CHAPTER 6

Toward an International Convention on Cyber Security

Abraham D. Sofaer

The case for international cooperation in dealing with cyber crime is overwhelming. The presentations and discussion at the Stanford Conference, distilled in this volume, demonstrate the growing threat and cost of such crime, as well as its transnational nature. The debate currently under way is over the form and scope such cooperation should take, and the extent to which the United States and other technologically advanced states should rely upon multilateral efforts to enhance cyber security.

Proposals for voluntary international cooperation have been ad-

vanced and are being implemented.[1] The principal elements of these proposals—to train law enforcement officials to understand and cope with cyber crimes, and to establish round-the-clock emergency response teams—are widely supported. In addition, the Group of Eight (G-8) and private groups such as the Internet Alliance have issued guidelines aimed at making voluntary cooperation more effective.[2] Although these groups recognize that international cooperation is essential, they have yet to accept the idea that an international treaty should be negotiated establishing legally mandated standards and obligations.

Support for voluntary, as opposed to legally mandated, international measures rests upon several arguments. Most cyber crime, it is argued, is conventional crime (fraud, drug dealing, money laundering, sexual exploitation of minors), in which cyber technology happens to be used. Existing treaties and international arrangements, including those providing for extradition and legal assistance, are potentially applicable in these cases. Securing international agreement on the wording of new cyber crimes will be difficult, moreover, and vast differences exist among states regarding appropriate regulation of content, the proper scope of transnational investigation, and the bases

1. See, e.g., Remarks of Attorney General Janet Reno to the National Association of Attorneys General, January 10, 2000, available at ⟨*http://www.usdoj.gov/ag/speeches/*⟩; U.S. Department of Justice Computer Crime and Intellectual Property Section (CCIPS) materials, including "The Electronic Frontier: The Challenge of Unlawful Conduct Involving the Use of the Internet: A Report of the President's Working Group on Unlawful Conduct on the Internet," March 2000, available at ⟨*http://www.usdoj.gov/criminal/cybercrime/*⟩.

2. See, e.g., "Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime," Moscow, October 19–20, 1999, Communiqué, available at ⟨*http://www.library.utoronto.ca/g7/adhoc/crime99.htm*⟩. See also Tom Heneghan, "G8 Nations Meet to Discuss Cybercrime," May 15, 2000, reported at ⟨*http://dailynews.yahoo.com/h/nm/20000515/ts/crime cyberspace 2.html*⟩. For details on Internet Alliance, see the materials posted at ⟨*http://www.Internetalliance.org/policy/index.html*⟩, as well as "Testimony of Jeff B. Richards, Executive Director of the Internet Alliance, Before the U.S. Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State, and Judiciary," *Hearing on Cybercrime*, February 16, 2000, available at ⟨*http://www.senate.gov/~appropriations/commerce/richards 00.html*⟩.

upon which tracking information and messages should be subject to seizure and scrutiny. Furthermore, a great disparity exists among states—even technologically advanced ones—as to the scope of privacy and other rights possessed by individuals under national laws that would either operate to limit an international agreement or be compromised by one. Finally, the Internet, many believe, has been a powerful vehicle for economic growth and enhanced communication in large part because it is controlled by the private sector rather than by governments, and this growth and creativity may be adversely affected by international legal requirements and regulation.

For these reasons, Drew C. Arena, then senior counsel to the assistant attorney general, U.S. Department of Justice, commented at the Stanford Conference that achieving consensus on "the specific steps" to be taken in negotiating a multilateral treaty would be "too hard" at the present time to warrant the effort.[3] University of Chicago School of Law Professor Jack L. Goldsmith has argued that, in the absence of a suitable international regime, the United States should rely on unilateral measures in fighting transnational cyber crime.[4] However, he does, in principle, favor the pursuit of such a regime.

These arguments against the creation of an international legal regime to deal with cyber security are cogent, but they are based on difficulties and dangers that are avoidable. Not only is the case for a multilateral agreement to combat cyber crime and terrorism strong, the need to undertake the effort of negotiating one is becoming clearer with the increasing costs of such activity. Though it may indeed be true that most crimes in which computers and networks are involved are conventional and potentially covered by international agreements, these are not the crimes against which a new treaty is needed. Existing

3. Drew C. Arena, "Obstacles to Consensus in Multilateral Responses to Cyber Crime," presentation at the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Hoover Institution, Stanford University, Stanford, California, December 6–7, 1999, p. 3.

4. Jack L. Goldsmith, "Cybercrime and Jurisdiction," presentation at the Stanford Conference, December 6–7, 1999, p. 9.

international agreements provide no help in dealing with crimes related directly to the information infrastructure, including attacks utilizing viruses (such as "Melissa" and "I Love You"), denials of service, and other destructive conduct. Furthermore, the need for an international agreement to deal with cyber crime rests not merely on the fact that such acts include new types of conduct but also on the need for new methods by which cyber crimes will have to be investigated and prosecuted to provide effective protection. Certainly it would be complicated to secure multilateral agreement on the precise wording of cyber crimes, but that effort need not be undertaken: a broad consensus exists with regard to certain conduct involving the information infrastructure that should be made criminal;[5] and a treaty could readily be drafted that describes such conduct and requires all States Parties to make such conduct criminal through any formula they choose to utilize.

The differences that exist among states concerning several key issues in developing a treaty must be taken into account and will limit and shape the arrangements that are currently feasible. But differences concerning such issues as regulation of content, scope of extraterritorial investigation, standards of proof, and protection of privacy and other rights can be resolved, largely through a willingness to begin this effort by focusing on measures likely to secure universal agreement. The sharp differences that exist among states with regard to what can be done unilaterally demonstrate, in fact, the need to attempt to secure agreed, multilateral arrangements, rather than establishing a basis for making no effort to do so.

