A CRITIQUE OF THE INTERNATIONAL CYBERCRIME TREATY

Ryan M.F. Baron

Crime is on the rise in cyberspace, and it is threatening the economic and social institutions that have begun to settle there. Cybercrime is quick to occur and difficult to prosecute.[1] Network intrusions and "hacks" can take place in a matter of seconds with complete anonymity. And those that do leave criminal trails do so through a maze of computer infrastructure, often far beyond the reach of a nation's laws.

Several Western nations have come together in an attempt to deter hackers and limit cyber attacks. The Council of Europe ("CoE") along with the U.S. Department of Justice ("DOJ") have been actively meeting since 1997 in the drafting of an international treaty whereby signatory countries are required to create and strengthen their domestic laws. This treaty in effect will create new cybercrimes, extend the interception and surveillance abilities of law enforcement and coordinate such enforcement so that authorities can communicate with one another and exchange information when investigating cyber "incidents." And given the unique nature of the Internet, increased power over surveillance and data interception may lead to intrusions into the personal lives of those that utilize and maintain that technology.

This comment serves as a critique of the international cybercrime treaty, from its shrouded origins to its final draft. First, this comment will briefly explore the exigencies of cybercrime that have stirred Western nations into a state of alarm. Second, it will explore the origins and early drafts of the treaty. Third, it will scrutinize the language of the treaty, examining its criminal law impact on cyberspace. Finally, this comment concludes that cybercrime's state of alarm is privacy's state of emergency and that the U.S. should not sign the present treaty as drafted.

I. THE INTERNATIONAL EXIGENCY OF CYBERCRIME

Globally, the amount of damages from network intrusions causes more than $15 billion in damages annually.[2] From hacks into credit card companies to identity theft to terrorism[3] such attacks have become so common that the newspaper headlines do not generally report these intrusions as primetime news.[4] Many of these attacks go unreported as companies fear negative publicity and lack confidence in their information practices.[5]

In 2000, the United States alone accounted for over $20 billion in e-commerce retail revenues.[6] Large amounts of online transactions have inevitably become a target for criminal activities. Congress has taken a number of statements from various law enforcement officials concerning the growth of cybercrime. The FBI reported opening 547 computer intrusion cases in 1998 that had

1 *See* Martin Stone, *Cybercrime Growing Harder to Prosecute – Report*, NEWSBYTES, *at* http://www.infowar.com/law/00/law_012400a_j.shtml (Jan. 21, 2000).

2 Steve Gold, *Security Breaches Cost $15 Bil. Yearly*, NEWSBYTES, *at* http://www.newsbytes.com/news/00/158197.html (Nov. 15, 2000). E-security white paper and allied report is available at *E-Security: Removing the Roadblock to E-Business*, THE DATAMONITOR GROUP, *at* http://www.datamonitor.com. There is a charge to access copies of this report.

3 Michelle Delio, *The Greatest Hacks of All Time*, WIRED NEWS, *at* http://www.wired.com/news/print/0,1294,41630,00.html (Feb. 6, 2001).

4 *Internet Security: Hearing Before the Subcomm. on Science, Technology, and Space of the Senate Comm. on Commerce, Science, and Transportation*, 107th Cong. (2001) (statement of Bruce Schneier, Chief Technical Officer of Counterpane Internet Security, Inc.), *available at* http://commerce.senate.gov/hearings/071601Schneier.pdf (last visited July 24, 2002).

5 Sylvia Dennis, *Internet Fraud Escalating in UK, Says Experian*, NEWSBYTES, *at* http://www.infowar.com/survey/00/survey_091500a_j.shtml (Sept. 14, 2000); *see also* Council of Europe, CYBER-CRIME – THE TARGET IT HITS, THE DAMAGE IT DOES, *at* http://press.coe.int/press2/press.asp?B=54,0,0,107,0&M=http://press.coe.int/dossiers/107/E/ecibles.htm (last modified Sept. 17, 2001).

6 U.S. CENSUS BUREAU, Department of Commerce, U.S. DEPT. OF COMMERCE NEWS, *at* http://www.census.gov/mrts/www/current.html (Aug. 30, 2001).

doubled by 1999.[7] The agency stated that although it had closed several of these cases, threats were growing at disproportionate rates.[8] Broad spectrums of groups are posing serious threats to the Internet, including so-called "insiders,"[9] hackers, virus writers, terrorists and other criminal groups.[10]

The United States has been hailed a "major importer of crime"[11] due to the large amount of business transactions that occur within it its borders and its increasing reliance on the Internet as platform for commerce. U.S. law enforcement officers not only deal with cybercrime in this country, but have been actively implementing international programs that coordinate access to information with other national law enforcement groups and train other international law enforcement officers to combat international crime. Thousands of foreign law enforcement officers from over forty countries are trained by U.S. officers.[12] Such initiatives train foreign officers in computer related skills, such as tracking and surveillance methods.

The U.S. has strict enforcement techniques, including customs programs and national monitoring of communications traffic due to the large amount hacking attempts that originate outside the country. Because of the continued growth of international crime, the FBI has established several programs designed to initiate and empower enforcement efforts.[13] The FBI, though, is not the only executive entity active about cybercrime. Criminal misuse of computers has also affected government systems. The Central Intelligence Agency ("CIA") reported that the major challenge concerning cybercrime is to "find ways to defend our infrastructure and protect our commerce while maintaining an open society."[14] A recent incident occurred where U.S. military systems were subjected to an "electronic assault" termed Solar Sunrise. Two teenage hackers in California hacked into U.S. military systems while under the direction of a teenage hacker in Israel. The intruders went undetected at first as they hid their "tracks" through networks of routers and servers.

Computer crime affecting commercial and military computer systems has not gone unnoticed. Hacking and network intrusions have spawned an international effort in the U.S. and other Western nations to implement model laws outlawing computer misconduct. With extensive help from the

---

7 *Cybercrime: Before the Subcomm. for the Dept's of Commerce, Justice, State, the Judiciary, and Related Agencies of the Senate Comm. on Appropriations*, 106th Cong. (2000) [hereinafter *Freeh Statement on Cybercrime*] (statement of Louis J. Freeh, Director of the Federal Bureau of Investigation), *available at* http://www.fbi.gov/pressrm/congress/congress00/cyber021600.htm (last visited July 24, 2002). The FBI reported that 1154 cases had been opened in 1999. These figures do not include crimes such as Internet fraud or online child pornography.

8 *See generally* Marc C. Goodman, *Why the Police Don't Care about Computer Crime*, 10 HARV. J.L. & TECH. 465 (1997) (stating five reasons as to how and why police have problems confronting and investigating cybercrime: cybercrime is outside the job description, difficulty of policing the Internet, lack of resources, police need additional technical help and a lack of public outcry); *id.* at 477–490. The author states that these institutional factors deter the police from *even investigating* cybercrime. *Id.* at 494.

9 These cases involve unauthorized access by disgruntled employees with inside information on their company.

10 *Cybercrime: Before a Special Field Hearing Before the Subcomm. on Tech., Terrorism, and Gov't Info. of the Senate Comm. on the Judiciary*, 106th Cong. (2000) (statement for the Record of Guadalupe Gonzalez, Special Agent in Charge, Phoenix Field Division, Federal Bureau of Investigation), *available at* http://www.fbi.gov/pressrm/congress/congress00/gonza042100.htm. An example of this category is an international group who penetrated the computer systems of MCI, Sprint, AT&T, Equifax and the National Crime Information Center of the FBI. Convictions were based on the theft of thousands of Sprint calling card numbers.

11 *See The Threat of International Crime and Global Terrorism and the International Law Enforcement Programs of the Federal Bureau of Investigation: Before the House Int'l Relations Comm.*, 105th Cong. (1997) (statement of Louis J. Freeh, Director of the Federal Bureau of Investigation), [hereinafter *Freeh Statement on International Crime*], *available at* http://www.fbi.gov/pressrm/congress/congress97/initiatives-int.htm.

12 *Id.*

13 *International Crime: Before the Subcomm. on Foreign Operations of the Senate Comm. on Appropriations*, 105th Cong. (1998) (statement for the record of Louis J. Freeh, Director of the Federal Bureau of Investigation), *available at* http://www.fbi.gov/pressrm/congress/congress98/intrcrime.htm.

