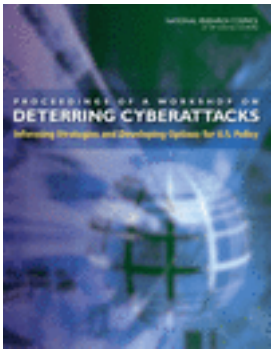

Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council

ISBN: 0-309-16086-3, 400 pages, 8 1/2 x 11, (2010)

The Council of Europe Convention on Cybercrime

Michael A. Vatis
Steptoe & Johnson LLP

I. BACKGROUND

The Convention on Cybercrime is an international treaty that seeks to harmonize national laws on cybercrime,[1] improve national capabilities for investigating such crimes, and increase cooperation on investigations.[2] The Convention was drafted by the Council of Europe (COE) in Strasbourg, France.[3] In addition to COE Member states, Canada, Japan, South Africa, and the United States participated in the negotiation of the Convention as observers.[4] The U.S., despite its official "observer" status, played an especially influential role, in part because it had more experience than other countries in addressing cybercrime and entered the process with well-formulated positions.[5]

[1]By "cybercrime" I mean those computer-related offenses specifically prescribed by the Convention, as discussed below in Part II.A.

[2]The Convention is available on the website of the Council of Europe at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; accessed July 30, 2010.

[3]The Council of Europe comprises 47 member States, including all 27 members of the European Union (Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom) plus Albania, Andorra, Armenia, Azerbaijan, Bosnia and Herzegovina, Croatia, Georgia, Iceland, Liechtenstein, Moldova, Monaco, Montenegro, Norway, Russia, San Marino, Serbia, Switzerland, The Former Yugoslav Republic of Macedonia, Turkey, and Ukraine. *See* Council of Europe website, available at http://www.coe.int/aboutCoe/index.asp?page=47pays1europe&l=en; accessed June 5, 2010. The COE was established in 1949 primarily as a forum to uphold and strengthen human rights, and to promote democracy and the rule of law in Europe. Over the years, the CoE has been the negotiating forum for a number of conventions on criminal matters in which the United States has participated. Non-European states may also participate in activities of the COE as observers.

[4]*See* Convention on Cybercrime, Explanatory Note ¶ 304, available at http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm; accessed June 6, 2010. Other states that have been invited to accede to the Convention, but have not yet signed or ratified it, are Chile, Costa Rica, the Dominican Republic, Mexico, and the Philippines. *See* Council of Europe website, available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=02/06/2010&CL=ENG; accessed June 6, 2010.

[5]*See, e.g.*, Computer Crime and Intellectual Property Section, U.S. Department of Justice, *Council of Europe Convention on Cybercrime Frequently Asked Questions and Answers*, available at http://www.cybercrime.gov/COEFAQs.htm#QA2; accessed June 7, 2010 ("The United States, represented by the Departments of Justice, State and Commerce, in close consultation with other U.S. government agencies and interested private parties, actively participated in the negotiations in both the drafting and plenary sessions, working closely with both CoE and non-CoE member States. Because the provisions in the Convention were generally adopted by consensus both in the drafting and plenary groups, rather than by member State vote, the United States had a real

One critical, but often overlooked, aspect of the Convention is that many of its procedural provisions are not limited to cybercrimes. Rather, they extend to *any* crimes for which it is necessary to collect evidence "in electronic form."[6] Thus, the Convention obliges ratifying states to create laws allowing law enforcement to search and seize computers and "computer data," engage in wiretapping, and to obtain real-time and stored communications data, whether or not the crime under investigation is a cybercrime.[7] In many ways, then the "Convention on Cybercrime" is a misnomer—or is at least a misleadingly narrow description of the Convention's substance.

The origins of the Convention date back to November 1996, when the European Committee on Crime Problems (CDPC) recommended that the COE set up an experts committee on cybercrime.[8] From the beginning, the CDPC recognized that "[t]he trans-border character of [cyber-space] offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities."[9] Accordingly, the CDPC opined then, "a concerted international effort is needed to deal with such" crimes, and "only a binding international instrument can ensure the necessary efficiency in the fight against these new phenomena."[10]

Following the CDPC's advice, the COE Committee of Ministers, in February 1997, established the "the Committee of Experts on Crime in Cyber-space."[11] The Committee of Experts' charge was to examine the following subjects and to draft a "binding legal instrument" addressing them, "as far as possible"

- "cyber-space offences, in particular those committed through the use of telecommunication networks, e.g. the Internet, such as illegal money transactions, offering illegal services, violation of copyright, as well as those which violate human dignity and the protection of minors";
- "other substantive criminal law issues where a common approach may be necessary for the purposes of international co-operation such as definitions, sanctions and responsibility of the actors in cyber-space, including Internet service providers";

---

voice in the drafting process."); J. Martin, U.S. Department of Justice, *The United States Experience* 1 (November 19, 2001) (The U.S. participated in negotiations in part "because we believed that given our long history with cyber crime, and our role in the development of networked communications systems, we could make valuable contributions to the negotiations."); ibid. at 5 ("During the negotiations, the U.S. delegation met frequently with representatives from industry and privacy groups, as well as interested individuals, to listen to their concerns and encourage an open process.").

The U.S. strongly supported inclusion in the Convention of the provisions to "create expedited channels of communication between countries and to reduce the number of hurdles required to exchange information," including: the 24/7 points-of-contact network; the requirements to preserve evidence without requiring dual criminality; and the requirement of expedited cooperation "not only for crimes committed by and against computers, but also for any crime involving electronic evidence." Ibid. at 4. The U.S. also "opposed measures that would permit countries to place untenable conditions on the exchange of information between law enforcement agencies, . . . proposals that would have required industry to deploy new technologies to assist law enforcement, or to routinely collect and retain data for long periods of time[,] . . . definitions of offense that were too general, thereby inadvertently creating criminal liability for legitimate commercial activities[,] . . . and measures that require the private sector to destroy critical evidence." Ibid. at 4-5. In addition, the U.S. sought the inclusion of the "federal clause," whereby Parties "may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities," thus making clear that such constituent States or territories are not each bound by the Convention. Art. 41. *See* J. Martin, *supra*, at 6.

[6]*See* Convention on Cybercrime, Art. 14(2)(c). *See also* Convention on Cybercrime, Explanatory Note ¶ 141 ("The Convention makes it explicit that Parties should incorporate into their laws the possibility that information contained in digital or other electronic form can be used as evidence before a court in criminal proceedings, irrespective of the nature of the criminal offence that is prosecuted.").

[7]*See* Convention on Cybercrime, Arts. 18-21.

[8]*See* Convention on Cybercrime, Explanatory Report, ¶ 7. The CDPC is a COE committee that advises the COE's Committee of Ministers on crime problems. The Committee of Ministers comprises the Foreign Ministers of all the COE's Member states, and acts as the COE's decision-making body. *See* Council of Europe website, available at http://www.coe.int/t/cm/aboutCM_en.asp#P25_338; accessed June 6, 2010.

