CHAPTER 2

International Responses to Cyber Crime

Tonya L. Putnam

David D. Elliott

Concerned technical experts well understand that information security issues are inherently and unavoidably global in nature. Judicial and law enforcement officials equally well understand that the means available to investigate and prosecute crimes and terrorist acts committed against, or through the medium of, computers and computer networks are at present almost wholly local and national in scope. The

The material for this chapter is drawn largely from papers prepared for, and presentations made at, Session Two, "International Response to Cyber Crime," of the Conference on International Cooperation to Combat Cyber Crime and Terrorism, Hoover Institution, Stanford University, Stanford, California, December 6–7, 1999. The following persons made especially valuable contributions: Drew C. Arena, Susan W. Brenner, George C. C. Chen, Ekaterina A. Drozdova, Marc D. Goodman, and Dietrich Neumann.

challenge therefore is how to regulate a technology that permits rapid transactions across continents and hemispheres using legal and investigative instruments that are fragmented across jealously but ineffectually guarded national and jurisdictional borders. When one adds to this the rapidity with which the technology itself continues to evolve and the difficulties this poses for designing, updating, and disseminating effective technical security measures, the full complexity of the problem begins to come into view. Recognition of this state of affairs points toward the desirability of arrangements at the international level to overcome these procedural barriers. However, in the short to medium term such efforts will need to build upon, or at least take into account, existing national and regional efforts to combat cyber crime and terrorism.

The International Convention to Enhance Security from Cyber Crime and Terrorism presented in this volume aims to formalize, in the near term, the highest degree of multilateral cooperation feasible. Points of similarity across national-level laws already promulgated by concerned lawmaking bodies in different countries should indicate where, both in substance and scope, efforts to bring about a multilateral arrangement are most likely to succeed. To this end, this chapter will survey a number of existing national laws that establish criminal penalties for various categories of behavior in cyberspace. It will consider whether and to what degree apparent similarities reflect an emerging international consensus[1] on the need for cyber law, on the types of conduct that should be treated as computer crimes, and on the conditions of pursuit and punishment of cyber criminals. In the second part of the chapter, we turn the focus on a brief examination of other multilateral initiatives to combat cyber crime and cyber terrorism, most of which have yet to reach fruition. The objective is to

1. "Consensus" as it is used in this discussion is defined broadly as a state of "general agreement." To find consensus on an issue, therefore, does not demand an identity of opinion on every aspect of the question; rather, it merely suggests that there is enough agreement among enough states to permit consideration of a multilateral effort.

demonstrate why a multilateral initiative that can be implemented over the short term, such as the proposed International Convention, is both necessary and desirable in spite of the ongoing parallel efforts of a number of international and regional organizations.

1. National Responses to an International Problem

As argued in the preceding chapter, a growing number of states appear to have recognized that cyber crime and terrorism pose a significant threat to the infrastructure, commercial interests, and public policies of highly industrialized and highly computerized societies. This emerging recognition is reflected most directly in the national legal codes of concerned countries. An examination of the legal codes of fifty countries conducted in mid-1999 by Ekaterina Drozdova, with the help of Marc Goodman, Jonathan Hopwood, and Xiaogang Wang, revealed that nearly 70 percent of the countries for which data were readily found have promulgated, or are planning to promulgate, laws prohibiting a reasonably comprehensive slate of computer-related crimes.[2] The remaining roughly 30 percent of states surveyed had few or no laws against computer-related crimes.[3]

2. Countries in the Drozdova survey found to prohibit, or to be in the process of promulgating legislation to prohibit, most of or all of the computer-related offenses specified as "consensus crimes" in the Draft Convention are: Australia, Austria, Bulgaria, Canada, Finland, France, Germany, Greece, India, Israel, Italy, Japan, Malaysia, Mexico, the Netherlands, Norway, the People's Republic of China, Portugal, Romania, Russia, Singapore, South Africa, Spain, Sweden, Switzerland, the United Kingdom, and the United States. In regional terms, the Drozdova survey encompasses 60 percent of the European countries, 100 percent of the North American countries, several countries in Central and South America and the Middle East, but fewer in Asia and the Caribbean, and very few in Africa. The survey covered roughly 50 percent of world population, including many populous nations such as China, India, Japan, the United States, Russia, and Brazil.

3. These countries are: Argentina, Brazil, Chile, Costa Rica, the Czech Republic, Denmark, El Salvador, Equador, Hungary, Iceland, Ireland, Jordan, Luxembourg, New Zealand, Oman, Panama, Peru, Poland, Saudi Arabia, Trinidad and Tobago, Tunisia, the United Arab Emirates, and Venezuela. The actual state of legal coverage for cyber offenses is, in all likelihood, considerably lower than 70 percent. Although

The Draft Convention discussed in this volume takes an "inductive" approach to determining what kinds of conduct should be considered cyber offenses. That is to say, it seeks to codify on an international scale conduct that all (or nearly all) states that have enacted criminal statutes against cyber crime *already* include among their criminally punishable offenses. The Drozdova survey found that, of the thirty countries identified as having laws against computer misuse, each prohibits, in some statutory form all, or most, of the following acts: (1) unauthorized access;[4] (2) illicit tampering with files or data (e.g., unauthorized copying, modification, or destruction); (3) computer or network sabotage (e.g., viruses, worms, Trojan horses, denial-of-service attacks); (4) use of information systems to commit or advance "traditional" crimes (e.g., fraud, forgery, money laundering, acts of terrorism); (5) computer-mediated espionage; (6) violations against privacy in the acquisition or use of personal data; (7) theft or damage of computer hardware or software. These seven acts will be referred to throughout the chapter as "consensus crimes." (See Figure 1.)

Clearly, the Drozdova data indicate at least some measure of international consensus on the desirability of punishing a small but significant group of acts perpetrated against, or by means of, computers and computer networks. But a great deal of national-level variation at the margins underlies this broad finding. Although points of legal difference in the substantive definition of cyber offenses, and even country-specific gaps in legal coverage, do not necessarily preclude a

---

the survey conducted by Drozdova et al. includes a high proportion of the most highly industrialized and most highly computerized countries, its coverage of the developing world is less thorough owing to limitations on the availability of information about the criminal codes of many of those countries. Insofar as more highly computerized societies have a greater incentive to promulgate laws against computer-related crime, the absence of data for much of Africa, Asia, and the Caribbean is not surprising.