> First, the FBI must have an active overseas presence that fosters the establishment of effective working relationships with foreign law enforcement agencies . . . Second, training foreign law enforcement officers in both basic and advanced investigative techniques and principles is a powerful tool for promoting cooperation . . . Third, institution building is necessary to help establish and foster the rule of law in newly democratic republics. *Id.*

14 *Cyber Threats and the U.S. Economy: Before the Joint Econ. Comm.*, 106th Cong. (2000) (statement by John A. Serabian, Jr., Information Operations Issue Manager for the Central Intelligence Agency), *available at* http://www.cia.gov/cia/public_affairs/speeches/archives/2000/cyberthreats_022300.html. The statement covered four threats: foreign entities could perform cyber reconnaissance of U.S. computers; an attacker could conceal points of origin by hopping through several intermediate way stations in cyberspace; an attacker could conceal his origin and erase cyber footprints from victim computers; cyber tools are readily available.

U.S., Europe has been actively discussing and has drafted a treaty that would do just that.

II. HISTORY OF THE DRAFT TREATY

A. The Rise of International Law

European discussions of cybercrime have been ongoing for several years. Although the general public may have had trouble obtaining such information, European directives have provided some indication that national legislation in the Community was beginning to address its share of the growing problem. The Council of Europe[15] ("CoE") has been the leading multi-lateral organization concerned with cybercrime thus far. In 1989, the CoE's Committee of Ministers[16] adopted Recommendation No. R. (89) 9 stating that Member States need to consider computer-related crime when reviewing national legislation.[17] The Recommendation also listed implementation guidelines for legislators that would criminalize certain criminal acts. Procedural policies were subsequently drafted in 1995. Recommendation No. R. (95) 13 was adopted to provide procedures for criminal law concerning issues such as search and seizure, surveillance and international cooperation.[18]

Although the Council issued specific recommendations, no formal process had been initiated that would coordinate the laws of member European states. But in 1997, a Committee of Experts on Crime in Cyber-Space (PC-CY)[19] was formed to examine problems related to computer crime and to implement criminal procedures dealing with this new and growing form of crime.[20] The PC-CY was to use the previous two recommendations as a foundation for examining the growing threat of computer crime and the appropriate legal structure to implement. PC-CY was charged with drafting "a binding legal document" that would eventually evolve into the present-day cybercrime treaty. The PC-CY's legal conclusions addressed five issues: cyber offenses through telecommunication networks, harmonization of substantive criminal law,[21] the investigative powers of law enforcement, conflict of laws issues and questions of international cooperation.[22] The terms of reference specified that participating countries appoint expert members,[23] and also provided the

---

15 The CoE is a "multinational organization that includes both European Union member states and several non-democratic countries." Comments of NetCoalition.com, *The Cybercrime Convention Will Harm U.S. Internet Users and Business*, NETCOALITION [hereinafter *Comments of NetCoalition*], at http://www.cdt.org/international/cybercrime/010100netcoalition.shtml (Jan. 2001). The Council of Europe consists of 43 member states. COUNCIL OF EUROPE, THE COUNCIL OF EUROPE'S MEMBER STATES, *at* http://www.coe.int/portal.asp?strScreenType=100&L=E&M=$t/1-1-1-1//portal.asp?L=E&M=$t/001-00-00-2/02/EMB,1,0,0,2,Map.stm (last modified Sept. 17, 2001) (listing Member States and the year these states joined the CoE). It was established in 1949 as an organization dedicated to strengthening human rights by promoting democracy and the rule of law in Europe. The U.S. Department of Justice notes that it is the negotiating forum for conventions on criminal issues. DEPARTMENT OF JUSTICE, *Frequently Asked Questions and Answers About the Council of Europe Convention on Cybercrime (Draft 24REV2)*, *at* http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm (last updated Dec. 1, 2000). Although the United States is not a member, it does maintain "observer" status at CoE deliberations. *Id.* For more information, *see generally* the CoE's website *at* http://www.coe.int.

16 The Committee of Ministers is the decision-making body of the Council of Europe. The Committee is also responsible for directly representing the governments of the member States. *See* Council of Europe, *Introduction to the Committee of Ministers*, *at* http://cm.coe.int/intro/intro.0.html. The Council of Ministers "is the main source of EU legislation." FIONA HAYES-RENSHAW & HELEN WALLACE, THE COUNCIL OF MINISTERS 1 (1997).

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

18 Recommendation No. R. (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology, 1995, *available at* http://www.coe.fr/cm/ta/rec/1995/95r13.htm [hereinafter Recommendation No. R. (95)]. The Recommendation also implemented procedures for electronic evidence, use of encryption, cooperation obligations and research, statistics and training.

19 The Committee of Experts on Crime in Cyber-Space (PC-CY) is a form of "subcommittee" housed in the CoE's European Committee on Crime Problems (CDPC).

20 *Specific Terms of Reference of the Committee of Experts on Crime in Cyber-Space*, Council of Europe's Fight Against Corruption and Organised Crime, §4(a)-(b), 583rd Meeting [hereinafter *Specific Terms of Reference*], *available at* http://www.cm.coe.int/dec/1997/583/583.a13.html (Feb. 4, 1997). The terms of reference are the recommendations and reports that PC-CY was to build upon when reviewing problems of computer-related crime.

21 The issues under this subject involved international cooperation approaches relating to "definition, sanctions and responsibility of the actors in cyber-space, including Internet service providers." *Id.* at §4(c)(ii).

22 *Id.* at §4(c)(iv) and (v). The PC-CY did not give examples of international cooperation, but such efforts would include coordination of intergovernmental enforcement agencies, the international interconnection of police computer databanks and 24/7 cybercrime hotlines. *See generally Freeh Statement on International Crime*, *supra* note 11.

23 Membership of the Committee included "one expert

"desired" qualifications to look for in the process of appointing these experts.[24] In addition, the U.S., Canada and Japan had been named as "observer" countries. The observers may send a representative, but do not have the right to vote.[25] These terms of reference were to expire originally on December 31, 1999,[26] but were later extended to December 2000.

Most of this information was minimally available to the general public.[27] At most, one could find an occasional passing reference to the PC-CY in European government materials.[28] The CoE's press release in February 1997 called for a legally binding document to be drafted in which the PC-CY met in relative obscurity up until the early months of 2000. At this time, USENET groups began to report that a cybercrime treaty was in the works.

In the early weeks of the new millennium, USENET[29] reports began circulating that European officials had been meeting in secret to discuss the drafting of a world cybercrime treaty.[30] Although the reports were not yet being posted by the more traditional sources of Internet news,[31] the word was that European officials had been holding discussions "that would try and ban hacking and Internet eavesdropping utilities."[32] It was reported that the U.S. government, along with Japan, Canada and South Africa, had been participating in the talks. The primary source for the USENET reports was a letter from the Dutch Minister of Justice written to the Dutch Parliament, which mentioned basic details of the treaty discussions and its objectives for increased eavesdropping and surveillance of the Internet.[33]

These early reports were generally unconfirmed, with European press officers declining to

appointed by the government of the following member states: Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Netherlands, Portugal, Sweden, 'the former Yugoslav republic of Macedonia,' as well as two scientific experts appointed by the Secretariat." *Id.* at §5(a).

24 The qualifications included "prosecutors or judges dealing with computer crime cases, experts in the field of substantive and procedural law aspects of computer crime, experts having carried out research in this field; persons appointed should also have international experience and sufficient knowledge of the technical aspects of computer crime. Members of previous Council of Europe expert committees on computer-related crime would be preferable." *Id.* at §5(c).

25 The observer countries were also required to pay their own expenses. Except for the Netherlands and Portugal, the participating countries could defray costs. *Id.* at §5(b), (d).

26 Some sources, though, reported that PC-CY was to complete the document by the end of 2000 and not 1999. *See, e.g.,* 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, 478 (1999).

27 In general, it is the policy of the CoE to not release drafts while negotiations are ongoing. It is not until negotiations have begun to close that the text of a draft treaty would normally be released. Interview with John Lynch, U.S. Attorney, Computer Crime and Intellectual Property Section, U.S. Department of Justice (Mar. 10, 2001) [hereinafter *Interview with John Lynch*]. In this case, the text of the draft treaty has only been released online.