[9]Convention on Cybercrime, Explanatory Report, ¶ 8.

[10]Ibid., ¶ 9.

[11]*See* ibid., ¶ 12.

- "the use, including the possibility of transborder use, and the applicability of coercive powers in a technological environment, e.g. interception of telecommunications and electronic surveillance of information networks, e.g. via the Internet, search and seizure in information-processing systems (including Internet sites), rendering illegal material inaccessible and requiring service providers to comply with special obligations, taking into account the problems caused by particular measures of information security, e.g. encryption";
- "the question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (*locus delicti*) and which law should accordingly apply, including the problem of *ne bis idem* in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts"; and
- "questions of international co-operation in the investigation of cyber-space offences. . . ."[12]

The Committee of Experts negotiated and drafted the text of the Convention (and its Explanatory Report) over the next four years, culminating in the final draft that was approved by the CDPC in June 2001 and then adopted by the COE's Committee of Ministers on November 8, 2001. The Convention was then submitted for signature by Member states and observer states in Budapest, Hungary on November 23, 2001.[13]

The Convention, by its own terms, would not take force until five nations had ratified it, including three COE Member states.[14] That occurred on July 1, 2004, after Lithuania had ratified it.[15] (Albania, Croatia, Estonia, and Hungary had already ratified the Convention, in that order.)[16] As of June 5, 2010, 29 nations have ratified the Convention.[17] Seventeen other states have signed the Convention but not ratified it.[18] The United States signed the treaty on November 23, 2001, and ratified it on September 29, 2006.[19] The Convention entered into force in the U.S. on January 1, 2007.[20]

The Convention is open to signature and ratification by any COE member states and any non-Member states that "have participated in its elaboration."[21] Additional states may be invited by the

[12]Ibid., ¶ 11.

[13]*See* Council of Europe website, available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CM=8&DF=02/06/2010&CL=ENG; accessed June 5, 2010.

[14]*See* Convention on Cybercrime, Art. 36.

[15]*See* COE, Convention on Cybercrime website, available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=02/06/2010&CL=ENG; accessed June 5, 2010.

[16]*See* ibid.

[17]The states that have ratified the Convention as of June 5, 2010, are: Member states Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, The Former Yugoslav Republic of Macedonia, and Ukraine, and non-Member state the United States of America. *See* ibid.

[18]The states that have signed but not yet ratified the convention are: Member states Austria, Belgium, Czech Republic, Georgia, Greece, Ireland, Liechtenstein, Luxembourg, Malta, Poland, Spain, Sweden, and Switzerland, and United Kingdom, and participating non-Member states Canada, Japan, and South Africa. Ibid. Five Member states (Andorra, Monaco, Russia, San Marino, and Turkey) and five non-Member states (Chile, Costa Rica, Dominican Republic, Mexico, and Philippines) have not signed the Convention. *See* ibid.

[19]*See* ibid. The United States made a number of technical declarations and reservations in its instrument of ratification. The declarations and reservations of all the ratifying states, including the United States, can be found on the COE, Convention of Cybercrime website, available at http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=185&CM=8&DF=02/06/2010&CL=ENG&VL=1; accessed July 30, 2010.

[20]*See* COE, Convention on Cybercrime website, available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=02/06/2010&CL=ENG; accessed June 5, 2010. The U.S. Department of Justice and the U.S. Senate took the position that the Convention required no implementing legislation in the United States, since "[a]n existing body of federal laws will suffice to implement the obligations of the Convention, although some minor reservations and declarations are needed." U.S. Sen., Exec. Rpt. 109-6, *Council of Europe Convention on Cybercrime (Treaty Doc. 108-11)* at 6 (November 8, 2005). *See also* Statement of Attorney General Alberto R. Gonzales on the Passage of the Cybercrime Convention (August 4, 2006) ("The Convention is in full accord with all U.S. constitutional protections, such as free speech and other civil liberties, and will require no change to U.S. laws."), available at http://www.justice.gov/opa/pr/2006/August/06_ag_499.html; accessed June 7, 2010.

[21]*See* Convention on Cybercrime, Art. 36.

COE's Committee of Ministers to accede to the Convention, after the Committee consults with and obtains the unanimous consent of "the Contracting States to the Convention."[22]

On November 7, 2002, the Committee of Ministers adopted the Additional Protocol to the Convention on Cybercrime.[23] The Additional Protocol requires ratifying Member States to pass laws criminalizing "acts of racist or xenophobic nature committed through computer networks." This includes the dissemination of racist or xenophobic material, the making of racist or xenophobic threats or insults, and the denial of the Holocaust and other genocides. It also commits ratifying nations to extend to these crimes the investigative capabilities and procedures created pursuant to the main Convention.

The Additional Protocol opened for signature on January 28, 2003. It came into force on March 1, 2006, after 5 states had ratified it.[24] As of June 5, 2010, 17 states have ratified the Additional Protocol.[25] Another 17 nations have signed but not ratified it.[26] The United States participated in the drafting of the protocol but did not sign it because of concerns that it was inconsistent with guarantees of the United States Constitution.[27] Ratification of the main Convention does not oblige a ratifying state to take any action under the Additional Protocol.

II. THE CONVENTION'S PROVISIONS

The Convention states as its goal the "protection of society against cybercrime" by "providing for the criminalisation of such conduct . . . and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation."[28] The Convention is divided into three principal parts. The first part addresses the substantive cybercrime offenses that each ratifying state is obliged to adopt in its national law. The second part concerns investigative procedures the states must implement. And the third part relates to mechanisms to enhance international cooperation.

A. Cybercrime Offenses

The Convention requires Parties (*i.e.*, ratifying states) to "adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally"[29]:

---

[22]*See* ibid., Art. 37.

[23]The Additional Protocol is available at http://conventions.coe.int/Treaty/EN/Treaties/html/189.htm; accessed June 6, 2010. The Explanatory Report accompanying the Additional Protocol is available at http://conventions.coe.int/Treaty/EN/Reports/Html/189.htm; accessed June 6, 2010.

[24]*See* COE, Convention on Cybercrime website, available at http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=189&CM=8&DF=05/06/2010&CL=ENG; accessed June 5, 2010.

[25]The following Member states have ratified the Additional Protocol: Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, France, Latvia, Lithuania, Montenegro, Norway, Portugal, Romania, Serbia, Slovenia, The Former Yugoslav Republic of Macedonia, and Ukraine. *See* ibid.

[26]The 17 nations that have signed but not ratified the Additional Protocol are: Member states Austria, Belgium, Estonia, Finland, Germany, Greece, Iceland, Liechtenstein, Luxembourg, Malta, Moldova, Netherlands, Poland, Sweden, and Switzerland, and participating non-Member states Canada and South Africa. Seventeen participating states have not signed the Additional Protocol: Member states Andorra, Azerbaijan, Bulgaria, Czech Republic, Georgia, Hungary, Ireland, Italy, Monaco, Russia, San Marino, Slovakia, Spain, Turkey, and United Kingdom, and participating non-Member states Japan and the United States of America. *See* ibid.