4. Note that throughout this chapter, the term "unauthorized entry" (the formulation used in the proposed International Convention to Enhance Security from Cyber Crime and Terrorism) is used interchangeably with the term "unauthorized access," the preferred formulation in many national cyber laws and international documents.

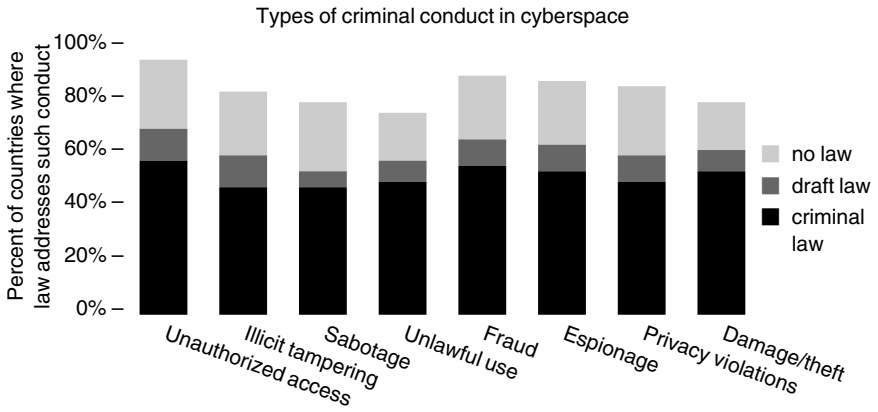

Fig. 1. Emerging international consensus on cyber crimes: Results of Global Cyber Law Survey of fifty countries in Africa, the Americas, Asia, Europe, the Middle East, and Oceania. (*Source:* Ekaterina Drozdova, prepared for the Conference on International Cooperation to Combat Cyber Crime and Terrorism, December 6–7, 1999, Hoover Institution, Stanford University.)

finding of consensus sufficient to sustain a multilateral effort, the existence of such differences at the very least counsels for closer examination. A country-by-country examination of cyber law on a global scale is, unfortunately, beyond the capacity of a single chapter. Therefore, in this section we examine cyber laws on the books in three geographic regions—the United States, East Asia, and Western Europe—to compile a handful of comparative snapshots of how different countries and regions have responded legislatively to the threats posed by computer and network misuse.

United States

The United States Code contains a number of statutes and statutory provisions to regulate the use of computers and computer technology. Chief among them is the Computer Fraud and Abuse Act (18 U.S.C. § 1030), enacted in 1984, which was "designed to deal specifically with unauthorized use of computers and the alteration and destruction

of the records they contain."[5] Unauthorized access to a computer or network without a further offense (e.g., system impairment, obtaining protected information) is per se illegal only with respect to computers used exclusively by the Government of the United States.[6] Unauthorized access to all other computers—for instance, those used nonexclusively by the federal government, including computers containing national security records, and those containing financial and credit records—require some further act or damage to occur in order for criminal penalties to apply. In addition to these offenses, the Act also prohibits use of a computer in interstate commerce to "transmit a program or command which damages a computer system or network," or interrupts the use of a cyber system; "trafficking" in passwords to U.S. Government computers; and the use of interstate commerce to transmit passwords with the intent to defraud.

Under the U.S. federal system, each of the fifty states of the United States is also permitted, within the constraints imposed by federal law, to pass additional substantive criminal laws to regulate computer use at the state level. As Susan Brenner described in her overview of state cyber crime statutes at the Stanford Conference, a number of state legislatures have exercised their ability to further criminalize a wide range of acts involving computers and computer networks. In so doing, these legislatures have provided an interesting demonstration of the degree of substantive variation possible in cyber law, even among entities that share many similarities in their general legal environment. At least as instructive, however, is the degree of coincidence evident particularly with respect to legislative activity on many of the "consensus crimes" identified above.

According to Brenner's research, "crimes involving intrusion and

5. Davis McCown, "Federal Computer Crimes" (1995), available at ⟨*http://www.davismccownlaw.com/*⟩.

6. Under U.S. federal law, unauthorized access includes not only prohibited access from outside a system or organization but also acts in which individuals with authority to access *part* of the data exceed that grant of permission and access nonauthorized data.

damage" are responsible for "by far the largest number of [state] substantive criminal statutes" related to computer crime. Almost all states have trespass and vandalism statutes. Many of these statutes make unauthorized entry a more serious offense when it occurs with the intent or effect of harming data. A substantial number of states outlaw "computer invasion of privacy," which generally entails gaining access to a person's personal financial, medical, employment, or academic information. A handful of states have also added statutes to cover the subsequent use or appropriation of illegally obtained data. Many states also have separate statutes covering use of computers and the Internet to "devise or execute" fraud, theft, and embezzlement. But, as Brenner observed, few states have outlawed computer "forgery," or falsification of data in computer systems; U.S. state legislatures distinguish themselves from the international norm in their uncommon degree of concern with sexual crimes involving computers, which constitute the second-largest body of criminal cyber crime statutes at the state level. In this category, the majority of statutes concern use of the Internet to solicit, entice, or lure minors into a sex act.

On the other hand, few U.S. states currently have statutes that criminalize potentially destructive acts of computer "mischief," such as the creation of viruses, worms, or "malicious logic" programs that can harm the information system or, in many applications, damage the equipment it controls.[7] A handful of states have enacted legislation criminalizing the disruption or denial of essential services, including "a public or private utility, medical services, communication services, or government services." In Brenner's opinion, the lack of activity in this area at the state level is due to a considerable degree to the small number of such incidents reported in the media. In practical terms, a large-scale attack against public or private infrastructure would fall squarely within the purview of federal law enforcement and federal criminal prosecution. However, Brenner argues, there is still room for

7. By contrast, a surprisingly large number of U.S. states have adopted separate statutes to cover the theft and destruction of computer equipment or computer supplies.

state legislatures to act effectively in the criminalization of infrastructure and service attacks.[8] First, state law is necessary for state courts to be able to deal directly with small-scale attacks (that is, those confined to the territory of a single state or portion of a state) against essential services.[9] Second, state law may, under some circumstances, also function as an adjunct to federal prosecution.[10]

Asia-Pacific

George Chen identified categories of computer and network misuse that approach the status of consensus crimes in Asia (Figure 2). These include: unauthorized access; unauthorized use; modifying or damaging data stored on a computer system; theft of money, financial documents, assets, and services by means of a computer; theft of computer software, data, and other forms of information; and damaging or destroying a computer system. Chen cautioned that apparent parallels in the black-letter laws being promulgated in many Asian countries may conceal vastly different modes of interpretation and patterns of enforcement.