28 *Specific Terms of Reference, supra* note 20. It is the policy of the CoE to conduct its meetings in private. Rules of Procedure of the Council, art. 4(1), 1996 O.J. (Dec. 10, 1996).

29 *Webopedia*, an online encyclopedia, defines a USENET as "[a] worldwide bulletin board system that can be accessed through the Internet or through many online services. The USENET contains more than 14,000 forums, called *newsgroups*, that cover every imaginable interest group. It is used daily by millions of people around the world." WEBOPEDIA, INTERNET.COM, *at* http://webopedia.internet.com/TERM/U/USENET.html.

30 Steve Gold, *World Cybercrime Treaty May Be Underway*, NEWSBYTES, *at* http://www.newsbytes.com/news/00/142185.html (Jan. 14, 2000) [hereinafter Gold]. The article stated that reports of the treaty had been circulating on a Dutch USENET, which may be viewed at http://www.bof.nl. A user of landfield.com posted a similar article in the news archives of Internet Security News. *[ISN] US-Europe Cybercrime Treaty Happening in Secret*, LANDFIELD.COM, *at* http://www.landfield.com/isn/mail-archive/2000/Jan/0019.html (Jan. 13, 2000). Internet Security News is a part of Landfield.com's USENET service where users can post information related to the specific subject matter.

31 I refer to traditional sources of Internet news as CNN.com, ABCnews.com, WashingtonPost.com, etc.

32 Gold, *supra* note 30. Many news websites began using the USENET post and the *Newsbytes* article as their sources for their own reports on the treaty discussions.

33 Press Release, Dutch Minister of Justice, *Crime in Cyberspace Convention: International Measures to Tackle Internet Crime*, *at* http://www.minjust.nl:8080/c_actual/persber/pb0549.htm (Dec. 24, 1999) [hereinafter *First Draft Press Release*]. The letter was stated to have been translated from Dutch to English and then posted on the USENET group. Interested parties may find an English translation of the letter at the above website. M. Wessling, *US-Europe Cybercrime Treaty Happening in Secret*, POLITECHBOT.COM, *at* http://www.politechbot.com/p-00849.html (Jan. 13, 2000) [hereinafter Wessling]. The author of the post translated and discussed the context of the Dutch letter.

> Protection against so-called CIA-crimes (confidentiality, integrity and availability) of public and closed networks and systems: computer hacking, unauthorized eavesdropping, unauthorized changing or destroying of data (either stored or in transport). In discussion are also denial of service attacks to public and private networks and systems. This will probably not cover spam. The treaty will outlaw the production, making available or distribution of hardware and software tools to do the abovementioned (hacking, denial of service, eavesdropping, etc.). The letter does not mention the possession of these tools. *Id.*

comment on the subject.[34] One source did state that a draft treaty would need considerable public debate and that all countries would need to be in agreement before becoming signatories.[35] Cybercrime enforcement had been underway for several years, and the CoE was answering any specific questions concerning the draft convention or a possible treaty.[36]

In April of 2000, a "first" draft[37] of the treaty was finally made available to the public as well as a press release[38] that described the basic legal elements and philosophies behind the draft convention.[39] The press release officially declassified the draft convention and called for "businesses and associations" to comment "before the final adoption of the text."[40] It also stated that the CoE was focusing on the harmonization and the implementation of procedural and substantive criminal law with regards to cybercrime. One of the main goals was the coordination and cooperation of international law enforcement. The U.S., Canada, South Africa and Japan were named as actively participating in the treaty negotiations.[41]

An official of the U.S. DOJ mentioned the treaty as early as February 1999,[42] and then Attorney General Janet Reno also made a passing reference in September 1999, but in reference to trans-border searches.[43] In December 2000, the U.S. DOJ officially acknowledged on its website that it had been participating in the negotiations of the draft convention for a few years prior to the first public draft and stated that it "has had a real voice in the [current] drafting process."[44] The President of Silicon Defense, Stuart Staniford, while appearing on a panel about the draft treaty at the European Computer Security Conference, stated that even though the U.S. is an observer at the CoE, it "has apparently been heavily involved in the drafting."[45]

While the first public release of the draft treaty was in its 19th version,[46] several drafts have subsequently been released. In June 2001, the final draft was approved by the European Committee on Crime Problems.[47] It has since been finalized by the Committee of Ministers and opened up for signature.[48]

---

34 Gold, *supra* note 30.

35 *Id.*

36 *Id.* A law journal article by Michael Sussman, attorney with the DOJ, references a telephone interview with the Counselor for Criminal Justice Matters with the European Union concerning the draft convention. *See* 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, 459 n.29, 478 n. 103 (1999).

37 The press release called the draft treaty the "[f]irst draft of international convention released for public discussion." While this was the first draft released to the public, the draft treaty was in its 19th revision. *First Draft Press Release, supra* note 33.

38 Early news reports on the treaty had mistakenly reported the European Union as negotiating the treaty. The European Union is a distinct entity separate from the CoE. *See* EUROPEAN UNION, THE ABC OF THE EUROPEAN UNION, *at* http://europa.eu.int/abc-en.htm (last visited Dec. 23, 2001).

39 *First Draft Press Release, supra* note 33.

40 *Id.*

41 These countries are named as "observers" and may participate, but may not have a vote in the PC-CY. *Id.* at §5(e).

42 *Interview with John Lynch, supra* note 27.

43 Janet Reno, Speech Before the High Technology Crime Investigation Association 1999 International Training Conference, *at* http://www.cybercrime.gov/agsandie.htm (Sept. 20, 1999).

44 DEPARTMENT OF JUSTICE, FREQUENTLY ASKED QUESTIONS AND ANSWERS ABOUT THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME (DRAFT24REV2), *at* http://www.usdoj.gov/criminal/cybercrime/newCOEFAQs.html (July 10, 2001) (alteration in original). The Department of Justice hosts this web page answering some "frequently asked questions" regarding the CoE Convention on Cybercrime. The DOJ stated that it had been invited to participate as an "observer" in the development of the Convention. The DOJ has a history of being an "observer," both times in the Recommendations addressing the need for laws concerning crime over computer networks published in 1989 and again in 1995. *Id.*

45 Stuart Saniford, *Common Vulnerabilities and Exposures: The Key to Information Sharing, Panel on Cybercrime Treaty, at* http://www.cve.mitre.org/board/archives/2000-10/msg00007.html (Oct. 5, 2000) [hereinafter Saniford]. CVE is a collaborative effort including "representatives from numerous security-related organizations such as security tool vendors, academic institutions, and government as well as other prominent security experts," which "aims to standardize the names of all publicly known vulnerabilities and security exposures." COMMON VULNERABILITIES AND EXPOSURES, ABOUT CVE, *at* http://www.cve.mitre.org/about (Jan. 22, 2001).

46 EUROPEAN COMM. ON CRIME PROBLEMS, DRAFT CONVENTION ON CYBER-CRIME (DRAFT NO. 19) OF THE COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE, *at* http://conventions.coe.int/treaty/en/projets/cybercrime.htm (Apr. 25, 2000) [hereinafter *Cybercrime Treaty Draft 19*].

47 EUROPEAN COMM. ON CRIME PROBLEMS, DRAFT CONVENTION ON CYBER-CRIME OF THE COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE, *at* http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm (June 29, 2001) [hereinafter *Cybercrime Treaty Final Draft*]. Drafts No. 19 through 24 can also be accessed through the CoE website.

48 Committee of Ministers, *Convention on Cybercrime ETS no.: 185, at* http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185&CM=8&DF=12/12/01 (last visited Dec. 23, 2001).

III. THE TREATY EXPLAINED

Since its initial release in April 2000, the treaty has been revised several times in response to much criticism over its language and the potential problems with its procedural implementation. Groups have called the treaty "alarming and quite disturbing,"[49] with criticism stemming from the U.S. and within Europe. Many organizations have come together to protest and comment on the treaty's backseat treatment of privacy rights.[50] The following analysis will show that these apprehensions are rightfully appropriate.