[27]*See* U.S. Department of Justice, Computer Crime and Intellectual Property Section, *Council of Europe Convention on Cybercrime, Frequently Asked Questions and Answers*, available at http://www.justice.gov/criminal/cybercrime/COEFAQs.htm; accessed June 5, 2010.

[28]Convention on Cybercrime, Preamble.

[29]The Convention also obligates Parties to criminalize intentional aiding and abetting of the offenses described in the text. *See* ibid., Art. 11. In addition, the Convention requires Parties to enact measures holding corporations criminally, civilly, or administratively liable for any listed offenses committed by an individual "who has a leading position" in the corporation and commits

- "the access to the whole or any part of a computer system without right"[30];
- "the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data"[31];
- "the damaging, deletion, deterioration, alteration or suppression of computer data without right"[32];
- "the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data"[33];
- "the production, sale, procurement for use, import, distribution or otherwise making available of," or the possession of: "a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences [described above]," or "a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed," where the action is taken "without right" and "with intent that it be used for the purpose of committing any of the offences [described above]"[34];
- "the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic," when done "without right"[35];
- "the causing of a loss of property to another person by . . . any input, alteration, deletion or suppression of computer data . . . [or] any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person," when done "without right"[36];
- the production for the purpose of distribution, the offering or making available; the distribution or transmission, the procurement, or the possession of child pornography on or through a computer system, when done "without right."[37]

---

the offense for the benefit of the corporation. *See* ibid., Art. 12(1). Parties must also provide for the liability of a corporation where "the lack of supervision or control" by a person with "a leading position" in the corporation allows another person under the authority of the corporation to commit one of the listed offenses. *See* ibid., Art. 12(2).

[30]Ibid., Art. 2. However, "[a] Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system." Ibid.

The term "without right" is meant to "refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law." Convention on Cybercrime, Explanatory Report ¶ 38. In particular, the Convention "leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised." Ibid.

[31]Ibid., Art. 3. However, "[a] Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system." Ibid.

[32]Ibid., Art. 4. However, "[a] Party may reserve the right to require that the conduct . . . result in serious harm." Ibid.

[33]Ibid., Art. 5.

[34]Ibid., Art. 6(1). However, "[a] Party may require by law that a number of such items be possessed before criminal liability attaches" on the basis of possession of one of the listed items. Ibid., Art. 6(1)(b). In addition, a Party may reserve the right not to enact into law any of the offenses described in this Article other than those concerning "the sale, distribution or otherwise making available of a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed." Ibid., Art. 6(3).

[35]Ibid., Art. 7.

[36]Ibid., Art. 8.

[37]Ibid., Art. 9. "Child pornography" is defined as including "pornographic 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; or 3) realistic images representing a minor engaged in sexually explicit conduct." Ibid., Art 9(2). However, each Party may reserve the right not to criminalize all offenses concerning the procurement or possession of child pornography. Ibid., Art. 9(4). In addition, a Party may reserve the right not to criminalize the listed activities if they involve a person appearing to be a minor engaging in sexually explicit conduct, or realistic images of a minor engaging in such conduct, if the material does not actually involve a minor. Ibid.

The Convention also requires Parties to criminalize the "willful" infringement of copyright and related rights when done "on a commercial scale and by means of a computer system."[38] In addition, Parties must ensure that all of the listed offenses "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty."[39]

B. Investigative Procedures

The second principal part of the Convention requires Parties to enact certain procedural mechanisms and procedures to facilitate the investigation of cybercrimes or any crimes committed with a computer or for which evidence may be found in "electronic form."[40] The provisions in this part require states to "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 order to give authorities the opportunity to seek disclosure of the data[41];
- with respect to preserved traffic data about a communication, "ensure the expeditious disclosure to the Party's competent 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"[42];
- empower its authorities to order "a person in its territory" to produce "specified computer data in that person's possession or control,"[43] and to order "a service provider offering its services in the territory of the Party" to produce "subscriber information relating to such services"[44];

[38]Ibid., Art. 10. A Party may reserve the right, however, not to criminalize such acts "in limited circumstances," as long as "other effective remedies are available" and the reservation does not derogate from the Party's obligations under other international agreements. Ibid., Art. 10(3). Copyright infringement was included in the Convention because "copyright infringements are one of the most widespread forms of computer- or computer-related crime and its escalation is causing international concern." Convention on Cybercrime, Explanatory Report ¶ 35.

[39]Convention on Cybercrime, Art. 13(1). For corporations, such punishment must include "monetary sanctions." *See* ibid., Art. 13(2).

[40]Specifically, the Convention requires that these procedures be available to investigate the substantive offenses described in the Convention, "other criminal offences committed by means of a computer system," and "the collection of evidence in electronic form" of any type of criminal offense. Ibid., Art. 14(2).

The Convention also requires that these mechanisms and procedures include "conditions and safeguards" necessary "for the protection of human rights and liberties," including "judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure." Ibid., Art. 15.

[41]Ibid. Art. 16. If a Party implements this requirement "by means of an order to a person to preserve specified stored computer data in the person's possession or control," such order shall require preservation of the data "as long as necessary, up to a maximum of ninety days," with the preservation period subject to renewal. Ibid., Art. 16. Parties must also ensure that the person directed to preserve the data keeps the undertaking confidential. *See* ibid., Art. 16.

[42]Ibid., Art. 17.

[43]Ibid., Art. 18. The drafters of the Convention intended that data within a person's "possession or control" not be limited to data that is stored in the territory of the state. "The term 'possession or control' refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute 'control' within the meaning of this provision." Convention on Cybercrime, Explanatory Note ¶ 173.

[44] Convention on Cybercrime, Art. 18. "Subscriber information" means "subscriber information" means any information held by a service provider "relating to subscribers of its services other than traffic or content data," and which relates to "the type of communication service used" and technical aspects of the service; the "period of service"; "the subscriber's identity," address, "telephone and other access number"; "billing and payment information"; and "any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement." Ibid., Art. 18(3).

- "empower its competent authorities to search or similarly access" and to seize "a computer system" or a "computer-data storage medium" in its territory, and to search and seize data stored therein[45];
- empower its authorities to "collect or record through the application of technical means" on its territory, "traffic data, in real-time, associated with specified communications in its territory[46] transmitted by means of a computer system," or to "compel a service provider, within its existing technical capability,"[47] to do the same or to cooperate and assist the authorities' own collection or recording"[48];
- empower its authorities, in the case of "serious offences," to "collect or record through the application of technical means" on its territory "content data, in real-time, of specified communications in its territory transmitted by means of a computer system," or to "compel a service provider, within its existing technical capability," to do the same or to cooperate with the authorities' own collection or recording[49];
- establish jurisdiction over any of the substantive offenses set forth in the Convention that are committed in the state's territory[50]; and

[45]Ibid., Art. 19(1). Parties must also ensure that if their authorities search a computer system and then have reason to believe that the data they are seeking is stored in another system in the state's territory and that "such data is lawfully accessible from or available to the initial system," the authorities "shall be able to expeditiously extend the search . . . to the other system." Ibid., Art. 19(2). In addition, Parties must empower their authorities "to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the" search or seizure of the relevant computer systems or data. Ibid., Art. 19(4).

