THE COUNCIL OF EUROPE'S CONVENTION ON CYBERCRIME

By Amalie M. Weber

Cybercrime legislation is plagued by a lack of geographically based jurisdictional boundaries.[1] As Professor James Boyle noted, "If the king's writ reaches only as far as the king's sword, then much of the content on the Internet might be presumed to be free from the regulation of any particular sovereign."[2] This observation is particularly apt in the criminal enforcement context. It is impossible to regulate criminal behavior without a means to ensure enforcement of sanctions. The Council of Europe's Convention on Cybercrime (the "Convention" or "treaty") seeks to extend the ambit of the king's sword through cooperation.

This paper evaluates the potential efficacy of the Convention's treatment of the jurisdictional conflicts underlying cybercrime regulation. First, the paper will illustrate the international jurisdiction problems that prompted the search for a solution requiring an international instrument. It will then present a brief history of how the Council of Europe positioned itself to undertake the jurisdictional challenge these situations presented. The paper also summarizes the major portions of the treaty, and evaluates the treaty's potential impact on United States domestic law. Finally, it will critically appraise the general shortcomings of the Convention and suggest possible alternatives. This paper concludes that the Convention, while flawed, is the best available solution to the jurisdictional dilemma of cybercrime.

I. THE HISTORY OF THE TREATY

The Council of Europe's Convention on Cybercrime was created to address the jurisdictional issues posed by the evolution of the Internet. Its solution was to harmonize cybercrime laws and assure the existence of procedural mechanisms to assist in the successful prosecution of cyber

1. *See generally* David R. Johnson & David G. Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996) (arguing that cyberspace cannot be governed by laws that rely on traditional territorial borders).

2. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 179 (1997). *See id. at* 178 (identifying three main difficulties states have encountered in attempting to regulate cyberspace).

criminals.[3] This section provides a description of the core problems encountered in the attempted prosecutions of international cyber criminals as well as a history of the development of the treaty, to better explain the evolution of the Convention and some of its criticisms.

A. The Problem of Cybercrime Jurisdiction

The jurisdictional problem of cybercrime manifests itself in three ways: lack of criminal statutes; lack of procedural powers; and lack of enforceable mutual assistance provisions with foreign states. Because international cooperation on cybercrime has traditionally been the exception rather than the rule, these requirements are frequently an insurmountable barrier to the successful prosecution of cyber criminals. The following examples illustrate how these problems thwart criminal prosecutions.

1. Lack of Criminal Statues

Many states have yet to enact statutes criminalizing computer misuse offenses.[4] In May of 2000, the "I love you" virus infected forty-five million computers around the world.[5] The virus, along with copycat viruses that emerged in its aftermath, is estimated to have cost between 6.7 and 10 billion dollars in lost productivity.[6] However the main suspect, Onel De-Guzman, remains unpunished despite having been identified and tracked to the Philippines, because the Philippines lacked an appropriate computer crime statute at the time of the attack.[7]

2. Lack of Procedural Powers

States often lack the resources and procedural tools necessary to conduct computer crime investigations. In October of 2002, a coordinated de-

3. *See Explanatory Report to the Convention on Cybercrime* ¶ 6, *available at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (last visited Aug. 29, 2002) [hereinafter *Explanatory Report to the Convention on Cybercrime*].

4. *Cyber Crime. . . and Punishment? Archaic Laws Threaten Global Information, McConnell International*, *available at* http://www.mcconnellinternational.com/services/CyberCrime.htm (Dec. 2000).

5. Jovi Tanada Yam, *Cybercrime Treaty Under Way*, BUSINESSWORLD, May 3, 2001, pg 9, *available at* LEXIS, News Group File.

6. *Id.* Patricia L. Bellia, *Chasing Bits Across Borders*, 2001 U. CHI. LEGAL F. 35, 36 n. 6 (2001) (citing *Love Bug, Damage Costs Rise to $6.7 Billion*, COMPUTER ECONOMICS EFLASH, May 9, 2000; Rob Kaiser, *'Love Bug' Has Cousins; They Bite Too: Cyberattack Considered Most Disruptive Ever*, CHI. TRIB. May 6, 2000, at 1).

7. *Internet Virus Named after Philippine President*, DEUTSCHE PRESSE-AGENTUR, Sept. 1, 2000, *available at* LEXIS, News Group File.

nial of service[8] attack occurred on central Internet root servers[9] around the world.[10] The incident puzzled law enforcement officials for weeks, raising fears that it was the work of an organized criminal group intending to disrupt vital communications networks.[11] In response to increasing numbers of such attacks, Europol[12] formed the High Tech Crime Centre to coordinate cross-border cybercrime investigations in Europe, and to bolster the response to these types of crimes.[13] Despite this Centre, experts feel that if such an attack were to target a European communications network, police would have a "very difficult time tracking down the culprits."[14] The High Tech Crime Centre continues to be under-manned and under-resourced.[15]

3. Lack of enforceable mutual assistance provisions

Even when both the host and victim states have adequate criminal statutes and investigative powers, prosecution is frustrated by a lack of enforceable cooperation. For example, during the spring of 2000, American banks and credit card businesses were serially attacked by international hackers who broke into secured files, extracted credit card numbers and merchant identification numbers, and then used this information to extort money from their victims in exchange for security "consulting services."[16] The extortion scheme caused enormous damages, and the targeted companies were unable to keep the hackers out of their systems.[17]

---

8. "Denial of service" attacks overwhelm networks with streams of high quantities of data until the networks fail. David McGuire & Brian Krebs, *Large Scale Attack Cripples Internet Backbone*, WASH POST, Oct. 23, 2002, at E05 *available at* LEXIS, News Group File.

9. Computers act as the backbone of the Internet. Seven of the thirteen servers that make up this backbone failed completely during the attack. Two others failed intermittently during the hour long attack. *Id.*

10. *Id.*

11. *Police Admit They Can't Keep Up with Cyber Criminals*, REUTERS (London), Nov. 1, 2002, *at* http://www.siliconvalley.com/mld/siliconvalley/news/editorial/4421571.htm [hereinafter *Police Admit*].