In 1997 the Taiwanese criminal code was revised and laws prohibiting computer crimes were added. After a long debate Taiwanese lawmakers decided that merely accessing a computer system without authorization would not be considered an offense unless there was also proof of an additional crime, such as modification or destruction of data. However, the bar on what constitutes an additional offense was set quite low, to include, for example, acts such as reviewing, without consent, e-mail not intended for the intruder. Since 1997, electromagnetic records have been accorded the same protections under Taiwanese law as written documents, including provisions against

8. E-mail correspondence with Susan Brenner, March 6, 2000.

9. The alternative is for a state court to rely upon federal statutes, such as 18 U.S.C. § 1030, to prosecute computer crimes occurring wholly within its territory.

10. Brenner notes, for example, that Oklahoma state law was used in the federal court prosecution of Terry Nichols, one of the suspected perpetrators of the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City.

	Theft of electronic data	Destruction or damage of a computer system	Disclosure of secrets	Computer fraud	Unauthorized access	Forgery of e-document	Defamation/libel	Business disparagement	Obscenity
Taiwan	•	•	•	•	•	•	•	•	•
Hong Kong	•	•	•	•	•	•	•	•	•
China	•	•	•	•	?	•	•	•	•
Japan	•	•	•	•	•	•	X	X	X
Singapore	•	•	□	•	•	•	•	•	•
Thailand	•	•	•	•	•	•	•	•	•
Vietnam	X	X	X	X	X	X	•	•	•
Malaysia	•	•	•	•	•	•	X	X	X

•=prohibited □=weakly or incompletely prohibited X=no prohibition ?=unknown

Fig. 2 Cyber law coverage in selected Asian countries.

forgery and theft, and are likewise regarded as movable property. This feature of the code can be applied broadly in the future to cover everything from transactions involving electronic currencies to interference with the processing of electromagnetic files through, for example, the release of viruses into a system. The Taiwanese code makes it an offense to perpetrate fraud by means of "input [of] false information or commands into a computer or related device, to infringe on copyright, or to appropriate the possessions of others." Other acts that have been criminalized include "libel," "business disparagement," "obscenity," "making threats," "gambling on the net," and "disclosure of secrets."

Under Japanese law, unauthorized access to a computer in which an individual may view secret information is itself a criminal offense, even if there is no damage to the system. The disclosure of secrets that may result from unauthorized access falls under the Business Secrets

Act Against Unfair Competition. Also criminally punishable under Japanese law are "offenses against e-mail," "damage and destruction," "disruption of operations," "computer forgery of electromagnetic documents," and "interception of computer data or files." The current legal trend in Japan is toward making interception of electronic records an offense against movable property, as in Taiwan.

In Singapore, computer crimes are covered by the Computer Misuse Act. Under this Act "unauthorized access," "disclosure of secrets," "destruction or damage of computer systems or electronic data," and "computer fraud" are all prohibited. Although Singapore has no special provisions against defamation or libel, business disparagement, or obscenity perpetrated by means of cyberspace, these offenses are covered under the standard Penal Code. In Malaysia, a Computer Crime Act issued in 1997, though not yet entered into force, covers essentially the same offenses as the Singapore Computer Misuse Act. However, Chen noted, in Malaysia, defamation and libel, business disparagement, and obscenity offenses are subject to civil liability only.

In Hong Kong, computer crimes are, as a rule, governed under the Telecommunications Ordinance. Exceptions include the crimes of "defamation" and "business disparagement," which are covered under the Defamation Ordinance together with Common Law provisions, and also computer obscenity, which is covered by the Control of Obscene and Indecent Articles Ordinance. Under Hong Kong law, "offenses against e-mail," "damage and destruction," "computer fraud," and "theft of electronic data" are all criminal offenses.

In the People's Republic of China, computer-related crimes are covered by Articles 285–287 of the Criminal Code. As Chen explained, the Chinese provisions of which he is aware are notable both for the breadth of their drafting and the severity of the penalties attached. Offenses such as "illegally interfering in the operation of a computer system," for example, are punishable by a minimum sentence of five years in prison, but in 1998 two brothers from Jiangsu Province were sentenced to death after having been convicted of breaking into a bank's computer system pursuant to a robbery. The PRC is also con-

cerned about possible subversive content in network communications, and has undertaken to monitor and criminalize such communications. This effort goes beyond the norms of most other states and is unlikely to find its way into any international agreement.

Finally, in Vietnam and Thailand no law specifically targeting computer crime has been propagated or proposed at the time of this writing. Apparently it is up to prosecutors to stretch provisions in the Criminal Code to cover Internet-related offenses. The general approach has been to attempt to persuade courts in these countries that electronic data should be treated as movable property, thereby extending the protection of existing penal laws against offenses such as theft, fraud, disclosure, defamation, and "mischief." This type of legislative inaction will in all likelihood leave important legal gaps that cannot be papered over with existing statutes. Even supposing that law enforcement and judicial officials in these countries were to take a highly assertive approach to the pursuit of computer crime, the successful prosecution of so-called "pure" computer crimes under existing statutes would demand a high degree of legal creativity and massaging of definitions. In civil code countries lacking a strong tradition of judicial discretion, the chances that such a strategy will prove effective are quite remote.