[46]The reference to "communications in its territory" (in the provisions dealing with collection of both traffic data and communications content) is meant to be expansive, and includes situations where one of the parties to a communication is in the state's territory, or where a computer through which the communication passes is in the territory. *See* Convention on Cybercrime, Explanatory Note ¶ 222 ("For the purposes of this Convention, it is understood that a communication is in a Party's territory if one of the communicating parties (human beings or computers) is located in the territory or if the computer or telecommunication equipment through which the communication passes is located on the territory.").

[47]The reference to a service provider's "existing technical capability" (in the provisions concerning both collection of traffic data and communications content) is intended to make clear that providers are not legally obliged to build or acquire the technical capability necessary to effectuate a collection order. "The article does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems. However, if their systems and personnel have the existing technical capability to provide such collection, recording, co-operation or assistance, the article would require them to take the necessary measures to engage such capability." Convention on Cybercrime, Explanatory Note ¶ 221.

[48]Convention on Cybercrime, Art. 20(1). A Party must also enact such measures as are necessary "to oblige a service provider to keep confidential the execution" of such power "and any information relating to it." Ibid., Art. 20(3). Note, however, that a Party may reserve the right to apply this authority only to the same "serious offenses" for which it authorizes real-time collection of communication content under Article 21. *See* ibid., Art. 14(3). It may also reserve the right not to apply this authority to communications on computers transmitted within a computer system that "is being operated for the benefit of a closed group of users" and "does not employ public communications networks and is not connected with another computer system." *See* ibid., Art. 14(2), (3).

[49]Ibid., Art. 21(1). A Party must also enact such measures as are necessary "to oblige a service provider to keep confidential the execution" of such power "and any information relating to it." Ibid., Art. 21(3).

[50]Ibid., Art. 22(1)). The Convention also calls on Parties to establish jurisdiction over cybercrimes committed "on board a ship flying the flag of that Party," "on board an aircraft registered under the laws of that Party," or "by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State." Ibid. However, Parties may reserve the right not to assert jurisdiction in such cases, or only in specific cases or circumstances. *See* ibid., Art. 22(2).

The Convention does not define what "committed in the state's territory" means. In the Explanatory Note accompanying the Convention, the drafters remark, "Each Party is required to punish the commission of crimes established in this Convention that are committed in its territory. For example, a Party would assert territorial jurisdiction if both the person attacking a computer system and the victim system are located within its territory, and where the computer system attacked is within its territory, even if the attacker is not." Convention on Cybercrime, Explanatory Note ¶ 233. The drafters' examples do not include—nor do they exclude—a situation where the computer system attacked is outside the state's territory but the attacker is within it. From the perspective of international cooperation, it is perhaps most critical that states extend their jurisdiction to cybercrimes that emanate from their states even if the effects are felt elsewhere, since those states will have the greatest ability to investigate the origin of the attack and to arrest the perpetrator.

- establish jurisdiction over any of the substantive offenses set forth in the Convention "in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition," and where the offense is punishable in both states by deprivation of liberty for a maximum period of at least one year.[51]

C. International Cooperation

The third principal part of the Convention sets out mechanisms by which Parties to the convention will assist each other in investigating cybercrimes and other crimes involving electronic evidence. The Convention provides that Parties "shall co-operate with each other . . . to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[52] However, this cooperation shall occur "through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws."[53] This suggests that cooperation may be limited or delayed if required by law or other arrangements. The specific cooperation measures are described below.

First, Parties must regard the substantive offenses set forth in the Convention as extraditable offenses, as long as the offense is punishable in both states by deprivation of liberty for a maximum period of at least one year, "or by a more severe penalty.[54] However, "[e]xtradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition."[55] If a Party refuses to extradite a person solely on the basis of his nationality, "or because the requested Party deems that it has jurisdiction over the offence," the requested Party must refer the case (if requested by the Party seeking extradition) to its own competent authorities "for the purpose of prosecution."[56] Such authorities "shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature."[57] But there is no requirement that the person actually be prosecuted. Rather, the Requested party must simply "report the final outcome to the requesting Party in due course."[58]

Second, Parties must "afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[59] Parties must "accept and respond to" requests made by "expedited means of communication, including fax or email, to the extent

---

The U.S. delegation to the CDPC interpreted this provision of the Convention as calling for states to assert jurisdiction over cybercrimes committed by persons within their territory against computers outside their territory. *See* K. Harris, U.S. Department of Justice, *Jurisdiction and international cooperation provisions in the Convention* 2 (Nov. 20, 2001) (paper submitted to nations considering signing the Convention) ("Since sophisticated locally based cybercriminals may also target victims in other countries, the exercise of territorial jurisdiction also plays an important role in reducing international cybercrime."). It is worth noting, too, that the U.S. Department of Justice for many years took the position that the principal American "cybercrime" law, the Computer Fraud and Abuse Act (CFAA), 18 USC. § 1030 et seq., applied to cases in which the attacker was inside the United States but the victim computers were not. But this position was not explicitly embodied in the CFAA until 2001, when the definition of "protected computer" in the CFAA was amended by the USA PATRIOT Act, Pub. L. 107-56, § 814(d)(1), so that it included a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 USC. § 1030 (e)(2)(B).

[51]Convention on Cybercrime, Art. 22(3).

[52]Ibid., Art. 23.

[53]Ibid.

[54]*See* ibid., Art. 24(1)-(4).

[55]Ibid., Art. 24(5).

[56]Ibid., Art. 24(6).

[57]Ibid.

[58]Ibid.

[59]Ibid., Art. 25(1).

that such means provide appropriate levels of security and authentication," but may require "formal confirmation to follow."[60] However, Parties may refuse cooperation on any ground provided for under its domestic law "or by applicable mutual assistance treaties," except that a Party shall not exercise its right to refuse assistance in the case of cybercrimes "solely on the ground that the request concerns an offence which it considers a fiscal offence."[61]

Third, Parties may, to the extent permitted by their domestic laws, spontaneously forward to another Party information that it has uncovered that it thinks might assist the receiving party in investigating a cyber crime.[62] Before providing such information, the "providing Party may request that it be kept confidential or only used subject to conditions. . . . If the receiving Party accepts the information subject to the conditions, it shall be bound by them."[63]

The fourth set of mutual assistance provisions applies when two Parties do not have an existing mutual legal assistance treaty or some other formal arrangement between them (or when the Parties agree to apply the Convention provision in lieu of their existing arrangement).[64] The Convention requires each Party to "designate a central authority" responsible for sending, answering, or executing requests for mutual assistance.[65] The COE Secretary General shall keep an updated register of these central authorities.[66] Parties agree to execute requests "in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party."[67] The Convention provides, however, that Parties may refuse assistance not only for reasons specified in their domestic law or in existing MLATs, but also on the ground that "the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence" or that "execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests."[68] In addition, a "requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a) kept confidential . . ., or b) not used for investigations or proceedings other than those stated in the request."[69]

Fifth, Parties must "take all appropriate measures to preserve [computer data] expeditiously" at the request of another, where such data is located in the requested Party's territory and the requesting party intends to follow up with a request to search, seize, or disclose that data.[70] Such data must be preserved

[60]Ibid., Art. 25(3).