12. Europol is the European Police Office established by the Europol Convention to "improve the effectiveness of the competent authorities in the Member States and cooperation between them. Europol Convention: European Police Office *at* http://europa.eu.int/scadplus/leg/en/lvb/l14005b.htm (last visited Jan. 26, 2003).

13. *Police Admit*, *supra* note 11.

14. *Id.* (quoting Rolf Hegel, head of Europol's serious crime department, from an interview conducted shortly after the incident).

15. *Id.*

16. Monte Morin, *U.S. Indicts Russian Citizen in Hacking Case*, L.A. TIMES, June 21, 2000, at Part 2 page 2, *available at* LEXIS, News Group File.

17. *Id.*

However, when the FBI finally identified two suspects in Russia, Russian authorities refused to assist in the investigation.[18] Although the United States has approximately 40 mutual legal assistance treaties ("MLATs") to aid law enforcement in capturing data in foreign countries,[19] the Russian MLAT does not specify computer crimes as one of the crimes in which assistance is rendered.[20] Finally, in November 2000, without the support of Russian authorities, the FBI conducted a sting operation in which the two suspected Russian hackers were lured into the United States with false job offers.[21] During the staged interview, the FBI monitored the suspects' communications with their servers in Russia, obtained their passwords and login identification, and used this information to access and download files for use as evidence of their prior hacking and extortion activities against U.S. companies.[22] A major international debate continues over whether the United States had the authority to conduct a search of a private, protected server located outside the boundaries of the United States (a remote extraterritorial search) in order to obtain evidence required to indict these suspects.[23]

While the Philippines has now passed legislation criminalizing computer misuse[24] and Europol continues to support the High Tech Crime Centre,[25] such piecemeal efforts have only served to gradually relocate computer crime to states where enforcement efforts are less coordinated. A more comprehensive approach is needed.[26]

B. Development of the Treaty

The Council of Europe's Convention on Cybercrime was developed in response to a growing concern about the adequacy of legislation criminal-

---

18. Robert Lemos, *Lawyers slam FBI 'hack'*, ZD NET NEWS, May 1, 2001, *available at* 2001 WL 4732801.

19. ORIN S. KERR, U. S. DEPT. OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 33 2001 [hereinafter DOJ SEARCH AND SEIZURE MANUAL].

20. Lemos, *supra* note 18.

21. *Id.*

22. *Id.*

23. *See* Nathan Thornburgh, *2 Russian Hackers Nabbed in FBI Sting,* MOSCOW TIMES, Apr 28, 2001, *available at* LEXIS, News Group File.

24. DEUTSCHE PRESSE-AGENTUR, *supra* note 7.

25. *See Police admit, supra* note 11.

26. *See* Communique from Secretary General Janet Reno, to the Meeting of the Justice and Interior Ministers of The Eight (December 9-10, 1997) *available at* http://www.usdoj.gov/criminal/cybercrime/communique.htm; *see also* Michael A. Sussmann, *The Critical Challenges from International High-Tech and Computer Related Crime at the Millennium*, 9 DUKE J. COMP, & INT'L L. 451, 488 (1999).

izing certain activities occurring over computer networks.[27] In 1989, the Council of Europe published a set of recommendations addressing the need for new substantive laws criminalizing disruptive conduct committed through computer networks.[28] This was followed by a second study, published in 1995, addressing the inadequacy of computer-related, criminal procedural laws.[29] Building on these reports, the Council of Europe established a Committee of Experts on Crime in Cyberspace (PC-CY) in 1997 to draft a binding convention facilitating international cooperation in the investigation and prosecution of computer crimes.[30] The result is the Council of Europe's Convention on Cybercrime.[31]

The Convention on Cybercrime is a multilateral agreement geared at facilitating international cooperation in the prosecution of cyber criminals.[32] It is the first international treaty on crimes committed via the Internet and other computer networks, and is the product of four years of work.[33] In Budapest, on November 23, 2001,[34] the Council of Europe opened the treaty for signature by member states[35] and by nonmember states, including the United States, that participated in its development.[36]

---

27. Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime (Final Draft, released June 29, 2001), A2, *at* http://www.cybercrime.gov/newCOEFAQ's.html (last updated July 10, 2001).

28. *See* Recommendation No. R. (89) 9 Of the Committee of Ministers to Member States on Computer-related Crime, *available at* http://www.cm.coe.int/ta/rec/1989/89r9.htm (Sept. 13, 1989).

29. *See* Recommendation No. R. (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology, *available at* http://www.coe.int/ta/rec/1995/95r13htm (Sept. 11, 1995).

30. Frequently Asked Questions, *supra* note 27 at A2.

31. *See* Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185, *available at* http://conventions.coe.int/Treaty/en/cadreprincipal.htm [hereinafter Convention on Cybercrime]

32. Department of Justice web site, *at* http://www.usdoj.gov/criminal/cybercrime/intl.html (last visited November 18, 2002).

33. *See id.* (the Convention was signed in September of 2001); Frequently Asked Questions, *supra* note 27, at A2 (work on the Convention commenced in 1997).

34. Council of Europe Web site, *at* http://conventions.coe.int/treaty/en/cadreprincipal.htm (last visited November 18, 2002).

35. Member states include: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Russia, San Marino, Slovakia, Slovenia, Spain, Sweden, Switzerland, the former Yugoslav Republic, Turkey, Ukraine, and the United Kingdom. *Id.*

36. *Id.* (The non-member states are the United States, Canada, South Africa and Japan).