Europe

The legislatures of Western and Central European countries have been active in promulgating laws prohibiting unauthorized access, computer sabotage, computer espionage, data manipulation, and computer fraud. Though the diversity of national cultures and legal traditions in Europe all but guarantee variation among national laws in this group of states, the European Union (EU) operates in this, as in other fields, as a force for legal harmonization across national approaches.[11]

11. A thorough account of the national laws of all fifteen Member States of the European Union is beyond the scope of this chapter. For more information, consult

All EU Member States, with the exception of Austria, have enacted laws prohibiting some form of unauthorized access to computers and computer networks. Although most EU Member States have statutes prohibiting "mere access" of systems without authorization, some states attach further requirements in order to trigger criminal penalties. In Germany and the Netherlands, for example, the law against unauthorized access protects only "secure systems" for which some effort has been made to inhibit open access. In Spain, some damage to the penetrated system must occur for criminal sanctions to apply. Ulrich Sieber has noted that some general antihacking provisions, such as those in the United Kingdom and Finland, have a built-in progression from a "basic" hacking offense to more serious forms of conduct implicating "ulterior" offenses.[12]

One area in which the national laws of European countries are significantly in agreement is that of computer sabotage, which encompasses purposeful damage to the integrity of computers, computer networks, and computer data. Variation in the extent of protection afforded to computer-stored data (CSD) among the criminal laws of European states is, according to Sieber, rooted in varying requirements of intent and degree of damage caused that underlie vandalism or criminal mischief statutes more generally.[13] States with statutes specifically protecting CSD include Austria, Denmark, Germany, Finland, France, Luxembourg, the Netherlands, Spain, Sweden, and the U.K.; so far in Europe, the enactment of laws prohibiting computer sabotage and the destruction of data includes only a small number of national provisions directed specifically against the creation or distribution of destructive programs, such as viruses, worms, or Trojan horses. Italy, Sweden, and the Netherlands are among the handful of countries that have included such provisions in their respective criminal codes. Only

"Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study" (1998), prepared for the European Commission by Dr. Ulrich Sieber, University of Würzburg, Germany.

12. Ibid., p. 72.
13. Ibid., p. 78.

Germany and Italy have promulgated laws directed specifically against forms of computer sabotage "leading to the obstruction of business or national security."[14]

The degree of protection afforded by national laws of EU Member States against computer espionage has in many cases been achieved by extending the coverage of laws protecting trade secrets to computer and data processing. Denmark, Germany, the Netherlands, Sweden, and the U.K. have all enacted provisions to reinforce trade secret protection. Civil provisions aimed at discouraging unfair competition in Europe have attained a significant measure of harmonization through First Pillar initiatives in the European Union. By contrast, the criminal sanctions that underlie those policies are anchored in varying national traditions relating to the legal protection of various types of property, including intellectual property, and thus exhibit greater variation. Sieber notes that, whereas intellectual property is an established category in the common law tradition, the civil law (or "continental law") tradition "does not regard information as per se protectable."[15] The situation is similar with respect to computer fraud and computer forgery. While all Member States of the European Union criminally sanction fraudulent acts in general terms, not all have statutes specifically directed against computer fraud.[16] European states that have promulgated laws against computer forgery include Germany, Finland, France, Greece, Luxembourg, and the U.K. Sieber explains that

14. Ibid.

15. For example, civil law states tend to take a much narrower view of the exclusive ownership rights that accrue under copyright, trademark, and patent law. Ibid., p. 75.

16. The countries that have enacted computer fraud statutes include: Austria, Denmark, Germany, Finland, France, Greece, Luxembourg, the Netherlands, Spain, Sweden, and the U.K. Sieber notes that the absence of a computer fraud statute can complicate catching fraud by means of financial manipulations, because many national statutes, including those of Italy and Germany, require deceit of a "person," which leaves untouched a host of offenses involving electronic misappropriations. The fraud statutes in Belgium and France require an "abuse of confidence" as a trigger. Normally, abuse of confidence is understood to apply only to actors in high positions and may not extend to low-level programmers and operators. See ibid., pp. 82–83.

many of the remaining states have forgery statutes that can be extended without difficulty to cover computer forgery. However, in Austria, Belgium, and Italy—none of which has computer forgery statutes—the traditional forgery statutes in force limit protection to "visually readable" documents, thereby excluding electronic and computer stored data from protection.[17]

A survey of national legal initiatives in Europe would not be complete without a few words regarding European Union–level initiatives that increasingly place important limitations on the legislative autonomy of EU Member States. The Council of the European Union has been the most important engine driving EU Member States toward a harmonized approach to combating computer-related crime, but combating computer-related crime inside the European Union is complicated by the fact that the issue straddles important divisions in the EU structure. Issues mainly commercial or economic-regulatory in nature, including, for example, telecommunications, fall within the purview of the European Community, which forms part of the First Pillar of the EU's three-pillar structure.[18] Harmonization in the criminal legal sphere, together with questions of law enforcement and judicial cooperation, are handled under the Third Pillar, Justice and Home Affairs. Whether a matter is handled as a First Pillar or a Third Pillar issue is key to determining the available mechanisms for attempting to bind Member States to a common course of action. The situation is further complicated by the fact that one and the same body, the

17. Ibid., p. 81.

18. The three-pillar structure was established in 1993 under the Treaty of the European Union (TEU) signed at Maastricht. Under this treaty, the First Pillar contains three components, the most important of which is the European Community (EC) (formerly the European Economic Community). The other two components are the European Coal and Steel Community (ECSC) and the European Atomic Energy Community (Euratom). The Second Pillar of the European Union structure is Common Foreign and Security Policy (Title V, TEU). Justice and Home Affairs forms the Third Pillar (Title VI, TEU). See Josephine Shaw, *Law of the European Union*, 2d ed. (London: Macmillan, 1996).

Council of the European Union, can operate under either set of rules, depending upon the question at hand.

Under the Third Pillar, the Council of the European Union acts as an intergovernmental body of national representatives, and not in the legislative capacity it serves under the First Pillar. This means, for example, that when acting in a Third Pillar capacity, the Council operates under a "unanimity" decision rule, as opposed to the "qualified majority" rule normally used for First Pillar affairs. In addition, under the First Pillar, the Council is empowered to issue, in accordance with the rules of co-decision with the European Parliament, Directives and Regulations that are binding upon Member States, and enforceable by the European Court of Justice. By contrast, under the Third Pillar constraints, Council decisions are more akin to traditional international agreements and are therefore not directly enforceable through First Pillar mechanisms. However, the gulf between First and Third Pillar capacities is narrowing slowly as European integration progresses. Under Article 34 of the Amsterdam Treaty adopted in 1997, the Council, acting in its Third Pillar capacity, acquired the power to issue legally binding framework decisions. With regard to the national laws discussed above, this means that the Council may now affirmatively require Member States to bring national legislation into concordance with EU standards in areas where the EU chooses to "occupy the legal field," thereby overcoming at least those points of national difference that inhibit realization of the EU policy.