[61]Ibid., Art. 25(4). In the Explanatory Note to the Convention, however, the drafters suggest that a Party's right to refuse cooperation is more limited than the text of the Convention suggests on its face. The Explanatory Note explains that certain provisions of the Convention must be implemented regardless of existing domestic laws or treaties, such as the obligation "to provide for the forms of co-operation set forth in the remaining articles of the Chapter (such as preservation, real time collection of data, search and seizure, and maintenance of a 24/7 network)." Convention on Cybercrime, Explanatory Note ¶ 258. Though the meaning of this statement is far from pellucid, it appears that Parties must implement "the forms of cooperation" required by the Convention, but they may refuse to actually cooperate if doing so would violate the terms of their domestic laws or existing treaties (or if non-cooperation is expressly allowed by some specific provision of the Convention, such as Article 27's reference to refusing to assist if executing a request would prejudice the requested State's sovereignty or security).

[62]*See* Convention on Cybercrime, Art. 26(1).

[63]Ibid., Art. 26(2).

[64]*See* ibid., Art. 27(1).

[65]*See* ibid., Art. 27(2). "In the event of urgency," however, "requests for mutual assistance...may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party," with a copy sent simultaneously to the requested Party's central authority through the central authority of the requesting Party. Ibid., Art. 27(9).

[66]Ibid., Art. 27(2).

[67]Ibid., Art. 27(3). In addition, "[t]he requesting Party may request that the requested Party keep confidential the fact of any request. . . . If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed." Ibid., Art. 27(8).

[68]Ibid., Art. 27(4). The requested Party may also "postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities." Ibid., Art. 27(5).

[69]Ibid., Art. 28(2).

[70]Ibid., Art. 29(1), (3).

for at least sixty days.[71] A party may not refuse a preservation request in a case involving a cybercrime (*i.e.*, one of the substantive offenses set forth in the Convention) on the basis of "dual criminality"—*i.e.*, that the offense at issue is not an offense in the requesting state.[72] However, a requested Party may refuse a preservation request if it concerns an offense that "the requested Party considers a political offence or an offence connected with a political offence" or "the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests."[73]

Sixth, a Party must respond to requests to search, seize, or disclose computer data located within its territory.[74] Notably, however, the Convention states that the requested Party shall respond "through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws."[75] This suggests that a response to a request to search, seize, or disclose data may be delayed or rejected where so required by relevant laws or arrangements.

Seventh, the Convention permits a Party, "without the authorisation of another Party," to "access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."[76] This means, for instance, that a law enforcement agency in Country A may remotely access a computer in country B if it obtains the consent of the owner of that data. Less clear is whether this authority extends to a situation where an LEA in Country A obtains a court order *requiring* the data owner (who may have an office in Country A and thus is susceptible to Country A's jurisdiction) to disclose the data or to allow the LEA to access the computer in Country B.

The issue of "unilateral" access to data stored in another country was controversial during the negotiations of the convention.[77] Apparently some states were in favor of allowing greater authority for unilateral action across borders to access computers and data, while others were opposed. The drafters settled on the two sorts of unilateral actions all could agree on—access to data with the consent of the

[71] *See* ibid., Art. 29(7). In addition, if, in the course of executing a preservation request, a requested Party "discovers that a service provider in another State was involved in the transmission of the communication," it must "expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted." Ibid., Art. 30(1). A requested Party may withhold such data only if the preservation request "concerns an offence which the requested Party considers a political offence or an offence connected with a political offence" or "the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests." Ibid., Art. 30(2).

[72] *See* ibid., Art. 29(3). However, dual criminality may be a reason to reject a preservation request in cases involving other types of crimes. *See* ibid., Art. 29(4).

[73] Ibid., Art. 29(5).

[74] *See* ibid., Art. 31(1), (2). A Party must respond "on an expedited basis" when "there are grounds to believe that relevant data is particularly vulnerable to loss or modification;" or when relevant laws or arrangements otherwise permit expedited cooperation. Ibid., Art. 31(3).

[75] Ibid., Art. 31(2), citing Art. 23.

[76] Ibid., Art. 32. In addition, a Party may, "without the authorisation of another Party . . . access publicly available (open source) stored computer data, regardless of where the data is located geographically." Ibid.

[77] As the Explanatory Note to the Convention says: "The issue of when a Party is permitted to unilaterally access computer data stored in another Party without seeking mutual assistance was a question that the drafters of the Convention discussed at length. There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. " Convention on Cybercrime, Explanatory Note ¶ 293. *See also* K. Harris, *supra*, at 6 ("The establishment of rules to permit direct, unilateral access in other cases proved elusive, and it was decided to wait until further experience has been gained before attempting to fix further rules in this area.").

data owner, and access to open source information.[78] However, the Explanatory Note to the Convention also makes a point of stating that other types of unilateral access "are neither authorized, nor precluded" by the Convention.[79]

Eighth, the Convention provides that "Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system."[80] This mandate is subject to the caveat that the "assistance shall be governed by the conditions and procedures provided for under domestic law."[81] However, Parties are obligated to provide the requested assistance "at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case."[82] This provision is meant to allow Parties "to trace the source of an attack in real time, while a transmission is in progress."[83]

Ninth, "[t]he Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws."[84] This means Parties must assist each other by engaging in wiretapping of computer communications, but only to the extent permitted under their domestic laws. This does not necessarily mean that if a requested state may wiretap when investigating the same type of offense, it must render the requested wiretapping assistance when another state is investigating an offense. The requested state may have jurisdictional requirements, among other things, that would preclude it from wiretapping in order to assist the Requesting State.