A. The Preamble

The treaty contains 48 articles,[51] categorized under lengthy chapters, titles and subsections. Its beginning starts with a preamble stating the document's intent. The intent is to foster a "common criminal policy aimed at the protection of society against cyber-crime."[52] To foster protection, it promotes cooperation between governments and industry. As cybercrime can happen abruptly and without detection, the drafters find it crucial that law enforcement be able to mobilize swiftly and efficiently. This would require "increased, rapid, and well-functioning international co-operation" against cybercrime.[53] Other elements of the treaty address deterrence as a necessary function of the draft convention.[54] The preamble states that facilitation of "detection, investigation and prosecution" will protect the "confidentiality, integrity and availability of computer systems."

While the primary themes of the treaty focus on the prevention of criminal acts and the coordination of international law enforcement, a large part of the preamble attempts to devote a theme to the issue of "fundamental human rights."[55] "Mindful" of the rights of individuals, the draft treaty states that it balances this against the interests of law enforcement. The preamble "enshrines" itself within the major international human rights documents drafted by the Council of Europe.[56] Unfortunately, this rhetoric of rights ends as quickly as it begins. It should be noted that the first release of the public draft failed to mention the need for individual rights.[57] The provisions dealing with rights have only come about in subsequent drafts showing, quite possibly, that human rights were never of importance to the committee drafters.

More examples of law enforcement's truncated balance are evident with a reading of the terms of reference, listed toward the end of the preamble. The original terms of reference, as explained ear-

---

49 Jason Wallace, *Council of Europe Cybercrime Treaty Analysis, at* http://www.ithell.com/Opinion/Cybercrime_Treaty/body_cybercrime_treaty.html (November 2, 2000) [hereinafter Wallace]. The author argues that the vague nature of the treaty will trammel civil rights and that privacy procedures should be of first concern. *Id.* Ithell.com hails itself as "Where IT Professionals Vent!"

50 *See, eg.,* CENTER FOR DEMOCRACY & TECHNOLOGY, COMMENTS OF THE CENTER FOR DEMOCRACY AND TECHNOLOGY ON THE COUNCIL OF EUROPE DRAFT "CONVENTION ON CYBERCRIME" (DRAFT NO. 25), *at* http://www.cdt.org/international/cybercrime/010206cdt.shtml (Feb. 6, 2001) [hereinafter *CDT Comments*]. STATEMENT OF CONCERNS, TREATY LETTER BY INDIVIDUAL SIGNERS, *at* http://www.cerias.purdue.edu/homes/spaf/coe/TREATY_LETTER.html; *see also* SIGNERS OF THE CONCERNS LETTER, *at* http://www.cerias.purdue.edu/homes/spaf/coe/TREATY_SIGNATURES.html; GLOBAL INTERNET LIBERTY CAMPAIGN, GLOBAL INTERNET LIBERTY CAMPAIGN MEMBER LETTER ON COUNCIL OF EUROPE CONVENTION ON CYBER-CRIME, *at* http://www.gilc.org/privacy/coe-letter-1200.html (Oct. 18, 2000) [hereinafter *Global Internet Liberty Campaign*]. These organizations are just a few of the many groups against the current draft treaty.

51 For this paper, all references to a particular section of the treaty will be by article number.

52 *Cybercrime Treaty Final Draft, supra* note 47, at preamble.

53 *Id.*

54 Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international cooperation. *Id.*

55 *Cybercrime Treaty Final Draft, supra* note 47, at preamble.

56 The preamble lists the applicable human rights documents that the draft treaty is "enshrined" within. These include: the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms; the 1966 United Nations International Covenant on Civil and Political Rights; the 1981 Council of Europe Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data; the 1989 United Nations Convention on the Rights of the Child; and the 1999 International Labour Organization Worst Forms of Child Labour Convention. *Id.* Much of the draft treaty's rhetoric may pay lip service to these great documents, but nowhere does the draft treaty specifically answer how the principles of these great documents are incorporated on a practical level. This assumption of my analysis may be naïve, but a draft treaty that articulates the practical concerns of law enforcement, yet only crafts theoretical notions of human rights with absolutely no practical implementation of such should be deemed as "hollow rhetoric." *Id.* at art. 15.

57 *Cybercrime Treaty Draft 19, supra* note 46.

lier, included Recommendations No. R. (89) 9 and No. R. (95) 13, which dealt with guidelines for considering computer crime and related problems in criminal procedure law, respectively.[58] Additional Recommendations have been added, including those dealing with the interception of telecommunications,[59] copyright infringement and piracy[60] and "regulating the use of personal data in the police sector."[61] While these subjects were to be examined by the committee,[62] additional recommendations concerning law enforcement have been added by the committee, thereby loading the language of the draft treaty with enforcement references.

B. Language of the Treaty

The preamble states the general philosophical foundations of the treaty. A working paper written by the Center for Democracy and Technology states that the draft is actually "a combination of three treaties."[63] First, signatory countries must implement substantive criminal provisions to unify the scattered state of Western cyber laws. Second, unilateral procedures must be adopted that allow for increased government power in cyber-criminal investigations. Finally, the treaty requires the institution of international cooperation efforts in collecting evidence and intercepting communications.

The treaty is composed of four main chapters. Chapter one deals with the use of terms and definitions. Chapter two calls for substantive and procedural measures to be implemented at the national level. Chapter three concerns international cooperation efforts, with chapter four left for the final provisions and other miscellaneous treaty components.

Chapter two is split into two sections that deal with the specific laws and procedures to be enacted by each signatory country through its domestic laws. Section one of the chapter covers substantive criminal law while section two examines measures at the procedural level.

The most controversial arguments against the treaty concern the debate over what sort of laws will be enacted domestically. This section has produced some of the most fervor because it allows countries to enact new criminal regulations without guidance or prediction as to how these regulations will impact the general population of computer users.

Articles 2 through 10 discuss the first aspect of the treaty: the enactment of substantive criminal laws, broken up into five titles. The first four deal with types of criminal offences: (1) those against the "confidentiality, integrity and availability of computer data and systems,"[64] (2) "computer-related offences",[65] (3) "content-related offences"[66] and (4) "copyright offences."[67] Title five covers ancillary liability and sanctions.

These nine articles appear as an entire treaty in themselves.[68] Although nine offenses are listed, the draft convention actually enacts only four new cybercrimes[69] and mandates that new and additional forgery and fraud laws be added for com-

58 Recommendation No. R. (89), *supra* note 17. Recommendation No. R. (95), *supra* note 18.

59 Recommendation No. R. (85) 10 of the Committee of Ministers Concerning the Practical Application of the European Convention on Mutual Assistance in Criminal Matters in Respect of Letters Rogatory for the Interception of Telecommunications, *available at* http://cm.coe.int/ta/rec/1985/85r10.htm (June 28, 1985).

60 Recommendation No. R. (88) 2 of the Committee of Ministers on Measures to Combat Piracy in the Field of Copyright and Neighbouring Rights, *available at* http://cm.coe.int/ta/rec/1988/88r2.htm (Jan. 18, 1988).

61 *Cybercrime Treaty Final Draft*, *supra* note 47, at preamble.

62 *Specific Terms of Reference*, *supra* note 20.

63 *CDT Comments*, *supra* note 50.

64 *Cybercrime Treaty Final Draft*, *supra* note 47, at arts. 2–6.

65 *Id.* at arts. 7–8.

66 *Id.* at art. 9.

67 *Id.* at art. 10. The discussion on copyright will not be developed because it is outside the scope of privacy rights and is dealt with exclusively under a separate international treaty. It is the brief opinion of this article that new laws related to copyright are duplicative, and already quite controversial, and therefore, should be rethought in both a national and international context. *See generally* Gaylen Duncan, *Letter Regarding the Draft Council of Europe Convention on Cyber-Crime*, *at* http://www.cdt.org/international/cybercrime/001023itac.shtml. *CDT Comments*, *supra* note 50 (stating that intellectual property protection is an extremely complicated issue that touches upon both free expression and privacy issues and that is still in flux"); *Global Internet Liberty Campaign*, *supra* note 50 (arguing that "new criminal penalties should not be established by international convention in an area where national law is so unsettled").

68 *CDT Comments*, *supra* note 50 (noting that arts. 2–10 create a criminal law treaty).