The notion that the United States should act unilaterally when necessary to protect its interests is in principle sound. As discussed further below, the proposed draft international convention herein (the

5. See Tonya L. Putnam and David D. Elliott, "International Responses to Cyber Crime," Chap. 2 of this volume. The presentations on which this conclusion is based include those by Marc D. Goodman, Dietrich Neumann, and George C. C. Chen at Session Two, "International Response to Cyber Crime," of the Stanford Conference, December 6–7, 1999.

Stanford Draft) explicitly (in Article 20) excludes from its coverage the national security activities of states. Professor Goldsmith seems to recognize, however, that unilateral activities must be legally defensible, and resort to them must be in the nation's best interests. His assumption that it will take many years to negotiate and implement a multilateral convention may turn out to be wrong, in light of the increasingly obvious need and growing momentum for such an arrangement. Furthermore, even before a multilateral treaty is complete, the United States may be able to reach less comprehensive arrangements with other states to enhance legal protections. Unilateral conduct that offends other states, and leads them to reject or delay negotiating a desirable treaty, would harm U.S. interests.

Concerns expressed by the private sector over establishing legally mandated norms and obligations stem from the fear that law enforcement considerations will adversely affect (and greatly burden) Internet businesses and freedom of expression. Government control of the information infrastructure could well have detrimental effects, and international regulation could be especially damaging if political objectives and bureaucratic requirements are allowed to interfere with the present, privately dominated Internet regime.[6] National governments, including the U.S. government, have sought or imposed potentially damaging restrictions on Internet users, including limitations on the use and sale of advanced encryption, demands for the power to intrude upon, hear, and record Internet traffic,[7] and suggestions that private entities assume quasi-prosecutorial responsibilities in criminal investigations. These policies and suggestions have, however, unjustifiably evoked suspicion of all efforts to establish legally mandated

6. See Stephen J. Lukasik, "Current and Future Technical Capabilities," Chap. 4 of this volume, for a description of the present governing structure of the Internet.

7. Consider, for example, the Clinton administration's January 2000 "National Plan for Information Systems Protection," which drew criticism for, among other things, relying too heavily on monitoring and surveillance instead of simply focusing on making systems more secure. See Jennifer Jones, "U.S. Cyberattack Protection Plan Draws Criticism," February 3, 2000, which was reported at ⟨*http://cnn.com/2000/TEC...cyberprotection.crit.idg/index.html*⟩.

obligations. If, as we believe, voluntary efforts will not provide adequate security, legal obligations to cooperate can be devised that are consistent with continued private creativity and control. An international regime can be fashioned to satisfy the full range of cyber-security needs, in a manner that ensures continued private-sector control of Internet technology and practices. The United States is party to several international regimes encompassing the creation of consensus-based, nonmandatory measures crafted by public and private-sector experts, which a treaty for cyber security could draw on in providing a comprehensive and lasting system for international cooperation.

The strong case for a legally mandated, international regime has led to several significant developments. Treaty provisions are being proposed to close loopholes in existing multilateral commitments in the specific area of civil aviation.[8] This approach may be feasible in other areas, particularly to protect critical infrastructures from criminal and terrorist attacks, and it seems likely to cause little controversy.

The Council of Europe (COE) has taken a more comprehensive approach, publishing and refining a draft treaty on cyber crime.[9] This proposal includes definitions of cyber activities that must be made criminal by all States Parties, as well as other features and forms of cooperation.[10] The COE's draft assumes, correctly, that substantial consensus exists with respect to what cyber activities should be considered criminal, and that substantial benefits can be derived from a multilateral arrangement with common standards, investigative cooperation, and extradition.

8. See Mariano-Florentino Cuéllar, "Past as Prologue: International Aviation Security Treaties as Precedents for International Cooperation Against Cyber Terrorism and Cyber Crimes," Chap. 3, III, of this volume.

9. See "Draft Convention on Cyber-Crime (No. 24, Rev. 2)" released for public discussion on November 19, 2000, available at ⟨*http://conventions.coe.int/treaty/en/projets/cybercrime24.htm*⟩. The COE's Justice Ministers resolved on June 9, 2000, that the Council should speed its work and "conclude an international treaty by the end of the year." See ⟨*http://www.coe.fr/cp/2000/427a(2000).htm*⟩.

10. See, e.g., ibid., Chap. II ("Measures to be taken at the national level"), arts. 2–9; Chap. III ("International Co-operation").

This chapter seeks to demonstrate the advantages and feasibility of an even more comprehensive regime by proposing a draft international convention (the Stanford Draft) and discussing its principal elements. The Stanford Draft differs from the draft COE Convention on Cyber-Crime in several important respects. Most significantly, the Stanford Draft would limit the acts it covers to attacks on the information infrastructure and violations of antiterrorist conventions, whereas the COE Draft includes conventional crimes in which computers are used as well as content-related offenses but does not include violations of antiterrorist conventions. The Stanford Draft also would establish an international agency, modeled along the lines of successful, specialized United Nations agencies, to prepare and promulgate—on the basis of advice from nonpolitical experts—standards and recommended practices (SARPs) to enhance the effectiveness of protective and investigative measures, whereas the COE proposes detailed forms of cooperation without such a process.

1. Covered Conduct

The basis for international cooperation rests, most fundamentally, on the combination of a demonstrable need for international agreement to combat harmful cyber conduct and the existence of an international consensus on what conduct should be considered criminal. A review of existing statutory law and proposed international arrangements reflects widespread consensus on prosecuting as criminal the conduct covered in the Stanford Draft: attacks aimed at disrupting or damaging computer operations, deliberate and unauthorized intrusions, interference with computer-security measures, maliciously altering content, intentionally and materially facilitating the commission of prohibited conduct, using a cyber system in committing violations of any of several widely adopted antiterrorist conventions, and using a cyber system to attack critical infrastructures.