Finally, "[a] Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[85] These 24/7 points-of-contact are responsible for "facilitating" or "directly carrying out" the necessary assistance, including by providing technical advice, preserving data, collecting data, providing legal information, and locating suspects.[86] Each Party must ensure that the 24/7 points-of-contact are "trained and equipped" to fulfill these requirements and "facilitate the operation of the network."[87] The 24/7 network was modeled on a similar network created by the G8 group of nations in 1997 and subsequently expanded to include 20 nations by 2001.[88]

The Convention does not have any enforcement mechanism, *per se*, to ensure that Parties comply with their obligations under the Convention. Instead, the Convention provides that "[t]he European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention."[89] It also contains a dispute resolution provision, which states that Parties who disagree "as to the interpretation or application of th[e] Convention...shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned."[90] Nevertheless, if one

[78] *See* Convention on Cybercrime, Explanatory Note ¶ 293. Although the Explanatory Note says that "all agreed" on these two types of unilateral cross-border action, Russia—which is a COE member—has reportedly maintained a continuing objection to this provision. *See* J. Markoff and A. Kramer, *In Shift, U.S. Talks to Russia on Internet Security*, N.Y. Times (December 12, 2009), available at http://www.nytimes.com/2009/12/13/science/13cyber.html; accessed June 7, 2010.

[79] Convention on Cybercrime, Explanatory Note ¶ 293.

[80] Convention on Cybercrime, Art. 33(1).

[81] Ibid.

[82] Ibid., art. 33(2).

[83] K. Harris, *supra*, at 6.

[84] Convention on Cybercrime, Art. 34.

[85] Ibid., Art. 35(1).

[86] Ibid.

[87] Ibid., Art. 35(3).

[88] K. Harris, *supra*, at 6.

[89] Convention on Cybercrime, Art. 45(1).

[90] Ibid., Art. 45(2).

party refuses to submit to such arbitration, the other Party has no real recourse under the Convention as to that dispute.

III. REACTION TO THE CONVENTION

When the Convention entered into force, it was opposed by many civil liberties groups, which feared that the new investigative authorities that would be created in many ratifying states, and the increased law enforcement cooperation, would erode privacy and other rights.[91] The view of private industry was mixed, with copyright owners strongly supporting the convention, but Internet service providers and other network operators concerned about the increased burdens the Convention might place on them in the form of additional requests for interception and stored traffic data and subscriber information.[92] In more recent years, however, the opposition has been more muted. It is not clear whether this has been because the fears of opponents have not been borne out, or because the Convention is now seen as a *fait accompli*, at least in many countries.

One notable and continuing source of criticism has been Russia. Although a member of the COE, Russia has not signed the Convention, let alone ratified it. As discussed below, Russia has, since the mid 1990s, proposed a cyber arms control treaty in the United Nations that would restrict what nation-states can do with cyber weapons. With regard to the Convention, Russia has reportedly been opposed to the section of the provision allowing unilateral trans-border access by law enforcement agencies to computers or data with the consent of the computer- or data-owner, seeing this as a violation of national sovereignty.[93] Some have suggested that Russia's real reason for not signing the convention is its desire to avoid taking on an obligation to assist other nations in cybercrime investigations given the numerous cyber attacks that emanate from Russia, including some that many people suspect are state-sponsored.

The United Nations Office on Drugs and Crime has recently recommended that "the development of a global convention against cybercrime should be given careful and favourable consideration."[94] It cited the slow progress in getting nations to sign onto the COE Convention, and the reluctance of non-COE states to accede to a treaty that they had no hand in developing.[95]

The International Telecommunication Union (ITU), a U.N. agency responsible for information and communication technology issues, has also questioned whether the Convention should be adopted as a global standard. ITU General Secretary Hamadoun Touré has cited the fact that the Convention was developed solely by COE members and four observer nations. He has also reportedly said that the Convention is now "a little dusty."[96] As an alternative, the ITU sponsored the creation of the "ITU Toolkit

---

[91] *See* J. Pryce, *Convention on Cybercrime*, Privacy & Security Law Report, Vol. 5, No.1, p. 1451 (BNA, Inc., October 16, 2006). Some of the comments and concerns expressed by civil liberties groups and others can be found on the websites of the Center for Democracy and Technology, available at http://optout.cdt.org/international/cybercrime/; accessed June 7, 2010; the American Civil Liberties Union, available at http://www.aclu.org/technology-and-liberty/international-cybercrime-treaty; accessed June 7, 2010; and the Electronic Privacy Information Center, available at http://www.aclu.org/technology-and-liberty/international-cybercrime-treaty; accessed June 7, 2010.

[92] J. Pryce, *supra*, at 1451. Many of the initial concerns that had been raised by industry during the drafting process had been addressed by the time the final Convention went into effect. For example, amendments were made to clarify that the Convention did not mandate data retention or the use of specific interception technologies, to make clear that states would not criminalize the development or use of network security testing tools, and to limit the vicarious liability of corporations. *See* ibid.

[93] *See* J. Markoff and A. Kramer, *In Shift, U.S. Talks to Russia on Internet Security*, N.Y. Times (December 12, 2009), available at http://www.nytimes.com/2009/12/13/science/13cyber.html; accessed June 7, 2010.

[94] Secretariat of the United Nations Office on Drugs and Crime (UNODC), *Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime,* Working Paper submitted to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice (Jan. 22, 2010) at 15, available at http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050382e.pdf; accessed June 7, 2010.

[95] *See* ibid. at 11-12.

[96] M. Emert, *ITU will IP-Adressen verwalten*, heise Netze (October 21, 2009), available at http://www.heise.de/netze/meldung/ITU-will-IP-Adressen-verwalten-835928.html; accessed June 7, 2010.

for Cybercrime Legislation."[97] Drafted through the American Bar Association's Privacy & Computer Crime Committee, Section of Science & Technology Law, "with global participation," the toolkit serves as model legislation for countries to adopt. The goal of the Toolkit is to harmonize national legislation without requiring nations to join an international treaty. Still, the Toolkit's substantive provisions were based in part on the Convention, and its sections on international cooperation that resemble those in the Convention. The ITU has also promoted its own cyber-warning organization, the "International Multilateral Partnership against Cyber-Threats" (IMPACT), which is ostensibly modeled after the Centers for Disease Control and Prevention and strives to serve as an international "early warning system" for cyber attacks, but has relatively few members.[98]

The COE, however, has pushed back against the criticism, and said that what is needed is to get more countries to accede to the Convention, not to "reinvent the wheel."[99] The COE Secretary General has asserted that the Convention "has received strong support by the Asia-Pacific Economic Cooperation, the European Union, Interpol, the Organisation of American States and other organisations and initiatives as well as the private sector."[100]

In addition, the COE's Committee of Experts on Terrorism has stated that, for now, at least, no separate Convention is necessary to deal with the use of the Internet for terrorist purposes, including terrorists' attacks on computer networks, since "large scale attacks on computer systems appeared to be already covered by the Cybercrime Convention."[101] It stressed that "at the present stage primary focus should be on ensuring the effective implementation of the Cybercrime Convention and the Convention on the Prevention of Terrorism, as new negotiations might jeopardize their increasing impact on the international fight against cybercrime and terrorism."[102] Instead, the Committee recommended that the COE urge more nations to accede to the Convention on Cybercrime.[103] The Committee also stated, though, that "further consideration could be given to the question of responsibility of Internet providers."[104]

IV. EVALUATION OF THE CONVENTION

The Convention represents the most substantive, and broadly subscribed, multilateral agreement on cybercrime in existence today. It offers a relatively comprehensive approach to harmonizing national legislation to address cybercrime both substantively and procedurally, and presents a framework for international cooperation that did not exist before except on a bilateral or ad hoc basis.

