* text accompanying note 35.

56. *See* Ellen S. Podgor, *"Defensive Territoriality": A New Paradigm for the Prosecution of Extraterritorial Business Crimes*, 31 GA. J. INT'L & COMP. L. 1, 5-14 (2002) (discussing the use of the effects test with extraterritorial business crimes).

57. Arguably it can be said that jurisdiction is limited by the Restatement. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 403 (1986).

Equally ineffective in resolving jurisdiction issues is the conflict provision that provides no guidance to countries who seek to resolve which jurisdiction is the most appropriate for prosecution. Obviously possession of the defendant, possession of the evidence, and sufficient national laws may play a factor in resolving these jurisdiction conflicts. But leaving these issues for an after-the-fact resolution by countries again raises concerns of whether a jurisdiction plan is truly provided by this Convention.

Although there is criticism placed here on the failure to confine computer jurisdiction to a formulaic approach that predetermines conflicts among jurisdictions, there is also a recognition of the beneficial qualities of having countries adopt laws that will increase the ability to curtail computer criminality. The document's recognition of computer criminality as a problem, and emphasis on having new laws enacted to curtail this activity, is a recognition that this international concern merits international cooperation.

V. CONCLUSION

As technology continues to develop at speeds that exceed the legal regimes, it is important to at least determine who will be responsible for defining and punishing acts of computer illegality. It is necessary to dissect computer crimes and decide the appropriate jurisdiction lodging for each of the subcategories within cybercrime. Some will fall into national jurisdiction, others to transnational, and others might be designed "international crimes." In cases where jurisdiction appropriately falls into more than one of these categories, clear priorities need to be established. Computer crime jurisdiction will remain vague until such time as there is a clear recognition that this form of criminality differs from traditional crimes and until such time as it is realized that computer crimes come in many different forms.