69 Articles 2 through 5 include illegal access, illegal interception, data interference and system interference, respectively. "Offences against the confidentiality, integrity and availability of computer data and systems." *Cybercrime Treaty Final Draft*, *supra* note 58, at title 1.

puter crime.[70] A separate substantive offense for the misuse of devices also appears in this section.[71]

1. *New Cybercrimes*[72]

McConnell International reported that many countries do not prohibit cybercrimes.[73] Crimes concerning illegal access, interference and interception are being slowly implemented and are sparsely recognized. The treaty would correct this trend and require enactment of legislation to help combat cybercrime by allowing the heightened enforcement and prosecution of hacking.

a. *Article 2 and Illegal Access*

Article 2 states that it shall be unlawful to intentionally access in whole or in part another's computer system without right.[74] This provision, in effect, allows a nation to prosecute those that tamper with the means to enter a network or another's computer even if not actually entered. For example, a hacker that merely accesses a part of that system, such as a security program that allows entry, could be charged under a country's laws for access without right.

An endnote in the treaty defines "without right" stating that the expression should derive from its context under principles of the signatory country's laws. Essentially, (criminal) behavior conducted without the authority to do so. Countries are permitted to define what is "without right" based on their abilities to "maintain public order, protect national security or investigate criminal offences."[75] The Center for Democracy and Technology has argued persuasively against this endnote saying:

> "that what is not permitted is prohibited. In addition, the treaty would make violations of a service provider's terms of service into a criminal offense. The ISP subscriber who uses the service for a purpose prohibited by the terms of service is accessing the computer of the ISP 'without right.' The student who uploads or downloads a single music file in violation of the university's policy for granting students Internet access is committing a crime. If an employer tells its employees that they cannot use the Internet at work for personal purposes, the employee who logs on and checks a stock quote is committing an offense. Conversely, even though the treaty establishes a separate crime of 'illegal interception,' the phrase 'without right' appears there also, and would protect the ISP or service provider whose terms of service reserve the right to randomly or systematically read the communications of its subscribers."[76]

One should not be able to access another's computer system in whole or in part without a right do so. This is clear. However, this prohibition involves designating and defining who has the right to access and who does not. Some "hackers" are genuine security professionals that possess the right to access and may be performing "routine Internet functions such as security testing, price comparisons and automatic data collection."[77] Therefore, there are concerns over what sort of access is allowed and what would be prosecuted. Does the language of Article 2 allow a nation to outlaw security testing and security tools?[78] The drafters have attempted to clarify this point in their explanatory memorandum citing specific types of activity that constitute acceptable access and those that are unacceptable.[79] The memorandum attempts to draw a dividing line between acceptable and unacceptable access. It states that ar-

---

70 *Id.* at title 2.

71 *Id.* at art 6. (covering "[o]ffences against the confidentiality, integrity and availability of computer data and systems").

72 This comment only covers the controversial arguments of Chapter Two, which include illegal access and the misuse of devices.

73 *Cyber Crime. . .and Punishment? Archaic Laws Threaten Global Information*, MCCONNELL INTERNATIONAL, *at* http://www.mcconnellinternational.com/services/CyberCrime.htm (Dec. 2000) [hereinafter *Archaic Laws*] (arguing that the growing danger of cybercrime and the minimal protection offered by nations mandate that a model approach to law is needed to promote a secure environment for e-commerce).

74 *Cybercrime Treaty Final Draft*, *supra* note 47, at art. 2.

75 Explanatory Memorandum Related Thereto, Eur. Comm. on Crime Problems, at http://conventions.coe.int/treaty/en/projets/FinalCyberRapex.htm (June 29, 2001) [hereinafter Explanatory Memorandum].

76 *CDT Comments*, *supra* note 50.

77 *Comments of NetCoalition*, *supra* note 15.

78 An early concern was that security testing could be criminalized. *See Wessling*, *supra* note 33 (stating that such laws for those that test security "will make your job a lot more difficult," referencing a website forum for security professionals). This statement was made when the draft treaty was not yet released.

79 Explanatory Memorandum, *supra* note 75, at ¶ 62. This question raises larger concerns over whether a government should have oversight over this profession by implementing licensing and certification schemes similar to those that apply to attorneys, physicians or even to hairstylists. *See* Stevan D. Mitchell & Elizabeth A. Banker, *Private Intrusion Response*, 11 HARV. J.L. & TECH. 699, 716–719 (1998) [hereinafter Mitchell & Barker] (advocating licensing as "a novel venue for cooperation and compromise" for both government and industry oversight to deal with crimes of intrusion).

ticles 2 through 5 should not be construed to criminalize common Internet activities and those activities "inherent in the design of the networks or common operating or commercial practices."[80] Examples of acceptable activities include:

> sending electronic mail without it having been first solicited by the recipient; accessing a web page or ftp ("file transfer protocol") server that has been configured for public access; using hypertext links, including deep-links; or employing programs such as "cookies" or "bots" to locate and retrieve information where such programs can be filtered or rejected by the receiving server.[81]

These paragraphs are a good beginning to a clear set of guidelines, but the treaty soon becomes less specific with regard to the limitations of law enforcement and more specific with which laws should be enacted.

b. *Article 6 and the Misuse of Devices*

Controversy surrounds Article 6. Each signatory country would be required to outlaw the use of any device used in the commission of the previous five offenses. That is, one that used a cyber-device to access or interfere with another's network would be guilty of misusing the device and guilty of possession.[82] Possession or use of computer passwords or access codes also carries a penalty[83] for such items are the keys to the virtual door.

This article in effect outlaws the misuse of hacking devices or any devices used to gain access to another's system. Security analysts responding to Article 6 fear that such language could be construed as outlawing all attempts of hacking, even if the purpose is to test for security reasons.[84] Other critics fear that the article's language has a potential for over-inclusive definitions as to what operational methods constitute an illegal misuse of a device.

Article 6(1)(a) states that one cannot produce, sell or make available a device designed to commit one of the previous five offenses. The scenario is that a person could not sell or distribute a device that could "hack" or be used to help another device "hack" into an unauthorized and unowned computer system. Software that could access security or hardware that can be used to physically connect to another computer could potentially be outlawed as a "misuse of a device." A parallel example of outlawing the tools of a criminal intrusion is a law that forbids the possession or use of a "Slim Jim" used to open locked vehicles. The key is that possession, use, sales or any sort of distribution of such tools would be a criminal act subject to penalty. Article 6 also applies to the production and distribution of such tools, including their manufacture and retail. One would be prohibited from sharing with another if such device came under the legal definition of "adapted primarily for the purpose of committing any of the offences [previously] established . . ."[85]

Critics also fear that the vague language of Article 6 could lead to the banning of various devices, prohibiting their positive uses if a nation so desired. The treaty drafters have provided an exception to help quell these fears, stating that security analysis will not be outlawed.[86] As drafted, the

---

80 *Id.*

81 *Id.* at ¶ 48.

82 *Cybercrime Treaty Final Draft, supra* note 58, at art. 6, sec. 1.

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right: (a) the production, sale, procurement for use, import, distribution or otherwise making available of: (1) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2–5; (2) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2–5; and (b) the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2–5. A Party may require by law that a number of such items be possessed before criminal liability attaches. *Id.*

83 It should be noted that the treaty calls for outlawing certain cyber activities and does not institute penalization or sentencing guidelines.

84 *See Wessling, supra* note 33. *See Saniford, supra* note 45. *See* SLASHDOT GENERAL DISCUSSION, EUROPEAN CYBERCRIME TREATY 1.1, *at* http://slashdot.org/yro/00/11/13/1828213.shtml (Nov. 13, 2000); *see* Brian Krebs, *Tech Groups Still Wary of International Cyber-Crime Treaty*, NEWSBYTES, *at* http://www.computeruser.com/clickit/printout/news/30303936000335392O.html (Dec. 1, 2000).

85 *Cybercrime Treaty Final Draft, supra* note 47, at art. 6(1)(a)(1). Article 6(1)(b) specifies that a nation may, but does not have to, make possession with intent a separate offense.

86 *Id.* at art. 6(2). "This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence estab-

treaty states that nothing should be interpreted as imposing criminal liability on "authorized testing or protection of a computer system."[87] Another section reserves the right for signatories not to pass legislation criminalizing the distribution of offending devices.[88]

The underlying problem with this exception is defining and correctly understanding who has the right to possess and to use the "tool." The language of the treaty suggests that devices used *primarily* to commit cyber offenses would be banned from the general public except those used by security professionals (including law enforcement). But a counter argument is that security professionals use these devices primarily to *test* their own systems.[89] The security professional would be authorized to do this, but access to the device that helps him or her test the defending system may be unavailable in the territory of a signatory country. The problem is that even the most offensive of hacking devices are used and created by those that are not authorized to use them.[90] Common household users wishing to protect their systems privately, but not wanting to intrude upon others, could face the possibility of not having access to these devices in defense of their own networks.