The treaty will enter into force upon ratification by five States, at least three of which must be member States of the Council of Europe.[37] As of December 2002, the treaty had thirty-three signatories and had been ratified by Albania and Croatia.[38] In order for the treaty to take effect in the United States, the Senate must ratify it.[39]

The structure of the treaty reflects an awareness of the jurisdictional dilemma. The Convention on Cybercrime's main objective, set out in the preamble, is to pursue a common criminal policy to protect society from cybercrime.[40] The Council's approach recognizes that accomplishment of this goal is predicated upon finding solutions to the lack of criminal statutes, the lack of procedural powers, and the lack of enforceable mutual assistance provisions that result from the jurisdictional gap in cybercrime regulation.[41] The Council's solution requires parties to adopt appropriate legislation against cybercrime, to ensure that their law enforcement officials have the requisite authority and procedural tools to effectively investigate and prosecute cybercrime offenses, and to provide international cooperation to other parties engaged in such efforts.[42]

II. STRUCTURE OF THE CONVENTION ON CYBERCRIME

The treaty consists of four chapters. Chapter I defines terms used by the treaty. Chapter II establishes a common cannon of computer-based and computer-related crimes, requires a common set of procedural powers, and loosely establishes a set of rules by which parties can assert jurisdiction. Chapter III sets up a framework for cooperation in the use of those powers. Chapter IV includes miscellaneous provisions common to most Coun-

---

37. *Id.*

38. *Id.*

39. *See* U.S. CONST. art. II. § 2 cl. 2. *See also* CONGRESSIONAL RESEARCH SERVICE OF THE LIBRARY OF CONGRESS, TREATIES AND OTHER INTERNATIONAL AGREEMENTS: THE ROLE OF THE UNITED STATES SENATE, S. PRT. 106-71, at 1, 19 (2001) [hereinafter TREATIES] (advising and consenting to a treaty requires a two thirds majority of the Senators present).

40. Convention on Cybercrime, *supra* note 31, at Preamble.

> Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge.

Explanatory Report to the Convention on Cybercrime, *supra* note 3, ¶ 6.

41. *See* Convention on Cybercrime, *supra* note 31, Preamble.

42. *Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 16.

cil of Europe treaties.[43] This section will focus on the substantive provisions located in Chapters II and III of the treaty.[44]

A. Offenses

The Convention on Cybercrime calls for the criminalization of nine offenses in four categories. The first category targets "[o]ffenses against the confidentiality, integrity and availability of computer data and systems."[45] These include: illegal access, illegal interception, data interference, system interference, and misuse of devices.[46] The second category, "[c]omputer-related offenses", includes provisions calling for the criminalization of computer-related forgery and computer-related fraud.[47] "Content-related offences" requires criminalizing offences related to child pornography.[48] This third category is ostensibly supplemented by a new protocol adopted November 7, 2002 making any dissemination of racist or xenophobic material through computer systems a criminal offense.[49] However, the new protocol is a separate legal instrument from the treaty, and parties agreeing to the treaty are not obliged adopt it.[50] The fourth category, "[o]ffenses related to infringements of copyright and related rights," criminalizes copyright violations.[51] This section of the Convention also includes ancillary provisions that require the establishment of laws against attempt and aiding or abetting in the aforementioned crimes, as well as the establishment of a standard for corporate liability.[52]

B. Procedural Powers and Jurisdiction

The Convention on Cybercrime addresses procedural legal issues. It requires states to establish a minimum set of procedural tools at the national level whereby the appropriate law enforcement authorities within a state have authority to conduct certain types of investigations specific to computer crime offenses. Such procedural powers include: expedited pres-

---

43. *Id.* at ¶ 303.

44. Chapter I is self-explanatory and the content of Chapter IV is an artifact of the Convention being drafted by the Council of Europe. *See id.*

45. Convention on Cybercrime, *supra* note 31, ch. II § 1 tit. 1, arts. 2-6.

46. *Id.*

47. *Id.* at ch. II § 1 tit. 2, arts. 7-8.

48. *Id.* at ch. II § 1 tit. 3, art. 9.

49. Press Release, Council of Europe, The Council of Europe fights against racism and xenophobia on the Internet (Nov. 11, 2002), *at* http://press.coe.int/cp/2002/554a (2002).htm.

50. Frequently Asked Questions *supra* note 27, at C3.

51. Convention on Cybercrime, *supra* note 31, ch. II § 1 tit. 4 art. 19.

52. *Id.* at ch. II § 1 tit. 5 arts. 20-21.

preservation of stored data,[53] expedited preservation and partial disclosure of traffic data,[54] production orders,[55] search and seizure of computer data,[56] real-time collection of traffic data[57] and interception of content data.[58]

The treaty also includes a provision granting a participating state jurisdiction over offenses committed within that state's territory.[59] This allows a state to assert jurisdiction in a computer crime involving a computer system within its territory, even if the perpetrator committed the offense from a remote location outside of the state.[60] Further, the Convention grants a state jurisdiction over a citizen of that state who commits a covered offense outside of the state's boundaries, so long as the offense is also punishable by criminal law in the jurisdiction where it was committed, or if the offence occurred outside of the territorial jurisdiction of any state.[61]

---

53. *Id.* at ch. II § 2 tit. 2 art. 16 (requiring that competent authorities are able to protect stored data from modification, deterioration, or deletion in a timely fashion pending approval of further investigation); *see also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶¶ 158-64.

54. Convention on Cybercrime, *supra* note 31, ch. II § 2 tit. 2 art. 17 (ensuring that where one or more service providers are involved in the relaying of an electronic communication, expeditious preservation of traffic data can be achieved); *see also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶¶ 165-69.

55. Convention on Cybercrime, *supra* note 31, ch. II § 2 tit. 3 art. 18 (providing an appropriate legal basis for the release of stored computer data or traffic data from third parties to competent authorities); s*ee also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶¶ 170-83.

56. Convention on Cybercrime, *supra* note 31, ch. II § 2 tit. 4 art. 19 (assuring that computer data is considered a tangible object which can be secured on behalf of a criminal investigation); *see also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶¶ 184-204.

57. Convention on Cybercrime, *supra* note 31, ch. II § 2 tit. 5 art. 20 (obliging Parties to ensure that their competent authorities have the power to compel a service provider to collect and record traffic data to the extent that such collection is within their existing technical capabilities); *see also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶¶ 216-27.

58. Convention on Cybercrime, *supra* note 31, ch. II § 2 tit. 5 art. 21 (obliging Parties to ensure that their competent authorities have the power to compel a service provider to collect and record content data to the extent that such collection is within their existing technical capabilities); *see also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶¶ 228-31.

59. Convention on Cybercrime, *supra* note 31, ch. II § 3 art. 22 (including when an offense is committed upon a ship flying the flag of that party or an aircraft registered under the laws of that party).

60. *Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 233.

61. *Id.*

Although the Convention tacitly permits some cross-border access to stored computer data without the need to request mutual assistance,[62] such investigations are only allowed when access to the data is publicly available (open source) or when the state conducting the search has obtained "the lawful and voluntary consent of the person who has the lawful authority to disclose the data."[63] The drafters of the Convention on Cybercrime explicitly deny that the treaty permits remote exterritorial searches.[64] They concluded, "it was not yet possible to prepare a comprehensive, legally binding regime regulating the area."[65] The failure to reach an agreement on remote extraterritorial searches was attributed to the Committee's lack of experience with such situations and the notion that the permissibility of unilateral assertions of power would turn on "the precise circumstances of the individual case, thereby making it difficult to formulate general rules."[66]

C. International Cooperation, Extradition and Mutual Assistance

The Convention on Cybercrime provides three general principles of international cooperation.[67] First, international cooperation will be provided among states "to the widest extent possible."[68] Second, the obligation to cooperate extends not only to the crimes established in the treaty, but also to the collection of electronic evidence whenever it relates to a criminal offense.[69] Third, the provisions for international cooperation do not supercede preexisting provisions of international agreements on these issues.[70] These general principles are reiterated by the mutual assistance provisions.[71] The extradition provisions also defer to preexisting treaties or alternative extradition arrangements between party states.[72]

---

62. *See* Convention on Cybercrime, *supra* note 31, ch. III § 2 tit. 2, art. 32.

63. *Id.*

64. *See Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶¶ 293-94.

65. *Id.* at ¶ 293.

66. *Id.*

67. Convention on Cybercrime, *supra* note 31, at ch. III § 2 tit. 1, art. 23.

68. *Id.*; *see also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 242.

69. Convention on Cybercrime, *supra* note 31, ch. III § 2 tit. 1, art. 23; *see also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 243.

70. Convention on Cybercrime, *supra* note 31, ch. III § 2 tit. 1, art. 23; *see also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 244.

71. Convention on Cybercrime, *supra* note 31, ch. III § 2 tit. 1, art. 25; *see also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 253.

72. Convention on Cybercrime, *supra* note 31, ch. III § 2 tit. 1, art. 24; *see also Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 246.

Concerted international investigations of computer-related offenses and electronic evidence are made possible by the specific mutual assistance provisions of the treaty.[73] Thus, they mirror the procedural powers that states are required to have at the national level. These specific mutual assistance provisions include expedited preservation of stored computer data,[74] expedited disclosure of preserved traffic data,[75] accessing stored computer data,[76] real time collection of traffic data,[77] and interception of content data.[78]

The treaty explicitly rejects dual criminality as a prerequisite for mutual assistance regarding the expedited preservation of stored computer data.[79] Dual criminality, in which two countries have overlapping statutes prohibiting the same criminal behavior, is an innovation widely lauded for its introduction of flexibility into the relatively cumbersome development of extradition treaties.[80] However, the treaty does contain an electable reservation allowing it to tolerate a dual criminality requirement.[81] The drafters of the treaty defend the rejection of the dual criminality requirement by arguing that expedited preservation is necessary to deal with the extenuated circumstances of computer-related crime.[82] There is an acute need for rapid responses and minimal bureaucracy because electronic evidence is so easily tampered with or destroyed.[83] Furthermore, there is ample opportunity to cure a breach of procedural standards after the data has been secured but before it has been turned over to requesting authorities.[84]

---

73. *Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 281.

74. Convention on Cybercrime, *supra* note 31, ch. III § 2 tit. 2, art. 29.

75. *Id.* at ch. III § 2 tit. 2, art. 30.

76. *Id.* at ch. III § 2 tit. 2, art. 31.

77. *Id.* at ch. III § 2 tit. 2, art. 33.

78. *Id.* at ch. III § 2 tit. 2, art. 34.

79. *See, e.g.*, *id.* at ch. III § 2 tit. 1 art. 29 ¶ 3 ("For the purposes of responding to [an expedited preservation of stored computer data] request, dual criminality shall not be required as a condition to providing such preservation.").

80. *See* TREATIES, *supra* note 39, at 279.

81. *See, e.g.*, Convention on Cybercrime, *supra* note 31, ch. III § 2 tit. 1 art. 29 ¶ 4 A party that requires dual criminality as a condition for responding to a request for mutual assistance for the search . . . seizure . . . or disclosures of stored data, may, in respect of offenses other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. *Id.*

82. *See Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 285.

83. *Id.*

84. *See id.*

III. THE NEGLIGIBLE IMPACT OF THE TREATY ON UNITED STATES DOMESTIC LAW

The U.S. Department of Justice does not anticipate that implementing legislation will be required for the United States to become a party to the Convention on Cybercrime.[85] There are several reasons for this supposition: (1) because the United States participated in its drafting, the treaty largely tracks existing U.S. law, (2) the treaty generally permits states to reserve provisions where existing cybercrime laws conflict between states, and (3) the treaty defers to pre-existing international agreements.[86]

A. The Convention Generally Tracks Current United States Law

The United States Departments of Justice, State, and Commerce, in close consultation with other U.S. government agencies, played a big role in the negotiations of both the plenary sessions and drafting of the treaty.[87] As a result, the central provisions of the Convention are consistent with the existing framework of U.S. law and procedures.[88] An exhaustive mapping of current U.S. law against the provisions of the Convention is beyond the scope of this paper, however, Table 1 summarizes the correlation between U.S. federal laws and the substantive offense provisions of the treaty. The table introduces general types of unlawful conduct to facilitate comparison between the Convention on Cybercrime and comparable U.S. federal statutes. As the table demonstrates, nearly every substantive offense created by the Convention on Cybercrime is already criminalized in some fashion under U.S. federal law. Article 11 of the treaty is not included in the table. This Article (Attempt and Aiding or Abetting) criminalizes intentional conduct aimed at aiding, abetting or attempting the offenses criminalized under Articles 2 through 10.[89]

Table 1[90]

Types of Unlawful Conduct	Convention on Cybercrime Treaty Provisions	Examples of Potentially Applicable Federal Laws

85. Frequently Asked Questions, *supra* note 27, at A7.

86. *Id.*

87. *Id.* at A3.