Most of these forms of conduct are covered in the COE's draft proposal, although that draft attempts to classify cyber crimes into a

number of specific categories: illegal access, illegal interception, data interference, system interference, and the misuse of "devices" for the purpose of committing acts in the preceding categories.[11] The COE effort to generalize makes the categories of offenses relatively easy to comprehend, but may have created coverage on some issues that is undesirably broad. The prohibition on illegal access, for example, would prohibit intentional access to any part of a computer system "without right."[12] Acts "without right" may include conduct not deliberately undertaken to violate adequately communicated prohibitions on entry. This vague standard is included in most of the COE's proposed offenses. The draft then continues: "A party may require that the offense be committed either by infringing security measures or with the intent of obtaining computer data or other dishonest intent."[13] To the extent the COE Draft permits members to vary conduct it covers, in this and many other provisions,[14] the treaty's effectiveness will be undermined. Uniformity of commitments is in general of greater importance than any particular form or level of coverage.

The introductory language to Article 3 of the Stanford Draft—specifically the concept of "legally recognized authority"—is intended to incorporate the concept of self-defense. Efforts of governments, companies, and individuals to defend themselves from attacks may sometimes require measures that, if adopted without authorization or justification, would be criminal, such as alterations of code, or interfering with operation of computers being used by attackers. At times, such efforts may affect innocent third parties, but nonetheless may be reasonable. The complex issues that are certain to arise in applying

11. See "Draft Convention on Cyber-Crime," arts. 2–6.
12. See ibid., art. 2.
13. Ibid.
14. For example, Article 3's prohibition of "illegal interception"—one of the COE Draft's most fundamental provisions—provides in part: "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." These questionable exceptions (and many others) would enable Parties to create significantly disparate coverage, and raise difficult dual-criminality issues.

established principles of law to this new area of technological activity will be resolved over time, on the basis of experience.[15]

The Stanford Draft recognizes and attempts to deal with the fact that states have different standards in statutes that cover the conduct it proscribes. Instead of attempting to list specific, commonly defined "offenses," as in most extradition treaties, the Stanford Draft refers to types of conduct, and secures commitments from all States Parties to enforce any applicable law against every form of covered conduct, or to adopt new laws necessary to create authority to prosecute or extradite for such conduct. This approach overcomes the problem of attempting to develop precise, agreed-upon definitions of offenses, and therefore the requirement that every State Party adopt particular formulations as national crimes.

In addition to requiring criminal enforcement against conduct specifically aimed at the information infrastructure, the Stanford Draft requires criminal enforcement against the use of computers in the commission of offenses under certain widely adopted multilateral treaties. These include clearly defined crimes against aircraft, ships, and diplomats, and terrorist bombings. Computers can greatly enhance the potential damage caused by crimes, and can make them especially difficult to investigate. Therefore, since most states are parties to these multilateral treaties, they should be prepared to impose more stringent punishment for the use of cyber capacities in committing the targeted offenses. (The COE Draft, No. 24, Rev. 2, does not include such provisions.) Other, widely recognized forms of criminal conduct may also become more aggravated through the use of computers, such as forgery, fraud, theft, and conversion. These crimes are not included in the Stanford Draft, however, since they are in general already encompassed in extradition treaties, to the extent States Parties want such coverage. The cyber dimension of such activities, moreover, would generally involve conduct covered in the Stanford Draft, irrespective

15. See generally Gregory D. Grove, Seymour E. Goodman, and Stephen J. Lukasik, "Cyber-attacks, Counter-attacks, and International Law," *Survival* 42 IISS, London, Autumn 2000.

of the crimes such conduct may have facilitated. (The COE Draft includes coverage of "computer-related" forgery and fraud, but its definitions of these offenses seem likely to cause uncertainties.)[16]

Other types of conduct, when related to the information infrastructure, have been prohibited in some states, including copyright violations and sexual exploitation of minors. Such types of conduct are not covered in the Stanford Draft because their inclusion may prove controversial. These areas are covered by the COE Draft, however, as "Content-related offences."[17] In fact, a sufficient consensus for including some of these offenses—especially the use of computers for sexual exploitation of minors—may exist, and the Stanford Draft's coverage could be expanded to include such offenses. The COE Draft covers offenses related to child pornography, as well as "copyright and related rights," but whether the scope of copyright coverage should be coterminous with treaties in the area, such as the Berne Convention and other copyright treaties administered by the World Intellectual Property Organization, is left unsettled, and Parties are explicitly allowed to "reserve the right not to impose criminal liability" for copyright violations, "provided that other effective remedies are available."[18]

The Stanford Draft includes very limited coverage of "content" offenses, in part to avoid the strong differences that exist among states concerning restrictions on speech and political activity. No type of speech, or publication, is required to be treated as criminal under the Stanford Draft; if, for example, Germany were to decide to ban publication on the Internet of *Mein Kampf*, it would have to do so unilaterally and could not expect to receive enforcement assistance under the Stanford Draft. The single exception to this principle in the Stanford Draft is the narrow coverage of conduct described as the "distri-

16. The definition of forgery, for example, leaves members free to require or dispense with any dishonest intent, and that of fraud requires neither a false representation nor reliance. See "Draft Convention on Cyber-Crime," arts. 7 and 8.

17. Ibid., Tit. 3.

18. See ibid., art. 10.

bution of devices or programs intended for the purpose of committing" other conduct made criminal by the Stanford Draft. The Draft thereby makes criminal the knowing and deliberate effort to cause illegal attacks through such distribution, but not discussions of computer vulnerability intended for evaluating exposure to attacks on the Internet, or other protected speech. States Parties wishing to encourage open discussion of computer attacks and vulnerabilities could designate "safe harbor" sites at which discussion would be considered lawful. (The COE Draft would prohibit the "Misuse of Devices," defined to include the production or transfer, etc. of programs designed primarily to commit other violations, or passwords or other code used for access to computers for that purpose.)[19]

While the Stanford Draft avoids content regulation by focusing on protecting the information infrastructure and computers, the protection proposed is comprehensive. A convention based on such coverage could be used to protect activities that some States Parties may decline to protect as a matter of policy. For example, a company could use code to design protection for information that it could not otherwise protect; a person having the right under the law to obtain such information through lawful means might be prevented from doing so because of the convention's prohibition of efforts to gain access through any proscribed form of conduct. This is a serious concern, since the convention is not intended to enable parties to create a new method for restricting otherwise permissible personal, business, or political activities. It is unclear, however, whether the scope of the Draft's proposed protection could convincingly be restricted in terms that allowed any of the proscribed activities without undermining its credibility. The Draft therefore includes a public-policy exception to its enforcement in Article 13; a similar provision is included in the COE Draft.[20]

19. See ibid., art. 6. The COE Draft allows Parties to require that "a number of such items be possessed before criminal liability attaches."