---

[97]The ITU Toolkit is available at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html; accessed June 7, 2010.

[98]*See* M. Emert, *ITU calls for global cybersecurity measures*, The H Security (May 24, 2009), available at http://www.h-online.com/security/news/item/ITU-calls-for-global-cybersecurity-measures-741711.html; accessed June 7, 2010. Information about IMPACT's membership, mission, and services is available at http://www.impact-alliance.org/; accessed June 7, 2010.

[99]J. Kirk, *Council of Europe pushes for only one cybercrime treaty*, NetworkWorld (March 23, 2010), available at http://www.networkworld.com/news/2010/032310-council-of-europe-pushes-for.html; accessed June 7, 2010. At a COE cybercrime conference earlier this year, Maud de Boer-Buquicchio, the COE Deputy Secretary General, reportedly said, ""I think we will have the best chance to succeed if we unite around one international instrument that already exists." Ibid.

[100]Thorbjørn Jagland, Contribution of the Secretary General of the Council of Europe to the Twelfth United Nations Congress on Crime Prevention and Criminal Justice (February 16, 2010) at 18 (citations omitted), available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/SG%20Inf%20_2010_4%20-%20UN%20Crime%20congress_ENGLISH.pdf; accessed June 7, 2010.

[101]Council of Europe Committee of Experts on Terrorism (CODEXTER), Opinion of the Committee of Experts on Terrorism (CODEXTER) for the Attention of the Committee of Ministers on Cyberterrorism and Use of Internet for Terrorist Purposes (2008) at 1, available at http://www.coe.int/t/e/legal_affairs/legal_co-operation/fight_against_terrorism/4_theme_files/Cyberterrorism%20opinion%20E.pdf; accessed June 7, 2010.

[102]Ibid. at 3.

[103]*See* ibid.

[104]Ibid.

A U.S. Department of Justice official involved in cybercrime issues rates the impact of the convention as "very positive."[105] Although there are no statistics by which to meaningfully compare pre- versus post-Convention rates of international cooperation, the DoJ official states that such cooperation has increased "radically" in recent years, and that at least some of this increase is attributable to the Convention.[106] The greatest observable increase has occurred in countries that have ratified the Convention.[107]

In serious investigations, in which time is of the essence, cooperation has improved "remarkably" in the last few years, according to the DoJ official.[108] This includes cases involving destructive cyber attacks (such as denial of service attacks, viruses, and worms).[109] A good deal of this improvement is based on the Convention, in particular the ability to require preservation of evidence until authorities can seek its disclosure; the authority to engage in "spontaneous" cooperation; the creation of the 24/7 points-of-contact network; and the ability to engage in remote searches (though this authority is probably not used often).

Still, the shortcomings of the Convention are obvious. While a good number of European countries (and the United States) have ratified the Convention, a notable number of major players have not. Most conspicuously absent are Russia and China, which have been the source of many of the most serious cyberatttacks in recent years, some of which are suspected to be state-sponsored or, at least, state-tolerated. Beyond that, there is not a single nation from Asia, Africa, or South American that has ratified the treaty. When asked how the Convention might be improved, the DoJ official involved in cybercrime stated that more nations needed to become parties to the Convention.[110]

Substantively, the Convention is fairly comprehensive in addressing the most common categories of cybercrimes and the most common types of investigative tools used by law enforcement. And it clearly prescribes mechanisms and procedures for international cooperation, including expedited responses to requests for assistance. But the Convention also allows Parties to refuse to assist in many instances where assistance would conflict with domestic law or, notably, where a country claims that providing assistance would prejudice its sovereignty, *ordre public*, or "essential interests." Thus, where a Party is suspected of being responsible for an attack—or of tolerating it for its own purposes—that Party would likely be able to refuse to cooperate and still be in compliance at least with the letter of the Convention. And the Convention contains no enforcement mechanism by which countries that do not receive requested cooperation (and/or are the victims of cyber attacks emanating from or transiting through a Party) may seek redress.

Moreover, the Convention does not address the particular concerns that may be raised by cyber attacks that are not just criminal acts, but may also constitute espionage or the use of force under the laws of war. This may be because the negotiators of the Convention were primarily representatives of law enforcement, justice, and foreign affairs ministries and agencies, or it may be that nations simply refused to discuss military and intelligence matters in that setting. Whatever the reason, the Convention does not begin to deal with the issues that might arise when, for instance, a nation finds itself under a devastating cyber attack and cannot afford to wait to see if the countries that the attacks are coming from (or going through) will render the necessary cooperation.

Beyond having more nations ratify it, the Convention itself could be improved in several ways, so that it is a more useful tool for dealing with damaging cyberattacks. Some of the proposals that follow

[105]Telephonic interview of DoJ Official by author, July 29, 2010.

[106]Ibid.

[107]Ibid. The DoJ official notes, though, that "dozens" of countries that are not parties to the Convention have nevertheless enacted domestic legislation modeled on it. Ibid. The official also observes s that cooperation has increased not just in cybercrime investigations, but also in investigations into other crimes involving electronic evidence (including kidnapping cases and threats of violence communicated via email). Ibid.

[108]Ibid.

[109]Ibid.

[110]Ibid.

seem unlikely to be accepted by a majority of the parties to the Convention, out of concern over infringement of their sovereignty interests. Nevertheless, they at least offer a basis for discussion.

First, the grounds for rejecting a request for assistance under the Convention might be narrowed. Allowing nations to deny assistance based on "prejudice" to their "sovereignty, security, *ordre public* or other essential interests" allows them too much flexibility to reject assistance without offering specific and credible reasons. A nation that is itself responsible for the attack (or is purposely tolerating an attack carried out by private citizens within its borders) thus has an easy way to continue to hide its involvement. At the very least, the Convention could require that a requested nation that denies assistance provide *specific* reasons for doing so, in writing. This might at least have some deterrent effect against illegitimate denials of requests for assistance.

Second, a meaningful enforcement mechanism could be added to the Convention, by which a nation that is denied assistance can seek redress. One simple way to do this would be to amend the Convention's existing dispute resolution mechanism so that review by a neutral arbiter is mandatory whenever it is requested by a country whose request for assistance is denied, without requiring the agreement of the requested party before an arbiter can even hear the case. It seems unlikely that nations would agree to give a neutral arbiter the power to compel assistance. But the arbiter might at least be given the authority to declare whether the requested Party's denial of assistance was legitimate. This, too, would have some deterrent effect.

Third, a reporting requirement could be added to the Convention, so that denials of assistance requests—and the reasons for the denials—get reported to the CDPC (or some other entity). This information could then be published in some form, or at least shared with all ratifying states. Such a reporting requirement would also have some deterrent effect on illegitimate or baseless denials of assistance.