88. *See id.* at A7.

89. Articles 2-11 of the CoE's Convention on Cybercrime introduce the substantive criminal offenses mandated by the treaty. Convention on Cybercrime, *supra* note 31, ch. II, § 1, tit. 5, art. 11.

90. The table represents an adaptation of a table taken from the President's Working Group on Unlawful Conduct on the Internet. *The Electronic Frontier: The Challenge of Unlawful Conduct on the Internet*, at 18-19, *available at* http://www.cybercrime.gov/unlawful.pdf (Mar. 2000).

Computer Misuse	Art. 2 Illegal access Art. 3 Illegal interception Art. 4 Data interference Art. 5 System interference Art. 6 Misuse of devices	18 U.S.C. § 1030 (computer fraud and abuse act)
Internet Fraud	Art. 7 Computer-related forgery Art. 8 Computer-related fraud	15 U.S.C. §§ 45, 52 (unfair or deceptive acts or practices; false advertisements) 15 U.S.C. § 11644 (credit card fraud) 18 U.S.C. §§ 1028, 1029, 1030 (fraud connected with identification documents and information; fraud connected with access devices; fraud connected with computers) 18 U.S.C. §§ 1341 et seq. (mail, wire, and bank fraud) 18 U.S.C. § 1345 (injunctions against fraud) 18 U.S.C. §§ 1956, 1957 (money laundering)
Online Child Pornography, Child Luring, and Related Activities	Art. 9 Offenses related to child pornography	18 U.S.C. § 2251 et seq. (sexual exploitation and other child abuse) 18 U.S.C. § 2421 et seq. (transportation for illegal sexual activity)
Software Piracy and Intellectual Property Theft	Art. 10 Offenses related to infringements of copyright and related rights	17 U.S.C. § 506 (criminal copyright infringement) 17 U.S.C. § 1201 et seq. (copyright protection and management systems 18 U.S.C. § 545 (smuggling goods into the United States) 18 U.S.C. §§ 1341, 1343 (frauds and swindles) 18 U.S.C. § 1831 et seq. (protection of trade secrets) 18 U.S.C. §§ 2318-20 (trafficking in counterfeit labels for phone records, copies of computer programs or related documentation/packaging, and copies of motion pictures other audio visual works)

Even where the treaty diverges from U.S. law, American ratification of the treaty would not require new legislation. The Department of Justice maintains that the language of the Convention is purposefully vague to enable easy compliance with its terms.[91] However, where the treaty does materially depart from existing U.S. legislation criminalizing cybercrime offenses, enactment of the treaty will not automatically change federal criminal legislation. Treaties that specify international crimes or create criminal sanctions for particular activities still require implementing legis-

91. Frequently Asked Questions, *supra* note 27, at B1. "By their nature, multilateral conventions must take into account many different legal systems, and the test of such conventions is often more general than would be a domestic statute. The level of specificity in this convention is consistent with other multilateral law enforcement conventions." *Id.*

lation.[92] Since the extent of congressional obligation to enact legislation in compliance with a treaty is unresolved, it remains Congress's prerogative to implement legislation.[93]

Unlike the criminalized offenses, the provisions establishing procedural laws to provide law enforcement officials with the authority and tools necessary to comply with requests for international cooperation are less clearly traceable to existing U.S. law. Table 2 matches the provisions of the Convention with analogous procedural tools provided by U.S. statutes. Generally, U.S. law enforcement officials investigating computer crimes rely on the statutory privacy laws codified at 18 U.S.C. §§ 2510-21, 2701-2711, 3121-3127.[94] These statutes protect individuals against government surveillance (severely limiting the circumstances under which government agents may engage in surveillance activity) and also regulate how government agents may obtain search warrants and subpoenas to compel disclosure of electronic evidence from third parties.[95] Moreover, the Fourth Amendment constrains the ability of U.S. law enforcement officials to engage in some investigative activity.[96]

Table 2

Type of Procedural Power Granted to Law Enforcement	Convention on Cybercrime Treaty Provisions	Examples of Potentially Applicable Federal Laws and Rules of Criminal Procedure
Restrictions on police powers	Art 15. Conditions and safeguards	Fourth Amendment 1966 United Nations International Covenant

92. TREATIES, *supra* note 39, at 73 (citing AMERICAN LAW INSTITUTE, RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 111, comment I; LOUIS HENKIN, FOREIGN AFFAIRS AND THE UNITED STATES CONSTITUTION 203 (2d ed. 1996); quoting *The Over the Top*, 5 F. 2d. 838, 845 (D. Conn. 1925); "It is not the function of treaties to enact the fiscal or criminal law of a nation. For this purpose no treaty is self-executing . . . no part of the criminal law of this country has ever been enacted by treaty.").

93. *See* TREATIES, *supra* note 39, at 167 (citing LOUIS HENKIN, FOREIGN AFFAIRS AND THE UNITED STATES CONSTITUTION 205 (2d ed. 1996). However, failure to implement an internationally perfected treaty would constitute a violation of obligations assumed by the Untied States under international law. *See* Monroe Leigh, Legal Adviser, U.S. Department of State. Digest of U.S. Practice in International Law 1976, 221 (memorandum of Apr. 12, 1976).

94. DOJ SEARCH AND SEIZURE MANUAL *supra* note 19, at xi.

95. *Id.* at xiii.