Although certain legal scholarship has begun to opt for licensing measures that would certify those able to use security tools,[91] those that actually use the devices are skeptical. A website discussion on the treaty revealed that many security professionals believe that "it simply makes no sense to draft an international law banning the tools that help us secure systems. Of course, we would love some more enforcement power to use against potential crackers, but not if it is a trade off for our tools."[92] Despite this, other commentators argue that governments have the right to protect their citizens against the growing problem of cybercrime.

2. *Intrusion, Surveillance and Privacy Rights*

Privacy concerns are at their zenith.[93] As easily as technology allows a hacker to intrude upon another's network so too does the treaty permit a law enforcement officer to use the same technologies and employ the same methods of intrusion, but for different purposes. Thus, privacy and procedural laws are inextricably linked. For instance, American law once held that wiretapping was not tantamount to a search and seizure under the Fourth Amendment.[94] The opposite is true today,[95] but notions of search and seizure, wiretapping and surveillance have become more commonplace.[96]

Section 2 of the treaty deals with the procedural laws to be enacted by each signatory country. The provisions deal with issues ranging from the scope and safeguards of the laws to the actual allowance of search and seizure and data interception.

a. *Article 14 and the Scope of Procedure*

Article 14 of the draft treaty provides that signatories create or modify their prior procedural laws for the purpose of "specific criminal investiga-

lished in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system."

87 *Id.*

88 But, a nation may not reserve the right to exclude devices that make available "a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed." *Id.* at art. 6(1)(a)(2). In essence, a country may criminalize devices designed to commit cyber offences, but must criminalize devices that produce or distribute passwords or access codes.

89 *Wallace, supra* note 49.

90 Wallace's example of this is where a company arranges legitimate hacking efforts where "wargames" are held. "Wargames" invite hackers to crack the company's system to test that system. Cash rewards are given for successful attempts. "This could no longer be possible if the tools used in these wargames were made illegal to the every day user." *Id.*

91 Mitchell & Barker, *supra* note 79, at 716–719. This article discusses the future of effective cyber crime enforcement through coordinated efforts of both the public and private sectors. The authors advocate licensing as "a novel venue for cooperation and compromise." *Id* at 732.

92 Iamsure (web pseudonym), *European Cybercrime Treaty 1.1*, SLASHDOT, *at* http://slashdot.org/yro/00/11/13/1828213_F.shtml (Nov. 13, 2000). This posting came from an unofficial discussion concerning the treaty at Slashdot.org. Slashdot.org holds itself out as "News for Nerds. Stuff that matters."

93 *See* Simon Davies, *Re-engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity, in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 143 (Philip E. Agre & Marc Rotenberg eds., 1997) (stating that opinion polls show that privacy concerns are greater now than any other time in history).

94 Olmstead v. United States, 277 U.S. 438, 464 (1928) (stating that a search under the Fourth Amendment was to be of material things).

95 *See* Katz v. United States, 389 U.S. 347, 358–59 (1967) (holding that the electronic listening and recording of a conversation in a telephone booth constituted a search and seizure under the Fourth Amendment).

96 *See* INFO-SEC, THE EUROPEAN POLICE STATE, *at* http://www.info-sec.com/law/law_020298a.html-ssi (1998) (arguing that Europol not only keeps intelligence files, but stores information concerning "gossip and slanderous allegations").

tions"[97] so that law enforcement officers may utilize certain techniques similar to other communications investigations. Article 14(2) states that procedures are to apply to three aspects of cybercrime: those offenses dealt with in the substantive portion of the draft,[98] other potential cyber-related crimes not yet specified[99] and the electronic collection of evidence.[100] In a nutshell, this article provides a broad scope as to the purpose of the later procedural provisions.

b. *Article 15 and General Safeguards*

Article 15[101] is also stated broadly, but takes a rhetorical step in the right direction. This article functions as a general protection provision stating that all implementation and procedures listed under Section 2 are safeguarded "with due regard for the adequate protection of human rights . . . as provided in applicable international human rights instruments."[102] Enactment of domestic laws under the treaty should align with the letter of other prior treaties protecting civil and criminal rights.

The language used in this article appears to protect certain rights, but what particular procedures are needed to safeguard human rights?[103] Here, the draft treaty does not specify and appears cursory and indifferent. Nations are mandated to enact specific procedural provisions, but are only generally instructed as how to balance such procedures against issues of privacy.[104] What if a signatory has a poor record of privacy protection?[105] Are they now to enact new criminal procedure legislation without revising outdated privacy techniques? If so, then Article 15 is out of alignment with the "proper balance between the interests of law enforcement and human rights"[106] for a signatory can specify what law enforcement may do, but it does not need to specify what law enforcement may not do.[107]

Article 15[108] states that the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and the 1966 International Covenant on Civil and Political Rights are to be reflected in any procedural legislation. Privacy, though, is not mentioned in the first international treaty and is scantily referenced in the latter.[109] A "General Comment" to the privacy reference states that privacy measures require that national legislation be enacted to prohibit procedu-

97 *Cybercrime Treaty Final Draft, supra* note 47, at art. 14(1). ("Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings.").

98 *Id.* at art. 14(2)(a).

99 *Id.* at art. 14(2)(b).

100 *Id.* at art. 14(2)(c).

101 *Id.* at art. 15 ("Conditions and Safeguards").

> Each Party shall ensure the establishment, implementation and application of the powers and procedures provided for in this Section are subject to the conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. *Id.*

102 Footnote 29 in the text specifies the international instruments as the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocols and the 1966 International Covenant on Civil and Political Rights. *Explanatory Memorandum, supra* note 75, at ¶ 145.

103 There is also nothing explicit in the preamble to clarify these safeguards. *Cybercrime Treaty Final Draft, supra* note 47, at preamble.

104 EUROPEAN COMM. ON CRIME PROBLEMS, FINAL ACTIVITY REPORT OF THE COMMITTEE OF THE COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE, *at* http://conventions.coe.int/Treaty/EN/projects/FinalCybercrime.htm (June 29, 2001) [hereinafter FINAL ACTIVITY REPORT]. Paragraph 145 of the Final Activity Report declares that while signatory countries shall establish procedural safeguards protecting civil rights, each country is free to implement such rights according to its laws and procedure. *Id.* at ¶ 145. This provision allows for countries *not* to implement such rights according to its "domestic law and procedures of each Party."

105 Amnesty International, an organization dedicated to promoting international human rights, has reported that police abuse is common in many European countries, including the United Kingdom, France, Bulgaria and Moldova. EUROPE - HIGHLIGHTS OF AMNESTY INTERNATIONAL REPORT 2000, *at* http://www.web.amnesty.org/web/ar2000web.nsf/reg/0f2a0631827685758025 68f2005a59da.

106 *Cybercrime Treaty Final Draft, supra* note 47, at preamble.

107 Only one safeguard is specified. Signatories are given the option of weighing the economic impacts of burdening innocent third parties before intrusive procedures implemented. *Id.* at n.30, art 15. This footnote merely states that a country *may* consider such an impact, but a nation is not required to do so.