20. Ibid., art. 27(4)(b). A requested Party may refuse assistance if "it considers

A final issue concerning offenses is whether a cyber crime convention should cover only those offenses that provide for penalties exceeding some minimum term of imprisonment. Extradition treaties generally contain such a limitation, usually that the crime for which extradition is sought be punishable by one year of imprisonment or more. This rule is intended to exclude minor offenses from coverage. Given the complications and the effort required to satisfy extradition requests, this consideration is at least as important in a cyber crime convention as in any other. By having such a requirement, moreover, States Parties would in effect be required to cover prohibited conduct with potential penalties of at least one year in prison. The Stanford Draft therefore includes only crimes for which a potential penalty of at least one year's imprisonment is provided. (The COE Draft includes a separate article on this subject, which is designed to ensure serious penal and civil sanctions.[21])

2. Jurisdiction

The Stanford Draft anticipates that the conduct it covers will have effects potentially conferring jurisdiction on multiple States Parties for the same offense. It provides a set of priorities that Parties would agree to follow in performing their duties and pursuing their rights, to the extent practicable, given the difficulty of anticipating all the possible contingencies. A State Party must establish jurisdiction to try offenders who commit offenses in its territory, who are its nationals, or who are stateless residents in its territory and whose extradition from its territory is refused. A State Party may establish jurisdiction to try offenders who attempt to harm it or its nationals, or to compel it to perform or abstain from performing an act, or whose offenses have substantial

---

that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests."

21. See ibid., art. 13. The COE Draft provides for "Corporate liability," but in terms that would allow several defenses that uniform treatment of all covered entities would not permit. See ibid., art. 12.

effects within its territory. (The COE Draft provides less comprehensive coverage, and fails to provide any guidance with regard to priorities, requiring only "consultation" aimed at determining the "most appropriate" jurisdiction for prosecution.[22])

The problem of multiple-state jurisdiction over crime is by now commonplace in international law. Transnational fraud, for example, has led to decisions by national courts assuming jurisdiction on the basis of any significant connection to the conduct involved. Among these are the states where a fraud was planned, where an effort to defraud was initiated, where individuals worked at implementing the fraud, where or through which communications were made that were intrinsic to the fraud, where the victims were located, and where the fraud had material and intended effects.[23] The widespread recognition of fraud as criminal activity leads states readily to find jurisdiction over such activity, despite the significant relationship particular frauds may have to other states. They tend to assume that punishing fraud will be supported by other affected states, rather than opposed as violating their sovereignty.

Cyber crime is quintessentially transnational, and will often involve jurisdictional assertions of multiple states. To avoid the conflict such assertions of jurisdiction could cause, enforcement under the Stanford Draft is limited to cyber activities that are universally condemned. The Stanford Draft does not accede to a state's jurisdiction merely because someone within its territory is able to access a website in another state; to confer jurisdiction, someone in control of the

22. See ibid., art. 23.

23. See *Libman v. The Queen* [1985] 2 S.C.R. 178, a leading decision of the Canadian Supreme Court providing in-depth description of modern developments with regard to jurisdiction to prosecute conduct involving extraterritorial elements. See also Laurent Belsie, "Cops Narrow Gap on Web Criminals: This Week's Arrest of a Teen Hacker Shows That Law Enforcement Is Getting More Savvy," *Christian Science Monitor*, April 21, 2000, available at 2000 WL 4427576, reporting on the arrest in Montreal after investigations by the Royal Canadian Mounted Police and the FBI of "Mafiaboy" for allegedly sabotaging the CNN.com website in February 2000.

website must deliberately cause one of the covered crimes, with effects in the state seeking to assert jurisdiction. It seems likely, therefore, that states will in general accept all of the reasonably based jurisdictional claims approved in the Draft.

3. Cooperation in Criminal Enforcement

The Stanford Draft includes commitments by States Parties to engage in the full range of cooperative activities found in widely adopted international agreements. Under it, States Parties would agree to extradite or prosecute persons reasonably believed to have engaged in any form of the covered conduct or offenses. Where necessary, and on a proper evidentiary basis, they would arrest and hold alleged offenders for a short period pending an extradition request. They would also agree to cooperate in seizing, preserving, developing, and providing in usable form evidence for the prosecution of offenders in the courts of other States Parties. They would coordinate these activities through designated "Central Authorities," as in Mutual Legal Assistance Treaties, so that each State Party would know whom to address requests to, and would have an identified agency or person responsible for dealing with such requests in a timely and proper manner.

The COE Draft is detailed and comprehensive in the obligations it contains related to (what it terms) "Procedural Measures." It mandates prompt responses to cyber attacks and requests for cooperation, on a twenty-four-hour/seven-days-per-week basis.[24] (The Stanford Draft incorporates a similar commitment.) The COE Draft provides, among other things, for the expedited preservation and disclosure of stored or traffic data; production orders for computer data and subscriber information from service providers; search and seizure of data; real-time collection of data from service providers; and interception of content data.[25] Several of these provisions are controversial. The COE Draft deals with this by requiring that all such measures be

24. See "Draft Convention on Cyber-Crime," art. 35.
25. See ibid., arts. 16–21.

implemented in accordance with the domestic law of the requested Party, with due regard for the protection of human rights; and it also allows Parties to limit to certain cases their obligations to provide real-time collection of traffic data, and interception of content data.[26] Although these rules may prove useful, they have evoked distrust and opposition, and may well become dated or problematic over time, with the availability of new technologies or methods. The Stanford Draft avoids these problems by providing for commitments to cooperate on each of the subjects covered by the COE Draft, but without further specification, leaving it to the Parties to develop on a consensus basis detailed standards and practices with public input.