96. Orin S. Kerr, Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law 4-5 (November 2, 2002) (unpublished manuscript, on file with author) (arguing that due to the lack of a suppression remedy, only the Fourth Amendment genuinely acts as a protection of citizens against unauthorized investigations by the government).

		on Human and Political Rights 18 U.S.C. §§ 3121-3127 Pen Register and Trap and Trace Statute (limiting the ability of government agents and individuals to intercept communications) 18 U.S.C. § 2510 Electronic Communications Privacy Act (limiting the ability of government agents and individuals to intercept electronic communications)
Expedited preservation of electronic data	Art 16. Expedited preservation of stored computer data Art 17. Expedited preservation and partial disclosure of traffic data	18 U.S.C. § 2703(f) (permitting order for preservation of evidence)
Production of electronic evidence stored by a third party	Art 18. Production order	18 U.S.C. § 2703(d) (granting power to compel disclosure of electronic evidence stored by a third party)
Search and seizure of computers and stored computer data	Art 19. Search and Seizure of stored computer data	FED. R. CIV. P. 41(b) (authorizing agents to obtain a warrant to seize electronic evidence)
Real time collection of Internet traffic data and interception of content data.	Art 20. Real-time collection of traffic data Art 21. Interception of content data	18 U.S.C. § 2518 (interception authorized by Title III order) 18 U.S.C. § 2511(2)(c-d) (authorizing interception by consent of party to communication) 18 U.S.C. § 2511(2)(a)(i) provider exception (authorizing mass communication providers to routinely track user activity as part of their normal course of business)

The treaty's procedural requirements to aid law enforcement have been criticized for inadequately protecting civil liberties.[97] Critics have bemoaned the general lack of safeguards for human rights resulting from the treaty's excessive focus on procedural powers.[98] Specifically, they argue that the privacy interests of individuals are undermined by the treaty's allowance of real-time interception of traffic and content data, and that the treaty does not sufficiently balance the ostensible requirement for provid-

97. *See* ACLU, *at* http://www.privacyinternational.org/issues/cybercrime/coe/ngo_letter_601.htm (Jun. 7, 2001); GILC, *at* http://www.gilc.or/speech/coe_hate speach_letter.html (Feb. 6, 2002); Center for Democracy & Technology, *at* http://www.cdt.org/international/cybercrime/010206cdt.shtml (Feb. 6, 2001); Americans for Computer Privacy, *available at* http://www.cdt.org/international/cybercrime/001207acp.shtml (Dec. 7, 2000); NetCoalition.com, *available at* http://www.cdt.org/international/cybercrime/010100netcoalition.shtml (Jan. 2001); Internet Alliance, *available at* http://www.cdt.org/international/cybercrime/001000ia.shtml (last visited Jan. 27, 2003)

98. *See* ACLU, *supra* note 97.

ing keys to encrypted materials with the rights against self-incrimination.[99] However, many of these problems were addressed during the drafting of the Convention.[100]

The current draft of the treaty contains measures to protect civil liberties. For example, Article 15 of the treaty explicitly references the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms and the 1966 United Nations International Covenant on Civil and Political Rights to incorporate the principle of proportionality with respect to punishments of various crimes harmonized by the Convention. Furthermore, the Convention arguably requires only third parties, such as systems administrators with control over requested information, to provide keys or translations of encrypted materials.[101] Finally, neither the Expedited Preservation of Stored Computer Data article (Article 29) nor the Real-time Collection of Computer Data article (Article 33) require states to enable, by statute or otherwise, searches or seizures that are beyond their current capabilities.[102]

B. Reservations Mitigate the Effect of Controversial Provisions

Other differences between U.S. law and the treaty may be less problematic because the treaty allows states to selectively elect reservations from certain provisions. For example, Article 9 of the Convention criminalizes producing, trafficking in, procuring, and possessing child pornography and defines child pornography as "material that visually depicts (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; (c) realistic images representing a minor engaged in sexually explicit conduct."[103] Current U.S. law does not go this far. However, to resolve these types of inconsistencies, parties to the Convention are permitted to take reservations on a limited number of specified articles, or parts thereof.[104] For example, with respect to Article 9 on child pornography, the Convention permits parties to elect

---

99. *Id.*

100. *See, e.g.*, *Explanatory Report to the Convention on Cybercrime*, *supra* note 3; Frequently Asked Questions, *supra* note 27, at D1.

101. *Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶¶ 200-02.

102. "The drafters of the present Convention discussed whether the Convention should impose an obligation for service providers to routinely collect and retain traffic data for a certain fixed period of time, but did not include any such obligation due to lack of consensus." *Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 135; *See also* Convention on Cybercrime, *supra* note 31, ch. II § 2 tit. 1 arts. 14 ¶ 3, 20 ¶ 1b.

103. Convention on Cybercrime, *supra* note 31, ch. II § 1 tit. 3 art. 9.

104. Frequently Asked Questions, *supra* note 27, at A7, B1.

a reservation to the requirements of "procuring" and "possessing."[105] A state can also reserve part of the definition of child pornography as it relates to images containing "a person appearing to be a minor" and "realistic images."[106]

The Jurisdiction article (Article 23) is another instance where the United States will likely elect a reservation from a treaty provision.[107] The United States does generally assert jurisdiction over crimes committed by American citizens abroad and thus would take a partial reservation to this article.[108]

Reservations occur throughout the treaty.[109] "These reservation possibilities aim at enabling the largest number of States to become Parties to the Convention, while permitting such States to maintain certain approaches and concepts consistent with their domestic law."[110] The apparent flexibility of the reservations is misleading, however. While the Convention on Cybercrime has nine specified reservation clauses, it prohibits any other reservation.[111] The available reservations highlight the areas of disagreement between the parties to the Convention on Cybercrime and emphasize (by their absence) areas of consensus.[112] However, the clause

105. Convention on Cybercrime, *supra* note 31, ch. II § 2 tit. 3, art. 9 ¶ 4.

106. *Id.*

107. Frequently Asked Questions, *supra* note 27, at A7.

108. *Id.*

109. By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Convention on Cybercrime, *supra* note 31, ch. IV art 42. For a description of each reservation *see* footnote 112 *infra*.

110. *Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 320.