108 FINAL ACTIVITY REPORT, *supra* note 104, at ¶ 145.

109 "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation." 1966 INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS, Article 17(1), *available at* http://www.unhchr.ch/html/menu3/b/a_ccpr.htm.

ral abuse.[110] While this Comment may provide a signatory some direction in which to enact procedural safeguards, the treaty makes only passing reference to such an important protection for it does not specifically state what privacy rights are. Article 15's concern for safeguarding human rights was never a consideration in the original public release of the draft treaty as it was not mentioned until public outcry surfaced.[111] And although the drafters have now included privacy as a concern, the "experts" are still unable to agree on an acceptable standard because European case law concerning privacy varies.[112] In other words, experts representing over forty countries, including the U.S. DOJ, can agree upon a cybercrime enforcement standard, but cannot and will not agree upon a standard of enforcement for privacy.[113]

But if a cybercrime treaty is to deal with "the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks,"[114] it needs to provide a direction for procedural protections as well as the permissions it allows. The treaty references human rights documents that do reflect the differing problems of the information age. As one organization succinctly said, "A great deal has changed since 1950. If there is a need for a treaty requiring countries to adopt certain surveillance laws, then there is also a need for an updated international standard on privacy protections for government surveillance."[115]

Traditional lawmaking often emphasizes enforcement before privacy. If digital technologies have caused a need to update international criminal law, then privacy protections enacted before these technologies emerged should be equally updated. The treaty must further explain and provide for procedural safeguards that protect the public from intrusive enforcement mechanisms, such as what constitutes excessive surveillance or by what judicial standards should a court determine a proper police search and seizure was conducted. The treaty should declare specific human rights standards as laid out in other CoE treaties.[116] Given the nature of digital information, privacy rights need clarifying before international implementation.

c. *Articles 16, 17 & 18 - Expedited Preservation of Stored Computer Data & Production Orders*

The legal status of privacy is less than other comparable rights. "Privacy can be defined as a fundamental, though not absolute, human right."[117] A reading of Articles 16 through 23 adds strength to this statement for the articles call for international legislation of criminal procedure laws. The procedural mandates range from permitting law enforcement to search and seize computer data[118] to mandating that ISPs comply with criminal investigation efforts.[119] These procedural requirements make the safeguard provisions in Article 15 seem like a castle made of sand.[120]

Articles 16 and 17 require countries to adopt laws instructing individuals or businesses to preserve data when ordered to do so by law enforcement officers.[121] For instance, ISPs allow informa-

---

110 GENERAL COMMENT TO ARTICLE 17, *available at* http://www.unhchr.ch/tbs/doc.nsf/(symbol)/CCPR+Generalcomment+16.En?OpenDocument.

111 *Cybercrime Treaty Draft 19*, *supra* note 46.

112 Declan McCullagh, *Privacy a Likely Loser in Treaty*, WIRED NEWS, *at* http://www.wired.com/news/print/0,1294,40576,00.html (Dec. 7, 2000). CoE officials have expressly stated that privacy laws across Europe are too diverse to agree upon a set standard of procedural guidelines. Yet, the same diversity regarding computer crimes can be harmonized and coordinated.

113 To allow for some credit, paragraph 148 discusses the need for signatories to consider the public interest of proprietary interests and the rights and interests of third parties when considering "the sound administration of justice." *Explanatory Memorandum*, *supra* note 75. The specificity of what is just and in the public interest is left for each country to determine.

114 *Cybercrime Treaty Final Draft*, *supra* note 47, at preamble.

115 *CDT Comments*, *supra* note 50.

116 *See* Will Knight, *Cybercrime Treaty May Conflict with UN Declaration*, ZDNET.COM, *at* http://news.zdnet.co.uk/story/0,,t269-s2083139,00.html (Dec. 12, 2000) (reporting that civil liberty groups have actively criticized the draft treaty for not developing a framework more aligned with the United Nations Declaration on Human Rights).

117 David Banisar & Simon Davies, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, 18 J. MAR. J. COMPUTER & INFO L. 1, 8 (1999).

118 *Cybercrime Treaty Final Draft*, *supra* note 47, at art. 19. ("Search and Seizure of Stored Computer Data").

119 *Id.* at arts. 16–18.

120 And we all know that "castles made of sand melt into the sea, eventually." Jimi Hendrix, *Castles Made of Sand*, *on* AXIS: BOLD AS LOVE (Reprise Records 1967).

121 "Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of [specified] computer data, including traffic data, that has been stored by means of a computer system, in par-

tion to be transferred and stored through their services for the purposes of e-mail and user web pages. Law enforcement officers could get a court order forcing an ISP to preserve all data related to any investigation. If the FBI were to examine online child pornography rings, the agency could require companies such as AOL or Earthlink to preserve data related to the investigation. Such data could include bank records, credit cards or any other various financial or informational items.[122]

Article 16(2) specifies that an individual or business would be required to preserve such data transmissions for an "adequate period of time," presumably as long as a law enforcement investigation is being conducted.[123] The article further mandates that legislation shall be adopted to order those preserving the data to keep such procedures confidential.[124] In other words, an ISP preserving data at the requirement of law enforcement must do so within a certain timeframe and must not make public any information with respect to the investigation.

Article 17 goes one step further by ensuring that data is preserved regardless of the involvement of multiple service providers.[125] The article also ensures "expeditious disclosure" to a country's "competent authority,"[126] whereby all information would be turned over to law enforcement so that government officers could begin immediately tracing the transmission of data and identifying all the appropriate service providers involved.

Articles 16 and 17, as worded, storm past the fine line between criminal investigation and privacy. For example, the Internet Alliance[127] has argued that the draft treaty is at odds with the protection principles of the Data Protection Directive of the European Union ("EU").[128] This Directive was an enactment of the EU community in October 1995 asserting that data processing systems should be used to respect "fundamental rights and freedoms, notably the right to privacy."[129] The ease of processing and exchanging data was recognized as a fundamental threat to privacy since technologies could readily transport information and be susceptible to the interference of others. The argument is that without the proper procedural safeguards in place, a country could use the treaty as a means to enforce government policies unrelated to actual network intrusions, such as the identification and location of political dissidents.[130] A signatory country lacking procedural limitations could target more than cybercriminals. A signatory could track, investigate and seize information in the investigation of other unfavorable policy decisions.[131] The Internet currently provides anonymity for the politically perse-

ticular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification." *Cybercrime Treaty Final Draft, supra* note 47, at art. 16(1).

122 *CDT Comments, supra* note 50.

This provision applies to any evidence the government may want about any crime. It is not limited to communications. It applies to any data that has been stored in a computer system. Thus, any business of any kind that uses a computer can be ordered under this provision to store any data that the government might want: Bank records, credit card data, inventory data, invoices, word processing, Web surfing data. A business that has a video camera can be told to preserve the tapes. The operator of an intelligent highway system or a passkey system can be required to preserve the data on the comings and goings of vehicles and people. *Id.*

123 *Cybercrime Treaty Final Draft, supra* note 47, at art. 16(2).

Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for an adequate period of time, as necessary, to enable the competent authorities to seek its disclosure. *Id.*

124 "Each Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law." *Id.* at art 16(3).

125 *Id.* at art. 17(1)(a).

126 *Id.* at art. 17(1)(b) ("Each Party shall adopt such legislative or other measures as may be necessary to "ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.").

127 "The Internet Alliance (IA) is [an] organization of Internet policy professionals representing the Internet online industry on the state, federal and international levels." INTERNET ALLIANCE, THE INTERNET ALLIANCE: WHO WE ARE, *at* http://www.internetalliance.org/aboutisa/whoweare.html.

128 INTERNET ALLIANCE, *Internet Alliance Comments on Council of Europe's Draft Convention on Cyber-Crime No. 19, at* http://www.cdt.org/international/cybercrime/001000ia.shtml (Oct. 18, 2000) [hereinafter *Internet Alliance Comments*].

129 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281), 31 at ¶2, *available at* http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

130 *Internet Alliance Comments, supra* note 128.

131 *See AOL Removes 'Offensive' Website,* REUTERS, *at* http://

cuted, as many can express political and religious beliefs safely without fear of government sanction.

Government by itself cannot regulate and enforce. Nations need the help of those private entities that maintain the cyber architectures. Article 18 of the treaty concerns production orders and requires countries to order persons within their national boundaries to produce *any* computer data or information under that person's control.[132] The article also mandates that ISPs submit all subscriber information that pertains to citizens within a particular nation's territory.[133] The last section of Article 18 clearly defines subscriber information as any and all information that an ISP may possess.[134] This includes technical parameters of a person's system,[135] personal identifiers such as telephone numbers and billing information[136] and all information relating to an ISP's service agreement.[137] An ISP maintains certain licensing requirements that retain the right to keeping records on customer activity. In the event of a court production order, the ISP must provide assistance to law enforcement.

d. *Article 19 through 21 – Search, Seizure and Interception*

So far, this paper has established that law enforcement may, and will, be able to preserve stored computer data and force ISPs to submit to the authorities all information regarding their customers. Three more articles also intrude upon privacy by allowing law enforcement and ISPs to gather and collect information on suspected cyber offenses.