But if the basic principles of cooperation are clear, when it comes to implementation many problems still exist, and many more are certain to arise, for which answers have not as yet been developed. What, for example, should be the scope of a state's power unilaterally to seek information in a foreign state? A state may not know whether its electronic effort to obtain information about a crime will enter or have any significant effect within another state or states; it could not avoid such uncertainty even if it tried. Some tolerance of extraterritorial effects would, therefore, seem to be imperative in any viable, multilateral cyber-related arrangement. Both the Stanford Draft and the COE Draft call for the widest possible cooperation,[27] and both provide for reasonable unilateral action.[28]

Another area of current uncertainty is what duties an Internet Service Provider (ISP) should have to preserve and provide information of cyber crimes. Should any such duty be enforceable by law, and if so by what means? These are sensitive issues, since states have not yet imposed duties on ISPs and other Internet participants, such as those imposed in analogous contexts. What should states be required to do to enhance the prospects of preserving evidence that could be helpful in investigating an attack; in particular, should a state be required to

26. See ibid., art. 15.
27. See ibid., arts. 24 and 26.
28. Compare Article 6(5) of the Stanford Draft with Article 32 of the COE Draft.

seize such information? As noted, the COE Draft is much more specific on these issues than the Stanford Draft, although the former contains significant room for reservations.

These sorts of issues related to transnational investigation of cyber crime and terrorism raise several common questions. The first concerns technology: What technological measures are possible and/or desirable to assist States Parties in securing cooperation that goes beyond the conventional steps currently undertaken in treaties of extradition and mutual legal assistance? Rapidly changing technological capacities and needs make it fruitless to attempt to deal definitively in a draft convention with this aspect of the cyber crime and terrorism problem.[29] Instead, the Draft proposes general principles supporting certain existing technological objectives, and would establish an international agency (the "Agency for Information Infrastructure Protection" or "AIIP,") through which States Parties would cooperate in considering and proposing the use of particular technological measures to enhance cooperative efforts.

In addition to the technological dimension there are certain questions of principle concerning the right of States Parties to defend against or to investigate cyber crime. May a State Party, for instance, deliberately initiate investigative actions or countermeasures for law enforcement purposes that could involve sending transmissions into cyber systems located in other, sovereign territories? Based on experience to date, fast-spreading computer viruses and other cyber attacks demand prompt efforts to track down attackers, and it is difficult if not impossible to know in advance all the places to or through which any part of any cyber transmission might travel. Therefore, both the Stanford Draft and the COE Draft approve in principle unilateral measures where they are electronic and reasonable. The Stanford Draft provides, moreover, that any law enforcement activity undertaken that knowingly affects another State Party, including any effort to seek

29. Drew Arena is correct in making this point, but wrong to assume that any multilateral regime must share this deficiency. See Arena, "Obstacles to Consensus," p. 10.

cooperative measures from an entity located in another State Party, must be made known to the central authority of that state as soon as practicable. In addition, the Stanford Draft would require all entities, including ISPs, to comply with any standard or procedure developed by the AIIP and accepted by the State Party in which they are located, and would mandate that all States Parties enforce all such standards and procedures. Arrangements based on these principles seem likely to garner widespread support, and would be preferable to unilateral actions that some states could find objectionable (or even criminal).

The Stanford Draft includes a provision authorizing the seizure and forfeiture of equipment utilized in the commission of offenses, subject to due process protections. States could use the information contained in such equipment, or dispose of the equipment as they see fit, consistent with national law. Funds derived from forfeitures have provided resources in other areas for use in upgrading law enforcement capabilities.[30] The seizure and/or forfeiture of cyber equipment used in committing covered offenses is consistent with the universally recognized right of governments to seize instruments of crime.

4. Structure for Technological Cooperation

An effective transnational response to cyber crime requires a high level of technological cooperation with regard to virtually every function expected to be performed by the States Parties. Cyber criminals exploit the technological possibilities available, including the ability to mask their identity, to hide the origin of attacks and other actions by conducting them through intermediate sites, and to find and exploit weaknesses throughout the worldwide information infrastructure. The challenges of dealing with these capacities are further exacerbated by dynamic changes in technology, the continuing development of new

30. See, e.g., United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, December 20, 1988, T.I.A.S., 20 I.L.M. 493 ("Narcotics Convention" or "Vienna Convention on Narcotics").

methods for committing cyber crimes, the current widespread sharing of information and ideas about cyber system vulnerabilities, and a culture among users of cyberspace that is skeptical of, if not outright hostile to, government involvement.

Given these circumstances, it is unrealistic to expect that cyber crime will be significantly controlled or deterred through unilateral or voluntary or purely defensive measures. Defensive measures always make sense, and will prove effective for some entities, some of the time. But the pressure to operate openly in business, education, research, entertainment, and personal activities leads users to develop or choose accessible (hence more vulnerable) technology. Governments have seemed especially unable to defend their sites and systems, and have been frequent targets of attack.[31] Furthermore, the objectives sought through cooperation, and simply unavailable to states acting unilaterally, require a high level of technological coordination.[32] Take, for example, the need to anticipate, freeze, and trace information packets that are used in cyber crime. Those measures, once devised, will need to be approved and implemented by all participants in the information infrastructure, in a technologically compatible manner, or criminals will find and use gaps in coverage. Similarly, to enable states to conduct searches and seizures, to provide for extradition, and to develop evidence that is usable in the courts of all cooperating states, will require

31. Consider, for example, the numerous attacks in January 2000 that paralyzed several Japanese government websites. See Howard W. French, "Internet Raiders in Japan Denounce Rape of Nanjing," *New York Times*, January 31, 2000, available at 2000 WL 12395311, reporting that hackers posted messages on the website of Japan's postal service criticizing Japan's wartime role in China in the 1930s, "as a series of similar attacks" over the previous week "began to look like a daily ritual." See also "Hackers Become an Increasing Threat," *New York Times on the Web/Breaking News from Associated Press*, July 7, 1999, reporting on "high-profile electronic assaults [that] have included [U.S.] government" sites such as the White House, FBI, Senate, and Army Department), reported at ⟨*http://www.nytimes.com/aponline/w/AP-Hacker-Threat.html*⟩; Daniel Verton, "Cyberattacks Against DOD up 300 Percent This Year," which was reported at *CNN.com*, November 5, 1999.