And the EU has chosen to act in this area. Dietrich Neumann explained that the work undertaken in the European Union in the field of cyber crime has not been directed toward drafting a unified legal instrument.[19] Rather, the EU approach has sought to take into account and, where possible, to complement initiatives in the Council of Europe, the OECD, and the G-8.[20] Neumann points out that one way

19. Dietrich Neumann, Stanford Conference, Session Two, pp. 6–7.

20. Drew C. Arena identified the primary legislative measures specific to computer crime enacted by the EC and the EU, as the 1995 and 1997 Directives on Data

forward could have been to formally associate EU efforts with work in other international forums, without developing separate EU initiatives in order to avoid a duplication of effort. However, he argues, "the legislative and regulatory system of the EU allows much more effective action than would have been possible in other forums." Accordingly, the strategy adopted is to associate with existing initiatives where it makes sense and to develop EU instruments where necessary."[21] In concrete terms, these efforts have ranged from the promulgation of new legislation, to funding law enforcement training for investigation of high-tech crime, to initiatives to encouraging more regular coordination between First Pillar and Third Pillar institutions (for example, between telecommunications and law enforcement).[22]

Common Concerns

States in the international system differ widely in their vulnerability to criminal activity perpetrated against or by means of computers and computer networks.[23] They also differ widely according to the degree of threat they face from criminal and terrorist attacks, both domestically and internationally.[24] To a considerable extent, the observable variation in states' reactions to the growing potential for cyber crim-

---

Protection, the 1995 Council Resolution on the Lawful Interception of Telecommunications, the 1997 Council Resolution on Illegal and Harmful Content on the Internet. Pending measures include a Joint Action or Framework Decision on Child Pornography on the Internet and a Directive concerning electronic commerce. More recently, however, computer crime has been addressed at the strategic level in the European Union under the rubric of actions being taken to combat organized crime.

21. D. Neumann, p. 3.

22. See "Action Plan to Combat Organized Crime," adopted by the Council of the European Union on April 28, 1997, Official Journal C 251, 15/08/1997, pp. 0001–0016; see also Council document 11893/2/98, CRIMORG 157 REV 2, a 1998 statement outlining the EU approach to high-tech crime in ten strategic guidelines.

23. A state's vulnerability to computer crime and computer terrorism is a "technical issue" directly related to the degree of computerization of each state's national economy and infrastructure.

24. The "threat" posed to a state by cyber criminals refers to the motivation (economic, ideological, or otherwise) of others to exploit a given state's level of vulnerability, and therefore constitutes a factor distinct from mere vulnerability.

inal and terrorist activity can be explained with reference to these two dimensions.

The sizable group of states that have, or will soon have, laws directed specifically against cyber crime include the most highly industrialized countries, which, as a rule, are also the most dependent upon computers and computer networks. This group also includes a number of countries less dependent upon information technology (IT) that nevertheless share important economic and trading relationships with the IT giants.[25] Not surprisingly, the least computerized societies have been the slowest in passing national legislation against computer crime. Among countries in the Asia-Pacific region, for example, the toughest and most detailed cyber crime laws have been passed in states with the most highly industrialized and highly computerized economies, as exemplified by Taiwan, Japan, and Singapore.[26] States with little or no legislative action on cyber law have low levels of computerization and low reliance on network infrastructures, and they face little or no internal vulnerability from acts of high-tech crime and terrorism. But the very lack of vulnerability to cyber attack among states with low IT dependence is cause for concern in states that perceive a high threat of cyber attack, since the absence of internal vulnerability to cyber attack correlates strongly with a failure to take national legislative action to criminalize such offenses. Network attack

25. Arena pointed out in his Stanford Conference paper that even within this group, consensus on the recognition of the threat is quite new. He related that "only a few years ago, as the United States attempted to discuss the need for protection of critical infrastructure from cyber attack with colleagues from other very developed (but not as IT-dependent) countries I was often politely told that our concern was reminiscent of those who worried [in 1968] that student radicals would spike U.S. urban water supplies with LSD."

26. Although the cyber laws in the People's Republic of China are notable for their "toughness," as Chen pointed out, they are drafted more broadly than those of Taiwan, Japan, and Singapore, which makes them applicable in a wider set of potential circumstances. This difference in approach is probably explained by the greater degree of direct control maintained by the PRC government over most forms of private and public communications. Note that no information on South Korea was included in Chen's research.

can be launched from virtually any geographic location against any other with an international telephone connection, and some countries can become legal operating bases and safe havens for cyber criminals in their attacks against IT-vulnerable states.

Addressing the failure of some states to respond to the threat of cyber crime and cyber terrorism will almost certainly demand differentiated tactics and incentives. In some instances, traditional political pressures at the regional or international organizational level may be sufficient to prompt legislation to bring the laws of less IT-dependent states into line with international minimum standards. Among the least economically well-off states, forging policy may require more tangible incentives along the lines of development assistance and technological transfers already familiar in other areas of international coordination. Even among states that have chosen independently to adopt legislation criminalizing cyber offenses, effort is needed to coordinate national responses both in terms of specifying offenses and in applying the laws that are enacted to cross-border illegal acts. Without measures that actively coordinate national actions and policies at the international level, the amalgam of national cyber laws and policies is unlikely to result in a coherent framework for the identification, investigation, and prosecution of computer crimes occurring within or affecting multiple jurisdictions at any time in the near future.

2. In Search of a Working Consensus

How, then, is it possible to recognize when consensus is present to a degree that could lead to an internationally acceptable but nevertheless substantive prohibition regime? The search for a working consensus demands both finding specific points of agreement and determining an overarching structure within which to frame those points. The purpose of the following survey is to suggest what the points of existing consensus might be and to contextualize them within a larger view of what, ideally, has to be done so that the level of consensus that exists can be put into effect.

In this section we identify two areas in which some level of consensus is necessary if law enforcement and judicial actors working from within various national jurisdictions are to be effective in identifying, investigating and prosecuting computer offenses. The first area is that of specifying what conduct will be treated as a criminal offense. Because this area shows the most potential for formal agreement in the short term, it is the main focus of the Draft Convention. The second area concerns points of existing consensus on what rules and procedures should dictate the scope and extent of operational powers enjoyed by law enforcement and judicial authorities inside their respective spheres of jurisdiction.