Articles 19 through 21 are the heart and soul of the treaty enforcement provisions. These articles allow for the search and seizure of stored computer data,[138] the collection and recording of computer traffic[139] and the interception of content data.[140] These articles develop procedural standards for law enforcement that increase communications monitoring without increasing privacy protections.

Article 19 reflects traditional search and seizure laws. A signatory must enact legislation that would allow law enforcement officials the ability to access any information within its territory.[141] If it is suspected that the same information lies on multiple computer systems, the draft treaty allows those systems likewise to be searched and seized.[142] The search and seizure ability includes the power to secure a computer system,[143] retain copies of any data information,[144] maintain the data so that it is not altered[145] and block accessibility or remove the data entirely.[146]

---

www.abcnews.go.com/sections/tech/DailyNews/aol_site980624.html (June 24, 1998). AOL closed down one of its websites that parodied the Koran and other Islamic customs. The country of Egypt protested, stating that the site was offensive to Muslims.

132 *Cybercrime Treaty Final Draft, supra* note 47, at art. 18(1) ("Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: (a) a person in its territory to submit specified computer data under this person's control, which is stored in a computer system or a computer-data storage medium.").

133 *Id.* at art. 18(1) ("Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: (b) a service provider offering its services in its territory to submit subscriber information under that service provider's possession or control.").

134 *Id.* at art. 18(3) ("For the purpose of this article, 'subscriber information' means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to users of its service, other than traffic or content data.").

135 *Id.* at art. 18(3)(i) ("[T]he type of the communication service used, the technical provisions taken thereto and the period of service.").

136 *Id.* at art. 18(3)(ii) ("[T]he user's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement.").

137 *Id.* at art. 18(3)(iii) ("[A]ny other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.").

138 *Id.* at art. 19.

139 *Id.* at art. 20.

140 *Id.* at art. 21.

141 *Id.* at art. 19(1) ("Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: (a) a computer system or part of it and computer data stored therein; and (b) computer-data storage medium in which computer data may be stored, in its territory.").

142 *Id.* at art. 19(2) ("Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1(a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.").

143 *Id.* at art. 19(2)(a) ("These measures shall include the power to (a) seize or similarly secure a computer system or part of it or a computer-data storage medium.").

144 *Id.* at art. 19(2)(b) ("make and retain a copy of those computer data").

145 *Id.* at 19(2)(c) ("maintain the integrity of the relevant stored computer data").

146 *Id.* at 19(2)(c) ("render inaccessible or remove those

Article 19 specifies how law enforcement may monitor data transmissions, but it leaves open possibilities for cumbersome intrusion into personal lives and business operations.[147] The draft treaty does not issue any constraining standards upon law enforcement. A suggestion would be to add a footnote explaining these standards so that businesses and individuals are not intruded upon unnecessarily.[148]

As previously noted, Articles 20 and 21 provide for domestic laws that allow law enforcement to monitor, collect and intercept data transmissions. These articles are analogous to wiretapping and surveillance procedures that are already used by law enforcement.[149] Article 20 provides that signatories empower their enforcement authorities to collect and record traffic data through "technical means."[150] Traffic data is defined under Article 1 as "any computer data relating to a communication by means of a computer system, generated by the computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying [network] service."[151] This appears to be an all-encompassing definition.

Article 21 is similar in that authorities will have the same powers over content data, as well as traffic data.[152] The two articles are virtually identical besides their different references to types of data. The treaty does not differentiate between the two types of data, for it fails to define what "content data" is. The term "content data" implies that it is a subset of "traffic data." Countries that outlaw the transmission or display of certain forms of content, such as hate speech,[153] would have a specific article to empower the interception of such transmissions. In addition, nothing in the treaty states why "content data" differs from "traffic data" and why it requires its own separate article, even though the language of the two articles are the same. A clear definition of "content data" is needed so that it can be differentiated from "traffic data" so that law enforcement has access to specific guidelines when intercepting or recording data transmissions.[154]

The linguistic problems of Articles 20 and 21 appear small, but when law enforcement is given significant surveillance and interception powers without being given sufficient guidelines concerning the intrusiveness of these powers, then definitional arguments are key. Definitions are fundamental, for the law uses definitions to separate issues of fact from issues of law.[155] One cannot legally state that content data is of the type that law enforcement may have power over if one does not know what content data is. And more importantly, if one cannot define the item that one has power over, then power becomes more centralized and general and abuse becomes harder to temper.

Summarily, Articles 19 through 21 threaten privacy because they lack specific guidelines as to the limits of interception and monitoring. Terms like "traffic data" suggest that all data may be intercepted so long as the purpose is to investigate cybercrime. Terms without definitions simply lack credibility for they are vague, over-empowering and do not provide a bright line between issues of fact and issues of law.

---

computer data in the accessed computer system").

147 *CDT Comments, supra* note 50.

148 *Id.* CDT argues that a government without restraint may shut down an ISP or web portal that contains any "seizeable" records. *Id.*

149 *See* Herman Schwartz, *The Legitimization of Electronic Eavesdropping: The Politics of "Law and Order,"* 67 MICH. L. REV. 455 (1969) (outlining an early critique of electronic monitoring).

150 *Cybercrime Treaty Final Draft, supra* note 47, at art. 20(1)(a) ("Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to (a) collect or record through application of technical means on the territory of that Party.").

151 *Id.* at art. 1(d).

152 *Id.* at art. 21(1) ("Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to (a) collect or record through application of technical means on the territory of that Party . . . [of] content data, in real-time, of specified communications in its territory transmitted by means of a computer system.").

153 France, Germany and Austria all have laws restricting hate speech and any display of such, especially that relating to the Holocaust. *See* Kathleen E. Mahoney, *Hate Speech: Affirmation or Contradiction of Freedom of Expression*, 1996 U. ILL. L. REV. 789, 801 (1996); Kenneth Lasson, *Holocaust Denial and the First Amendment: The Quest for Truth in a Free Society*, 6 GEO. MASON L. REV. 35, 72, n. 286 (1997).

154 *See Global Internet Liberty Campaign, supra* note 50 (arguing for more precise definitions of what constitutes "content data" and "traffic data").

155 Gerard A. Hauser, INTRODUCTION TO RHETORICAL THEORY 82–83 (1986).

IV. CONCLUSION: THE DRAFT TREATY CANNOT BE SIGNED

Lawrence Lessig states "that there is a decision to be made about the architecture that cyberspace will become, and the question is how that decision will be made. Or better, *where* will the decision be made."[156] This question is being answered all too quickly, and the resounding response is being met with widespread difficulty. Government officials are concerned with the threats of cybercrime and the rising costs of investigation.[157] Privacy is not a strong concern.

The chairman of the PC-CY has baldly asserted, "We cannot find an acceptable international standard in terms of privacy as it applies to this treaty."[158] In other words, European privacy laws are so diverse that a common ground upon which to agree is difficult. The cybercrime treaty was first implemented because the cyber laws across Europe *are* so different.

Without specific protections for privacy rights, nations may well enforce new standards of enforcement with little concern for outdated standards on privacy. The Council of Europe and the Department of Justice need to clarify the vague items that remain.[159] Although the U.S. has signed the treaty as written, it has not ratified the treaty into law and should not do so without further revision.

---

156 Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1411 (1996) (posing several questions about the current unregulation of cyberspace and what the potential bordering of cyberspace may become).

157 *Freeh Statement on Cybercrime, supra* note 7.

158 Declan McCullagh & Nicholas Morehead, *Privacy a Likely Loser in Treaty*, WIRED NEWS, *at* http://www.wired.com/news/print/0,1294,40576,00.html (Dec. 7, 2000) (quoting Henrik Kaspersen of the Council of Europe and chair of PC-CY stated at a panel debate hosted by McConnell International). Henrik Kaspersen has stated that those protesting the treaty either are American lawyers who do not understand European law or "Internet users." It can be assumed that this reference to "Internet users" may mean those people who use sophisticated communications but have sub-par understanding of international issues. This is an interesting comment from a party that is receiving tremendous legal advice from the U.S. DOJ.

159 The DOJ needs to also explain the treaty's impact on U.S. law.