32. Recall the discussion by Stephen Lukasik in Chap. 4.

adoption of uniform and mutually acceptable standards and technological solutions, on which all states can rely.

The pressures for multilateral solutions to information-infrastructure problems are, indeed, likely to be so great that solutions will be developed without the formal, open, and accountable processes associated with established international institutions. The story of how private and public actors developed and secured U.S. government support for a system of website domain protection illustrates both the need for and inevitability of multilateral solutions to at least some of the key issues, as well as the ad hoc and relatively undemocratic process that may occur in the absence of established, publicly accountable mechanisms.[33]

The process by which effective standards and practices are established for international cooperation in dealing with cyber crime and terrorism is likely to be the most important aspect of any multilateral agreement. Considerable guidance can be gained in designing a structure for setting such standards from other areas in which transnational standard-setting activities occur, such as airline safety, marine safety, telecommunications, and banking. In general, standard setting and cooperation in such areas is achieved by establishing an international agency assigned clearly articulated and widely shared objectives, with the technical and material resources to achieve those objectives, a professional and nonpolitical staff, substantial reliance on the private sector (especially on highly skilled technical experts), and continuous political involvement and ultimate control by representatives of the participating states.

The history and structure of the International Civil Aviation Organization (ICAO) are instructive in this regard.[34] ICAO is governed

33. For more on this subject, see Yochai Benkler, "Internet Law: A Case Study in the Problem of Unilateralism," *New York University School of Law: Public Law and Legal Theory Working Paper Series* no. 11 (Fall 1999), to be published in *European Journal of International Law*, available at ⟨*http://papers.ssrn.com/paper.taf?abstract id=206828*⟩.

34. ICAO was established under Part II of the Convention on International Civil Aviation, December 7, 1944, 59 Stat. 1693, 84 UNTS 389 ("Chicago Convention").

by an Assembly consisting of representatives from all its States Parties (185), which meets at least once every three years, establishes basic policies consistent with governing treaties, considers and recommends treaty revisions, approves the budget, which it funds through an apportionment among Member States, and elects delegates to the Council for three-year terms. The Council currently has thirty-three members, including representatives from states of chief importance in air transport, from states that make the largest contributions to international aviation, or chosen to ensure that all major geographical areas are represented. The Council implements Assembly decisions, prepares the budget, administers ICAO's finances, appoints the Secretary General and provides a Secretariat, and is empowered to adopt Standards and Recommended Practices (SARPs), which are incorporated into the ICAO Convention through Annexes. The Council acts by majority vote in carrying out its functions, including the adoption of SARPs, which are only adopted after exhaustive development and "technical monitoring, evaluation and backstopping."[35] Though it may delegate authority in any particular matter to a committee of its members, decisions of any such committee may be appealed to the Council by any interested contracting state.

The subjects dealt with in SARPs reflect the Council's authority to adopt measures necessary to maintain the safety and efficiency of international air transport. In performing these functions, the Council is assisted by the Air Navigation Commission, a body of fifteen persons with "suitable qualifications and experience," appointed by the Council from among nominees of Member States. This expert body is responsible for considering and recommending new or amended SARPs, establishing technical subgroups, and ensuring that the Council col-

---

See Mariano-Florentino Cuéllar's evaluation of the utility of international agreements on civil aviation security as precedents for the regulation of cyber activities and his recommendations for specific modifications to existing civil aviation conventions to close certain loopholes.

35. See "ICAO Technical Co-operation," available at ⟨*http://www.icao.int/icao/en/tcb desc.htm*⟩, and discussed in Chap. 3.

lects and disseminates to all Member States the information necessary and useful for the advancement of air navigation.

Technical assistance is a major aspect of ICAO's work. Member States license pilots in accordance with ICAO standards. Standardization of equipment and procedures is a major aim and activity, on the whole array of technical issues, including navigation, meteorology, charts, measurement, aircraft operation, air traffic services, search and rescue, accident inquiry, and security. Developing countries are actively assisted through a variety of programs, funded by ICAO, the United Nations Development Program (UNDP), and other sources. Some 80 staff members are involved in about 120 assistance projects each year, with an overall budget of $55 million. They provide training, technical advice, and help in purchasing necessary equipment.

A second international agency that performs duties analogous to those relevant to cyber security is the International Telecommunication Union (ITU). The ITU is the oldest intergovernmental organization in existence, having been formed in 1865 to implement the Telegraph Convention. It expanded its activities to radio in 1906, and currently deals with issues related to all forms of "telecommunications," including telephone, television, and telex. It operates along the same lines as ICAO,[36] and relies heavily on private-sector expertise and involvement.[37] In recent statements, the ITU has expressed its

36. The ITU Plenipotentiary Conference (of about 170 members) establishes general policies consistent with governing treaties; proposes revisions to the International Telecommunication Convention when necessary; develops the basis for a budget; and elects an Administrative Council, composed of 43 members chosen with due regard to equitable geographic representation, which meets once each year, supervises the Union's administrative operations, coordinates the activities of its permanent bodies, approves the annual budget, and interacts with other international bodies. Expenses are borne by the Member States, which are divided into several contribution classes based on relevant capacities. The Plenipotentiary also elects a Secretary General, who supervises the operations of the Secretariat, which is responsible for the ITU's administrative and financial affairs. The ITU, like ICAO, has a substantial program of technical assistance and training, especially for needy states, funded in part by the UNDP.