Condemnation of Specific Conduct

To cooperate across national borders, whether at the level of bilateral contacts in the course of an actual investigation or in the context of multilateral negotiations to establish a framework agreement, legal systems must agree that certain acts should be prohibited and punished. Particularly in the criminal sphere, international law enforcement and judicial cooperation depend upon at least general agreement on what conduct should be regarded as punishable offenses. The principle of double criminality, for example, prohibits extradition of a fugitive to a requesting state unless the offense charged is a crime in both states. In practice, this principle also extends to mutual legal assistance in gathering evidence in the course of a criminal investigation, particularly when the acts of discovery in question are considered intrusive.[27] Without a minimum basis for agreement, therefore, multijurisdictional computer crimes will not be fully investigated, and, as a consequence the perpetrators of those crimes will in many cases go unidentified and unpunished.

Several multilateral efforts to coordinate national responses to the

27. *U.N. Manual on the Prevention and Control of Computer-Related Crime* (1994), ¶ 270. See ⟨*http://www.ifs.unvie.ac.at/~pr2gq1rev4344.html/*⟩ (visited March 17, 2000).

threat of cyber crime have devoted considerable attention to the specification of offenses. The Council of Europe (COE),[28] the Organization for Economic Cooperation and Development (OECD), Interpol, the United Nations Committee on Crime Prevention and Criminal Justice,[29] and the European Union have all been active in various capacities. Additional organizations are becoming involved at a rapid rate: the Commonwealth Secretariat, the Organization of American States (OAS), and the Association of Southeast Asian Nations (ASEAN) have all recently initiated projects on international harmonization of law relating to computer crime among their members.[30] Drew Arena points out that these groups, many of which have overlapping memberships, have taken some pains "to exchange views and avoid duplication or conflicting approaches" in addressing international shortfalls associated with computer-related crime.[31]

The Council of Europe is so far the only organization to have made considerable progress toward negotiating an international multilateral agreement for the specification and criminalization of an enumerated

28. The Council of Europe was formed in 1949 as a standing forum for the promotion of democracy, human rights, and the rule of law among its members. In 1989, the organization's membership began to expand from the original ten Western European states to its current total of forty-one states, which includes many of the newly independent former Soviet republics and former Eastern bloc states. The COE should not be confused with either the European Council or the Council of the European Union, both of which are components of the entirely distinct European Union treaty structure. Unlike EU bodies, the COE has no power to issue binding instruments for its members. Instead, the COE operates primarily through negotiated conventions, roughly 160 to date, that its members are encouraged to adopt and implement.

29. According to Drew Arena, the primary contribution of the UN Committee, to date, has been the publication of its "Manual on Computer-Related Crime" in 1994.

30. The efforts of the Group of Eight, whose most noteworthy contributions have been in the sphere of procedural coordination, are discussed in the following subsection.

31. In Arena's words: "For example, representatives of the Eight and the EU Commission participate in the Council of Europe Committee; the Council of Europe has an observer in the G-8 Subgroup, and the EU hosts annual meetings of the Council of Europe, G-8 and OECD groups."

set of cyber offenses.[32] The Draft COE Convention on Computer-Related Crime concentrates largely on crimes directed against the "confidentiality, integrity and availability of computer data and systems"—"c.i.a.-offenses" for short. These offenses, which Arena also refers to as "pure" computer crimes, are qualitatively "new" offenses that are not readily classifiable under old statutory categories, particularly in countries without some experience in dealing with offenses against nontangible forms of property.[33] The five "consensus crimes" discussed by COE members are: (1) illegal access, (2) illegal interception, (3) data interference, (4) system interference, and (5) the production and distribution of illegal devices that may be used in the commission of any of the first four acts. Offenses against the possession (that is, taking without violating confidentiality), authenticity, and utility of information, although not spelled out explicitly in the Convention, are covered under Article 7 (computer-related forgery). A consensus has also emerged among COE members condemning certain offenses related to child pornography.[34] The aiding and abetting of

32. The UN General Assembly has also created an Ad Hoc Committee to draft a Convention on Transnational Organized Crime before the end of 2000. Arena notes (p. 2) that "in addition to certain references to computer-related issues in the draft text (for example in the context of mutual legal assistance) many states feel that eventually a protocol to this convention specifically addressing cyber crime should be negotiated."

33. Offenses such as "computer fraud" and "computer forgery" essentially entail the application of a new technology to commit an old crime and are therefore easily caught by existing fraud and forgery statutes, but the fact that so many lawmaking bodies in cyber law states have seen fit to promulgate statutes specifically outlawing *computer* fraud suggests that there may be some merit in a distinctive approach. As noted in the *U.N. Manual on the Prevention and Control of Computer-Related Crime*, "the criminal codes of all countries have, up to the present, predominantly protected tangible and visible objects" (¶ 84). Protection for intangible forms of property, such as "intellectual property" and copyright evolved over the course of the twentieth century but has been robustly enforced only in a relatively small number of countries. Even in jurisdictions accustomed to regulating intangible property, the extension of those protections to electromagnetic data and the integrity of information has necessitated new legislative responses.

34. Dietrich Neumann observed that even this modest degree of consensus around a content offense is rather remarkable given the range of opinion regarding the boundaries of free speech among Council Member States and around the globe. Content-

computer offenses is also punishable under the Council of Europe Draft Convention, as is the attempt to commit a criminal act, although detail regarding the contours of these latter offenses has yet to be enumerated.

Still, after more than three years of negotiation, the Draft Convention on Computer-Related Crime has yet to reach final approval.[35] Thus, although there is much to recommend the thorough approach of the Council of Europe's Draft Convention, the effort will require several additional years of negotiation before entering into force. In the meantime, the threats posed by cyber criminals and terrorists will continue to mount internationally as the vulnerability to attack grows.

The Council of the European Union,[36] in its ongoing effort to bridge Council of Europe efforts, issued its "Common Position of 27 May 1999 on negotiations of the European Union relating to the Draft

---

related offenses are particularly difficult to standardize and harmonize because they implicate some of the most closely held values on which different nations are constructed. For example, in Germany and Italy, both states with fascist periods in their past, legal tolerance for hate speech is low. By contrast, in the United States, the First Amendment to the Constitution establishes an extremely high barrier against government censorship on the content of speech, so much so that it protects the dissemination of information (scripts, codes, and the like) needed to perpetrate many of the crimes under discussion.