111. Convention on Cybercrime, *supra* note 31, ch. IV art. 42. *See supra* note 109.

112. Parties may elect the following reservations: Article 4, paragraph 2 (limiting the crime of data interference to situations where the conduct resulted in serious harm), Article 6, paragraph 3 (negating the requirement of criminalizing the production, sale, procurement, import or distribution of devices designed primarily to enable misuse of computers systems), Article 9, paragraph 4 (negating the requirement for criminalizing procurement or possession of child pornography) (limiting the definition of child pornography so as not to include images with persons merely appearing to be minors or nonphotographic images that are too realistic), Article 10, paragraph 3 (reserving the right not to criminalize copyright infringements so long as alternative remedies remain available), Article 11, paragraph 3 (reserving the right not to criminalize attempt of the crimes out-

prohibiting additional reservations in Article 42 is problematic for U.S. ratification because the Senate Foreign Relations Committee has taken the position that executive branch negotiators should not agree to such provisions, and that, in any event, such a clause will not be construed to constrain the Senate's right to attach any reservations deemed necessary to its advice and consent.[113]

Potential reservations further complicate an analysis of the likely efficacy of the Convention in the United States, since the Senate will not necessarily be aware of what reservations other parties have stipulated to in their acceptance.[114] Given the wide range of permutations on possible reservations, merely knowing that another country is a party to the Convention will not necessarily facilitate investigations. In the context of an ongoing, extraterritorial investigation, United States authorities will still need to determine the specific reservations made by the assisting party in order to determine the level of assistance obtainable under the treaty. Thus, the strengths and weaknesses of the Convention will be ultimately determined in practice.

C. Deference to Pre-existing Mutual Assistance Agreements

The scope of the treaty is further limited by deferring to pre-existing mutual legal assistance treaties (MLATs) and other multilateral agreements already in effect.[115] Parties "that have bilateral MLATs in force between them, or other multilateral agreements governing mutual assistance in criminal cases . . . shall continue to apply their terms, supplemented by

---

lined in the treaty, Article 14, paragraph 3 (reserving the right to apply the measures in Article 20 [real-time collection of traffic data] only to offenses specified in the reservation, provided that the range of such offenses is not more limited that the range of offenses to which it applies the interception measures referred to in Article 21 [interception of content data]), Article 22, paragraph 2 (reserving the right not to assert jurisdiction on board ships flying the party's flag, or aircrafts registered under the party, or upon nationals of that party), Article 29, paragraph 4 (permitting a party who requires dual criminality for providing assistance in search and seizure operations, and who has reason to believe at the time of the request that this burden shall not be met, to refrain from complying with an expedited preservation of stored computer data request so long as it does not pertain to offenses established under Art. 2-11 where, arguably dual criminality has already been established), and Article 41, paragraph 1(reserving the right of federal states to not enact federal legislation to be in compliance with the treaty, but rather permit reliance on "its fundamental principles governing the relationship between its central government and constituent States") ETS 185—Convention on Cybercrime, *supra* note 31.

113. TREATIES, *supra* note 39, at 16.

114. *Id.*

115. Convention on Cybercrime, *supra* note 31, ch. II § 1 tit. 3, arts. 25, 27; *Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶¶ 255, 257, 262, 263

the computer- or computer-related crime-specific mechanisms . . . unless they agree to apply any or all of the provisions of this Article in lieu thereof."[116]

While this deference seems to obviate the need for the Convention, it is nonetheless reassuring. MLATs represent a more recent type of treaty especially designed for the gathering of evidence in criminal cases.[117] MLATs typically provide "the means for tracking, freezing and confiscating crime-tainted assets found beyond the borders of the country in which the crime occurred."[118] They also typically include "escape clauses," which allow parties to deny assistance if the request does not conform to the treaty, relates to a political or military offense, or if rendering assistance would impinge upon the security or essential public interests of the state of which the request is made.[119]

IV. REEXAMINING THE VALUE OF THE CONVENTION ON CYBERCRIME

The ambiguity of each party's commitment to mutual assistance in cybercrime investigations and the subordination of the treaty to pre-existing mutual assistance agreements cloud the benefits of ratifying the Convention. However, there are two more pressing reasons for questioning the value of the Convention on Cybercrime. First, because the nature of cybercrime is rapidly changing, the cumbersome amendment process of treaties would risk a premature fixation of the law. Second, the treaty fails to resolve the extraterritorial jurisdictional issue, the core issue prompting development of the treaty.

A. The Convention and its Amendment Process Introduces Stagnation

Cybercrime legislation is in a nascent state and hence highly susceptible to alteration.[120] Widespread adoption of the Convention could stunt the

116. *Explanatory Report to the Convention on Cybercrime*, *supra* note 3, ¶ 263

117. TREATIES, *supra* note 39, at 282. The traditional procedure for obtaining such evidence is presentation of letters rogatory, a written request from the court of the investigating country to the court of country in which the investigation is to take place. U.S. officials have found this method of requesting evidence and legal assistance to be less satisfactory than the new MLATs because the agreements were not compulsory and frequently produced evidence which was inadmissible in the courts of the prosecuting country. *Id.*

118. *Id.*

119. *Id.* at 282-83.

120. *See generally* Orin S. Kerr, The Troubling Trigger of Cybercrime 8-22 (Aug. 15, 2002) (unpublished manuscript, on file with author).

development of cybercrime legislation. While the Convention essentially exports U.S. law, current U.S. law on cybercrime is far from ideal.[121] Cybercrime legislation in the United States is complicated by its residual ties to property law precedent and telephony-based statutory law.[122] Alternative paradigms may be more suitable to the domain of cyber space.[123]

Treaties are more difficult to amend than domestic legislation.[124] In theory, treaties to which the United States is a signatory require the participation of the Senate before modification or amendment.[125] The process is so onerous that it has been equated to the formation of an entirely new agreement.[126] The recent addition of the protocol on racist and xenophobic speech to the treaty demonstrates the intention of the Council of Europe to mitigate this issue by using protocols, which function as distinct multilateral agreements, separate from the treaty itself. But this solution does not address the concern that the provisions of the treaty itself may be in some significant way a sub-optimal solution to the reduction of cybercrime.