37. Technical activities constitute the bulk of the ITU's activities. It has several boards and committees of politically independent experts who make recommenda-

intent to become more involved with information-infrastructure issues.[38]

The ICAO and ITU regimes deal with underlying technological matters that differ from each other, and from Internet communications, in significant ways. But the needs that led to the creation of these, and of other, similar regulatory mechanisms, are largely analogous to those affecting the cyber world. The key factors behind establishment of these multilateral bodies have been safety and efficiency—the same considerations supporting a multilateral solution to the problem of cyber crime and terrorism. In addition, these multilateral entities are designed to: (1) enable all States Parties to learn of and become involved in the multilateral solutions of problems related to transnational technologies; (2) enable technologically advanced states to protect their interests; (3) ensure that solutions are based on the best possible scientific knowledge, developed with the input of expert advice; and (4) benefit from involvement and expertise of private interests (both commercial and nonprofit).

The Stanford Draft draws on the ICAO and ITU patterns in creating a proposed international institution, the "Agency for Information Infrastructure Protection" or "AIIP," to implement the objectives of States Parties with regard to protecting the information infrastructure from criminal and terrorist cyber activities. No single set of tech-

---

tions concerning technical and operating issues in different areas of telecommunications, including the International Frequency Registration Board, five radio experts elected by the Plenipotentiary from different regions of the world, which records frequency assignments and advises Member States concerning such issues as interference. In addition to representatives of Member States, experts from private companies operating telecommunication services routinely participate in the Committees' work.

38. See, e.g., "ITU Efforts to Build a New Global Information Infrastructure," available through ⟨*http://www.itu.int/newsroom/index.html*⟩, stating in part: "While many countries are already beginning to implement their own strategies to put in place new high-speed information infrastructures, there remains a need for a global approach which will foster worldwide compatibility between new technologies. The ITU, with its 188 government members and around 500 members from private industry, represents a global forum through which global standards that reflect the needs of a broad cross section of the infocommunications industry, from operators and governments to service providers and consumers, can be developed."

nical fixes will solve the problems that now exist, let alone those that will develop as the technological possibilities expand. The AIIP is therefore designed to play an ongoing role in formulating and revising standards and in proposing treaty revisions for enhanced safety, efficiency, and effective cooperation in light of continuing technological and political developments. Properly designed and structured, this type of agency should contribute materially to cyber security.

The Stanford Draft would require States Parties to establish the AIIP, with the following key components: an Assembly having functions similar to those exercised by the plenary bodies that operate in ICAO, the ITU, and some other specialized agencies; a Council that implements the policies set by the Assembly, through committees of experts, with heavy private-sector representation; and a Secretary General and Secretariat to implement Assembly and Council instructions and perform administrative tasks. The Council would formulate and the Assembly would adopt recommended standards and practices (SARPs) to advance the purposes of the Stanford Draft, and the AIIP would also propose amendments and additional international agreements to implement solutions to problems that require new authority from states. Some of the UN's specialized agencies have an impressive record for developing and proposing international agreements to deal with important areas not covered by their founding instruments. The International Maritime Organization (IMO), for example, has proposed over twenty treaties to deal with important issues of maritime safety or efficiency, most of which have been widely ratified. In addition, the AIIP Council would be authorized to create and implement, with the Assembly's support, assistance programs to help needy States Parties participate effectively in the activities contemplated in the Stanford Draft.

The standards and recommendations to be developed by the AIIP would be designed to have the same legal force attributed to SARPs developed by ICAO. SARPs adopted by ICAO are not legally binding; they become part of appendices to the ICAO Convention, and States Parties are expected to implement them. States Parties are, however,

required to advise other States Parties of their failure to implement SARPs, and the latter would be free to act to protect themselves from the potential consequences of a state's failure to abide by the standard or practice at issue. This type of arrangement has proved universally acceptable in civil aviation and in other areas of transnational regulation, to ensure that standards and practices proposed are thoroughly evaluated, widely supported, and accepted voluntarily on the basis of sovereign self interest and mutuality of obligation.

Authority is provided in Article 12 to the AIIP in the Stanford Draft to enable it to discipline States Parties, or states that are not parties but are participating in the information infrastructure. Where a state acts or allows persons to act in a manner that undermines the objectives of the Draft, the Council is authorized to recommend sanctions, and the Assembly is authorized to impose them on a two-thirds vote, up to and including expulsion from the AIIP, and a recommendation to states of exclusion from the information infrastructure. Although the Draft avoids regulating state conduct, actions that undermine its purposes, such as allowing persons to use a state's territory to launch attacks affecting other states, would allow the AIIP to exclude such states from membership or to recommend punishing persons and/or non–States Parties by excluding them from participation in the international information infrastructure.

5. Protection of Individual Rights

Transnational regulation of the Internet raises several important issues related to privacy and other individual rights.[39] The Stanford Draft ensures that, at a minimum, individual rights afforded by States Parties are not adversely affected. No State Party has any duty under the Stanford Draft to act in any manner that might infringe upon the privacy or other human rights of any individual or entity, as defined

39. See Ekaterina A. Drozdova, "Civil Liberties and Security in Cyberspace," Chap. 5 of this volume.

by the law of that state.[40] In addition, the Stanford Draft authorizes States Parties to refuse or cease cooperation in investigations or prosecutions they consider politically motivated or unfair. It would also create a subcommittee of experts as part of the AIIP, assigned the task of following and reporting upon the protection of privacy and human rights. Finally, the Draft provides that certain fundamental protections must be extended to persons detained for violations of any offense covered by its terms, including notice to the representative of the state of which an accused is a national, and the right to such representative's assistance.