35. The project was launched in 1997 on the initiative of the Council's Committee of Experts on Cyber Crime. Committee members include Member States of the European Union, Central and Eastern European states, and also a number of active observer states, including the United States, Canada, and Japan.

36. The Council of the European Union, also known as the Council of Ministers, is a body of officials holding ministerial positions within their states who are empowered to commit their governments on policy matters. The Council of the European Union carries out its work mainly through specialized subcommittees. It holds primary control over approval of the EU budget and also has the power to conclude international agreements between the EU and third states and international organizations. It functions as the coordinating body for police and judicial cooperation among EU Member States. As noted earlier (note 28) the Council of the European Union should not be confused with the European Council, which is the body consisting of the heads of state of the EU members, plus the president of the European Commission and the European Parliament that meets only at "European Summits" held biannually.

Convention on Cyber Crime."[37] In this document, the Council articulated what it perceived to be specific points of emerging consensus, including agreement on features most in need of future inclusion in the Council of Europe Draft Convention. The Council of Europe/European Union effort has sought, in Neumann's words, "ways to overcome, or at least reduce procedural obstacles that hamper international computer crime investigations and which partly relate to the principles of territoriality and national sovereignty." This effort is helped by a number of general measures instituted by the EU to facilitate police cooperation at the operational level[38] and to simplify requirements for the extradition of criminal fugitives among Member States.[39] The European Union has also encouraged its Member States to enact national legislation to facilitate mutual legal assistance in the search and seizure of evidence from organized crime and high-tech crime.[40]

The OECD has also been an active player in efforts to achieve

37. See Official Journal of the European Communities No. L 142, June 5, 1999, p. 1.

38. See, e.g., Joint Action of November 29, 1996, adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning the creation and maintenance of a directory of specialized competences, skills, and expertise in the fight against international organized crime, in order to facilitate law enforcement cooperation between the Member States of the European Union (96/747/JHA); Joint Action of June 29, 1998, adopted by the Council on the basis of Article K.3 of the Treaty on European Union, on good practice in mutual legal assistance in criminal matters (OJ L 191, July 7, 1998, pp. 0001–0003); Act of the Management Board of Europol of October 15, 1998, concerning the rights and obligations of liaison officers (OJ C 026, January 30, 1999, pp. 0086–0088); and the Draft Council Act establishing the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (OJ C 251, September 2, 1999).

39. See Council Act of March 10, 1995, adopting a simplified procedure for extradition (OJ C 78, March 30, 1995).

40. See, e.g., "Council Act of March 12, 1999, adopting the rules governing the transmission of personal data by Europol to third states and third bodies," Council Document 10888/99; Council Resolution of January 17, 1995, on the law interception of telecommunications (OJ C 329, November 11, 1996).

harmonization in the cyber laws of its Member States.[41] Like the approach adopted by the Draft Convention presented in this volume, the OECD initiative has sought to identify and build upon existing areas of international consensus. However, the OECD has not attempted to draft a formal agreement, instead confining its efforts to issuing recommendations and guidelines for action. In 1986 the OECD released its first report on cyber offenses, "Computer-Related Crime: Analysis of Legal Policy," which surveyed existing laws and proposed a minimum list of five substantive offenses that it recommended strongly for criminalization by OECD members. Those offenses are (1) unauthorized access, (2) illegal computer transfer of data or funds, (3) forgery, (4) interruption of service, and (5) illegal appropriation and exploitation of data or software. In 1992 OECD issued "Guidelines on the Security of Information Systems" together with a mandate for a periodic review of those guidelines every five years. The most recent set of guidelines, issued in March 1997, is a set of Cryptography Policy Guidelines, together with an extensive comparative report on cryptography policy.

Several of the Stanford Conference panelists cautioned that apparent patterns of coincidence in the choice of rules and terms may not represent a true consensus but may instead mask widely varying patterns of practice. Laws that appear to be similar or identical from a drafting perspective may be enforced differently by law enforcement and criminal justice officials acting entirely in good faith, owing, for instance, to differing interpretations of key terms or different views regarding the law's intended scope.[42] The potential for variation in practice, they argued, is heightened by the absence of a common vocabulary with which to discuss issues of cyber crime and cyber terror-

41. Arena describes the OECD as having been "active in the field since at least 1980 when it issued its Guidelines on the Protection of Privacy of Transborder Flows of Personal Data."

42. The *U.N. Manual on the Prevention and Control of Computer-Related Crime* notes that there is no globally accepted general definition of computer crime and, consequently, functional definitions are customary for international initiatives (¶ 21).

ism. Marc Goodman noted in his conference presentation that because many national laws do not define basic terms, such as "computer network," "protected system," or "data interference," the laws in which those terms appear have uncertain scope of application.[43] But since this condition obtains in virtually every multilateral legal agreement between sovereign states, and it is not preclusive of a functional international regime. Given the relatively small number of major cyber attacks to date, we simply do not know whether and to what degree these ambiguities may pose problems for international cooperation. Nevertheless, we do know that similar obstacles have been successfully overcome in regulating international intercourse on the open sea and in international air traffic.[44]

More problematic from the perspective of international consensus-building are laws that define the scope of their coverage very narrowly. This point is illustrated by comparing some laws that prohibit "unauthorized entry" into computer systems. In the People's Republic of China, for example, the relevant law makes it a criminal offense to "access computers without permission," particularly computer systems important to state security; in India the law makes it an offense to enter "protected systems" only. In the United States, the federal law has broadened over time from protection of "government computers," to protection of "federal interest computers" and eventually to protection of "computers involved in interstate commerce." It is not difficult to imagine how loopholes and gaps can arise—for instance, in translating the American concept of a "federal interest computer" into a Chinese or Indian equivalent for purposes of extradition, or to request permission for search and seizure of data. In some cases, the narrowness of a formulation chosen by a national legislature is in-

43. By contrast, the entire first chapter of the Council of Europe's Draft Convention on Cyber Crime concerns the definition of the terms that will be used, "such as 'computer system,' 'data,' 'service provider,' 'traffic data,' 'search and seizure of data,' and many more."