Of course, the United States has never felt corralled by treaties. The United States maintains that treaties may be superceded by an act of Congress,[127] even at the risk of incurring the ire of the international community and violating international law as established under the Vienna Convention.[128] It is unclear to what extent the development of U.S. cybercrime law would be hampered by ratification of the Convention.

B. Convention Does Not Resolve the Jurisdictional Issue

The Convention on Cybercrime does not resolve the extraterritorial jurisdictional issue because it ultimately fails to articulate a common set of crimes. The Convention is further hampered by the lack of universal participation.

The Convention lacks substance because the reservations act as loopholes for parties whose laws do not harmonize with existing U.S. law. Thus, the Convention represents only an illusory attempt to harmonize cy-

---

121. *Id.* at 24-52.

122. *Id.*

123. *Id.* at 60-71; *see also* Kerr, *supra* note 96.

124. *See* TREATIES, *supra* note 39, at 173.

125. *See id.*

126. *Id.*

127. *Id.* at 174 (citing Chae Chan Ping v. United States, 130 U.S. 581 (1889) (supporting the proposition that the outcome of the cases, though in violation of international law, did not present an issue of constitutional significance); Edye v. Robertson, 112 U.S. 580 (1884)).

128. Although the US has not yet ratified the Vienna Convention, it is still widely considered the primary source of international law. TREATIES, *supra* note 39, at 20-21.

bercrime laws between its prospective members. The reservations permit parties to preserve their existing laws and undermine harmonization. As a result of these reservations, it is unclear which parties, if any, will need to adjust their current domestic law to be in compliance with the treaty.[129]

Furthermore, the Convention does not establish a foundation of consensus, arguably because of overreaching by the drafters. By trying to incorporate all the crimes that all the parties wanted instead of criminalizing only activities on which there was a consensus, the Convention fails to articulate a common ground for cybercrime legislation. Under the treaty, any common ground of cybercrime legislation will remain unknown until all parties have acceded and all reservations have been stipulated.

Finally, the treaty fails if participation is not universal.[130] It will take years to ratify the treaty,[131] and once ratified, the cooperation mechanisms will only work if there is universal accession.[132] In the absence of worldwide participation in the Convention, cyber criminals could simply relocate to a jurisdiction outside of the Convention's reach, or avert detection by routing their online activities through a state outside of the Convention.[133] Other states, including the UNITED STATES, will still need to take unilateral action against individuals in countries that fail to join, ratify, implement or enforce the treaty.[134] In the mean time, the Convention inadequately addresses cross-border computer disruption crimes.[135]

V. AN ALTERNATIVE: A MODEL CYBERCRIME LAW

The Senate must either ratify the Convention on Cybercrime with the provided reservations, or reject it in its entirety. However, there are alternatives to the convention. One such solution is the establishment of a model cybercrime code.

The global community may be better served by a solution entailing a model cybercrime code than by the widespread adoption of a treaty codi-

---

129. *See* Frequently Asked Questions, *supra* note 27, at A7 (arguing that the United States will not need to implement new legislation in order to comply with the treaty once ratified, however, not specifying which countries would need to implement new legislation yet making broad pronouncements about the value of the treaty to United States law enforcement).

130. Jack L. Goldsmith, *The Internet and the Legitimacy of Remote Cross-Border Searches*, 2001 U. CHI LEGAL F. 103, 107 (2001).

131. *Id.*

132. *Id.*

133. *See id.*

134. *Id.*

135. *Id. See generally* Bellia, *supra* note 6.

fying the current law of the hegemony. A model cybercrime code is advantageous because it could be changed more easily as technology develops. Furthermore, states could better maintain consistency between their own legislative schemes and the model code. Finally, the process of developing such a model code might yield superior solutions to the jurisdictional problems permeating cybercrime legislation.

Nonetheless, establishment of a model cybercrime code is unlikely to be the panacea hoped for. Worldwide harmonization of cybercrime legislation would probably take even longer to achieve under a model code. Furthermore, although a model code might uniformly criminalize a cannon of offenses, it must also have a mechanism for insuring cooperation between states that implement its provisions. Most successful model codes are derived by identifying social norms and selectively elevating some to become tenants of the code.[136] Thus, a successful model code is likely to replicate much of the content of the Convention.

Despite its flaws, the Convention on Cybercrime is a starting point, and the ultimate value of the Convention may in attracting members over time. Even without universal membership, the Convention is still relevant as a tool to force harmonization with parties outside the Convention. If the current parties to the Convention generally concur on a paradigm of cybercrime legislation, then that hegemonic paradigm will be described by the Convention. The true process of harmonization will begin when the Convention admits new members to the treaty on the condition that they change their laws align with this hegemonic paradigm. Unilateral assertions of power by Convention member states against nonmember states might encourage universal entry into the Convention, thereby eventually bringing about worldwide harmonization of cybercrime laws and alleviating the problem of the no-man's-land in cyber law.[137]

VI. CONCLUSION

The Convention on Cybercrime is best understood as a potential tool for establishing a hegemony in Internet regulation and exporting that hegemonic regulatory scheme to the rest of the world, rather than as an

136. ". . . Karl Llewellyn, the scholar who directed the creation of America's most successful code, *The Uniform Commercial Code*, explicitly identified the best business practices and wrote them into the code." ROBERT COOTER & THOMAS ULEN, LAW & ECONOMICS 422 (3RD ED. 2000).

137. Goldsmith, at least, has concluded that such recourses are necessary and even desirable insomuch as they can be used as a tool to generate greater and more rapid incorporation of States into the Treaty, using assertion of power as a bully club of sorts. Goldsmith, *supra* note 130, at 117.

effort to harmonize the cybercrime laws of current members of the Convention. Irrespective of the ethics of such exportation, there are few realistic alternatives. As criminal activity becomes increasingly un-remediable by technological fixes and traditional mechanisms of international cooperation, countries will resort to unilateral assertions of power to conduct remote searches or otherwise assert jurisdiction to solve the problem of cybercrime. If digitally advanced countries, such as the United States, fail to come to terms in the context of a treaty or similar instrument, then the jurisdictional problem of cybercrime legislation will continue to threaten state sovereignty.