Efforts to protect privacy and other human rights will involve complications for States Parties, for private entities, and for the AIIP as an organization. Notions of privacy and the scope of procedural and human rights vary considerably among the states whose participation is needed for a workable international regime. These differences have led the Internet Alliance to conclude that a legally mandatory regime on Internet crime would likely "wreak havoc" on privacy protections.[41] In fact, no such result is necessary to have effective multilateral cooperation. By allowing States Parties to insist on the preservation of national norms as a minimum level of protection, the Stanford Draft would preclude its use to deprive any person of rights granted by any State Party, and the problems anticipated will be analogous to those created under the air transport and other antiterrorism conventions. Just as the United States and USSR were able to live with such differences in those contexts and still benefit from the agreements (for example, by securing extradition and prosecutions of hijackers), the Stanford Draft has been designed to enable states with radically different political values to work together on achieving mutually ben-

40. An analogous provision appears in the COE Draft. See "Draft Convention on Cyber-Crime," *supra* n. 10, available at ⟨*http://conventions.coe.int/treaty/en/projets/cybercrime24.htm*⟩, art. 27(4)(b).

41. See "An International Policy Framework for Internet Law Enforcement and Security: An Internet Alliance White Paper," May 2000, available at ⟨*http://www.Internetalliance.org/policy/leswp.html*⟩.

eficial aims without sacrificing those values. If, however, a serious and unresolvable situation emerged in which, for example, the regime of technical and operational cooperation developed under the Draft was abused by a state in some manner, the Assembly is empowered to impose sanctions in Articles 12, 13, and 21, including expulsion from the AIIP or a recommendation against the offending state's participation in the international information infrastructure.

In some situations, the requirement that all actions requested of a State Party must be consistent with its laws may provide less than optimal protection. A State Party could, for example, establish a method for preventing information from reaching its nationals that could be breached only through conduct inconsistent with one or more of the types of activities prohibited by the Stanford Draft. If a U.S. national engaged in a prohibited form of conduct in sending information into such a state he or she would theoretically be subject to extradition or prosecution, since the U.S. Constitution does not guarantee a right to communicate information into another state in a particular manner that is prohibited by treaty. States Parties should be able to determine, in such situations, whether compliance with a demand for cooperation would be manifestly inconsistent with established public policy, and on such a finding to decline cooperation. The Stanford Draft and the COE Draft both contain such provisions (Article 13(1) and Article 27(4)(b), respectively), which are consistent with the power explicit or implicit in all extradition treaties to decline cooperation as a matter of sovereign discretion.

6. National Security

The Stanford Draft makes clear, in a manner similar to other multilateral agreements, that it is inapplicable to state conduct and national security affairs.[42] A multilateral agreement on cyber crime will have

42. Deputy National Security Adviser Richard A. Clarke reportedly, at a June 19, 2000, American Enterprise Institute meeting—"Cyber Attacks and Critical Infrastructure: Where National Security and Business Converge"—declared publicly his oppo-

novel, complex, and important objectives apart from the possible use of cyber systems by states as military or intelligence tools. Efforts to control state conduct related to national security will be unhelpful in advancing the development of a multilateral approach to the problem of cyber crime, and unnecessary as well.[43] ICAO protects civilian aircraft from attack, and the ITU protects radio transmissions from interference. But these treaties do not attempt directly to control states in the conduct of their national security affairs. To the extent use of cyber technology as a weapon is a concern, existing arms control agreements, and treaties incorporating the laws of war, are all potentially applicable, as are the UN Charter provisions concerning the use of force.[44] The Draft does provide sanctions against conduct that undermines its purposes. If further measures need to be considered to limit the use of cyber technologies in areas of national security, they should be taken up separately and not used to hold hostage the development of a multilateral regime to advance the process of dealing with

sition to a multilateral treaty regulating cyber crime on the ground that it might foreclose the U.S. option to conduct information warfare. This position is based on an erroneous premise. The Stanford Draft would preclude such limitations even more comprehensively than other existing treaties. See, e.g., Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation (Sabotage), September 23, 1971, 24 U.S.T. 564 [Montreal Convention], art. 4(1): "This Convention shall not apply to aircraft used in military, customs or police services." See also International Convention for the Suppression of Terrorist Bombings, December 15, 1997, 37 I.L.M. 249 (Terrorist Bombings Convention), art. 19: "1. Nothing in this Convention shall affect other rights, obligations and responsibilities of states and individuals under international law, in particular the purposes and principles of the Charter of the United Nations and international humanitarian law. 2. The activities of armed forces during an armed conflict, as those terms are understood under international humanitarian law, which are governed by that law, are not governed by this Convention, and the activities undertaken by military forces of a state in the exercise of their official duties, inasmuch as they are governed by other rules of international law, are not governed by this Convention."

43. See "Developments in the Field of Information and Telecommunications in the Context of International Security," UN General Assembly Doc. A/54/213, August 10, 1999, pp. 8–10, in which the Russian Federation comments on UN initiative and warns against the creation of an "information weapon."

44. See Grove, Goodman, and Lukasik, "Cyber-attacks, Counter-attacks, and International Law."

criminal activities harmful to all states, their peoples, and their economies.

7. Dispute Resolution

The Stanford Draft relies initially on consensual resolution of disputes through negotiation and mediation. States Parties unable to resolve their disputes consensually are required to submit to arbitration in any agreed form. The Stanford Draft contemplates that the Council of the AIIP will, after its creation,[45] propose for the Assembly's consideration an arbitration mechanism through which disputes would be resolved by expert panels designated in advance to hear and decide such matters, perhaps in the relatively informal manner preferred by the industry for resolving disputes over website domain names.[46]

8. Amendments

The Stanford Draft contains a standard treaty provision enabling the States Parties to propose and approve amendments as necessary and appropriate.

45. The Stanford Draft makes no effort to deal with the technical measures necessary to create the AIIP, which would presumably be similar to the steps taken when, for example, ICAO was created toward the end of World War II.

46. See, e.g., *Noodle Time, Inc. v. Max Marketing*, DeC AF-0100 (March 9, 2000), reported in *Int'l Law in Brief*, April 1–14, 2000, available at ⟨*http://www.asil/org/ilibindx.htm*⟩, an example of the procedure set up by Internet users (with U.S. government support) to apply the rules governing website domain names, as established in the Uniform Domain Name Dispute Resolution Policy.