Fourth, and most radically, one could imagine an amendment that would authorize requesting Parties that are denied assistance, *without a legitimate, credible reason*, to engage in unilateral, cross-border investigative action, such as remotely searching computers in the requested nation. Such an amendment would go beyond the existing remote search authority in the Convention, which permits a Party to conduct a remote search only when it "obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system." An amendment along these lines could—as a logical matter, at least—go even further and allow the requesting Party—in the event of a destructive cyberattack—to remotely destroy or disable the computer(s) from which the attack is emanating. But such amendments would need to be drafted very carefully (to say the least), so that the circumstances in which such remote searches or counterattacks are authorized are clearly defined.

Even if amendments along the lines of the preceding paragraph could be drafted sufficiently clearly and tightly, in a way that avoids allowing a requesting Party to rely on them as a pretext for its own espionage or cyberattack, it seems highly unlikely that the Parties to the Convention would agree to them. A more realistic alternative, then, might be for Parties to state unilaterally that they reserve the right to engage in such measures when they experience a highly damaging attack and the requested Party denies a request for assistance without a legitimate, credible reason.

V. ALTERNATIVES TO THE CONVENTION

The principal alternative to the Convention that has been put forward thus far is Russia's proposal for an international cyber arms control treaty. Beginning in 1998, Russia has urged United Nations action to limit cyber attacks, likening the destructive effect of cyber weapons to that of weapons of mass destruction.[111] It sponsored a U.N. resolution, adopted by the General Assembly in 2000, that called upon

[111] *See* I. Ivanov, Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General (September 30, 1998), available at http://www.un.org/ga/search/view_doc.asp?symbol=A/C.1/53/3&Lang=E; accessed June 7, 2010.

Member States to consider "existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field" and to examine "international concepts aimed at strengthening the security of global information and telecommunications systems."[112] Russia also proposed a set of principles which, among other things, would have required states to "refrain from . . . [t]he development, creation and use of means of influencing or damaging another State's information resources and systems; . . . [t]he deliberate use of information to influence another State's vital Structures; . . . [u]nauthorized interference in information and telecommunications systems and information resources, as well their unlawful use; . . . [or e]ncouraging the activities of international terrorist, extremist or criminal associations, organizations, groups or individual law breakers that pose a threat to the information resources and vital structures of States."[113] And in 2008, Vladislav Sherstyuk, a deputy secretary of the Russian Security Council, reportedly described a proposed treaty that would prohibit secretly embedding malicious code in another country's computers for later use in the event of hostilities.[114] Russia has also proposed prohibiting attacks on noncombatant systems and on using deception in cyberspace.[115]

The United States has been cool (at best) to the Russian proposal, at least until recently. Late last year, the Obama Administration reportedly began meeting with Russian officials to discuss cybersecurity issues, including possible restrictions on the military use of cyber weapons, and agreed to begin talks in the U.N. Disarmament & International Security Committee.[116] Talks have continued this year, including at a Russian-sponsored cybersecurity conference in Garmisch-Partenkirchen, Germany in April. And in June 2010, Gen. Keith Alexander, the Commander of the U.S. military's new Cyber Command and the Director of the National Security Agency, said that "we have to establish the rules [for cyberwarfare] and I think what Russia's put forward is, perhaps, the starting point for international debate."[117] He also stated that "it's going to take all countries" to establish the rules of the road for how governments operate in cyberspace, and emphasized that the key to any new agreement will be enforcement mechanisms.[118] But he also suggested that the United States should develop a counterproposal to Russia's proposed treaty.[119]

It remains to be seen whether Russia's proposal gains any traction, in particular from the United States, which seems unlikely to agree to a ban on the offensive use of cyber weapons anytime soon. But even if Russia's proposal—or any other proposed treaty to limit nations' use of cyberattacks or to set norms of behavior in "cyberspace"—were adopted, such a treaty would not really be an *alternativ*e to

---

[112]U.N. Resolution 55/28, Developments in the field of information and telecommunications in the context of international security (November 20, 2000), available at http://disarmament.un.org/vote.nsf/511260f3bf6ae9c005256705006e0a5b/d368c1f35906aa318525697d00752cc6?OpenDocument&ExpandSection=3,5#_Section3; accessed June 7, 2010.

[113]Report of the U.N. Secretary General, Developments in the field of information and telecommunications in the context of international security (July 10, 2000) at 5, available at http://www.un.org/documents/ga/docs/55/a55140.pdf; accessed June 7, 2010.

[114]*See* J. Markoff and A. Kramer, *U.S. and Russia Differ on a Treaty for Cyberspace*, N.Y. Times (June 27, 2009), available at http://www.nytimes.com/2009/06/28/world/28cyber.html?_r=1&scp=3&sq=Vladislav%20Sherstyuk&st=cse; accessed June 7, 2010.

[115]*See* Ibid.

[116]*See* J. Markoff and A. Kramer, *In Shift, U.S. Talks to Russia on Internet Security*, N.Y. Times (December 12, 2009), available at http://www.nytimes.com/2009/12/13/science/13cyber.html; accessed June 7, 2010.

[117]Transcript of Remarks by Gen. K. Alexander at the Center for Strategic and International Studies, Washington, D.C. (June 3, 2010) at 11, available at http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf; accessed June 7, 2010.

[118]Ibid. at 14.

[119]*See* ibid. at 11-12. In July 2005, the United States, Russia, China and several other countries reportedly reached agreement on a set of recommendations directed at reducing the threat of attack on each others' networks. *See* E. Nakashima, Washington Post (July 17, 2010), available at http://www.washingtonpost.com/wp-dyn/content/article/2010/07/16/AR2010071605882.html; accessed July 30, 2010. The group reportedly "recommended that the U.N. create norms of accepted behavior in cyberspace, exchange information on national legislation and cybersecurity strategies, and strengthen the capacity of less-developed countries to protect their computer systems." Ibid. However, the author has been unable as of July 30, 2010 to find a copy of these recommendations.

the Convention, since it probably would not provide mechanisms for cooperation when a cyber attack does occur. Thus, for example, Russia might legally bind itself to a treaty banning nation-state attacks on civilian computer networks. But if an attack then occurs that appears to emanate from Russia, that treaty would probably not address how countries that have been attacked may respond, or whether Russia would have any obligation to assist in investigating the attack.

Therefore, a treaty on cyberattacks and the Convention on Cybercrime are not mutually exclusive. Indeed, the Convention could bolster a cyber attack treaty in some senses. For example, if a Party to the Convention rejects a request for assistance in investigating a cyber attack without a legitimate, credible reason, that rejection could be regarded as an indication (though not proof in and of itself) that the Party was directly or indirectly responsible for the attack, and thus in violation of the cyber attack treaty. Thus, even as the United States continues to explore the possibility of a multilateral agreement on cyberattacks, it should continue to urge other nations to ratify the Convention. It should also consider proposing ways of improving the Convention to deter illegitimate or inappropriate denials of assistance by requested Parties.