44. See Chap. 3 of this volume for a detailed discussion of the development of the latter of these regimes.

tended to stimulate a particular response among private entities claiming protection under the law. Germany's statute against unauthorized access criminalizes only the penetration of "specially protected computers."[45] Statutes of this kind are drafted to induce system owners to take proactive steps to protect their systems against outside access, rather than placing the entire burden of deterring criminal acts on *post hoc* legal remedies, as is the case under federal law in the United States. The Draft Convention proposes a definition that would require system users to make clear they intend to restrict access.

Finally, the narrowness of statutes may in some cases be due to practical considerations of enforceability rather than to failure to appreciate wider levels of threat. More broadly drafted laws would in many cases implicate, on a systematic basis, actors and assets located in other jurisdictions, thereby complicating the process of application and enforcement. This suggests that actual levels of consensus regarding computer-related crime may be broader than is immediately apparent from a textual survey of legal codes.

Administration and Operation of Cyber Law

As difficult as reaching consensus on issues of substantive law appears to be, the difficulties multiply when the discussion turns to administration and procedure.[46] Whereas the purpose of substantive law is to

45. Sec. 202 a, Penal Code Computer espionage: Unauthorized procuring of data not meant for the offender or specially protected against unauthorized access; penalty is up to three years' imprisonment or a fine. (Attempt: not punishable.) The term "data" is explained in the comments on Sec. 303a of the Penal Code. "Procuring" data does not imply knowledge of the data. The offense also covers procuring data for a third party. The offender must have acted without the necessary authorization by the party entitled to dispose of the data. The "specially protected" criterion (required to constitute the offense) is not defined by the law. The victim must make his interest in keeping the data secret clear by providing a certain level of access security. Prosecution is subject to a complaint lodged by the victim. The provision protects not only stored data but also data in the course of transmission or processing.

46. In practice, procedural issues are never entirely detached from the substantive specification of an offense. The specification of the elements and seriousness of the offense are important in determining whether the system in question will take cogni-

delineate what private citizens may or may not do, the purpose of procedural law is to regulate what law enforcement and judicial officials may or may not do in administering and enforcing substantive law. Though encouraging a country to incorporate a small number of computer-related offenses into its criminal code is unlikely to have a large impact on the character of the system as a whole, the altering or carving out of exceptions to procedural rules in order to facilitate the identification or investigation of computer-related crimes may have important implications for the national legal systems in question.

The enforceability of laws against cyber offenses enacted at the national level becomes complicated when, as is frequently the case, the source, object, or path of an attack has its physical nexus in more than one country. The main procedural difficulty is not, as some early commentators suggested, the absence of territorial *nexi* in crimes committed via cyberspace, but rather the *plurality* of national connections, each of which may carry its own jurisdictional claims.[47] Even among the several United States, Susan Brenner found that questions of who has jurisdiction to do what with respect to investigating and prosecuting computer crimes in which state lines are crossed in cyberspace are hotly contested.[48] Arena illustrates the types of issues that may crop up even in a relatively straightforward scenario:

> Consider a corporate Internet [host] used by employees of a foreign company in a U.S. city with the system server in another country. U.S. agents obtain a valid warrant to search the computers at the U.S. office for particular evidence of fraud. If the evidence was entered from the site in the U.S. and is still accessible from there, does or

zance of a suspected violation, and, if so, what level of intrusiveness will be permitted during investigation.

47. For an excellent summary and discussion of this debate, see Jack L. Goldsmith, "Against Cyber Anarchy," *University of Chicago Law Review* 65 (Fall 1998): 1199.

48. This is not to say that such questions are entirely unsettled. A large body of jurisprudence, termed the "Conflict of Laws," is directed precisely at resolving jurisdictional contests in a rule-bound fashion in situations where a number of entities have colorable claims to jurisdiction. However, the Conflict of Laws is a notoriously muddy area of the law, in both its domestic and international application, not easily distilled into a set of reliable general guidelines.

> should the location of the server matter? What if the location of the server is unknown? Should the U.S. authorities have to seek help from the authorities in the country where the server is located through an international letter rogatory or a Mutual Legal Assistance Treaty to obtain the evidence? Or may they rely on their U.S. search warrant to access and download [the information] at the U.S. site?

Arena points out that the scenario could be easily complicated by the addition of other common considerations, notably "the number of nations involved, the presence or absence of extreme urgency, the existence of consent and its voluntariness, and the extent to which the data sought is protected by firewalls, passwords or encryption." He argues further that a government's opinion as to whether a particular search should be allowed quite frequently depends upon whether it is part of the "searching" state, or the state on whose territory the search will take place. Again, although Arena rightly identifies these factors as impediments to law enforcement and judicial action, such impediments do not, in many respects, constitute new problems for transnational law enforcement.

Officials at the national level have developed mechanisms, in the form of mutual legal assistance treaties (MLATs), to facilitate transnational law enforcement and judicial cooperation generally. Experts at the Stanford Conference agreed that standard mutual legal assistance procedures designed for access to paper documentation are necessary but insufficient for conducting investigations in cyberspace.[49] Dietrich Neumann explained that under the standard approach, formal requests must be addressed to the relevant authority in the home country, which then forwards the request to the appropriate authority in the recipient country, which must then approve and execute the request. Depending on the circumstances, the process can take weeks, months, or even years to complete. By contrast, traffic data and other potentially important sources of information about particular cyber

49. For example, identification of the source of a cyber attack can be made most efficiently while the criminal is still on-line, thereby necessitating an extremely rapid response on the part of investigators.

attacks are stored only temporarily in most servers and may become irrecoverable if not seized quickly. Two possible remedial approaches have emerged. The first is to find ways to accelerate traditional mutual legal assistance processes for the investigation of computer-related crimes in which rapid response is key. The second approach anticipates a qualitatively new regime of mutual legal assistance that would, for example, permit law enforcement officials limited powers of direct, cross-border search and seizure, subject to the post-search notification of the searched state.

Although attractive in theory, solutions that would require a drastic overhaul of the existing structure of mutual legal assistance may be beyond political reach, at least in the near future. Even in Europe, with its fairly robust consensus regarding substantive offenses, the COE Committee has made no significant progress on the search and seizure issue, leaving its draft article on transborder search "to be determined." Neumann summarizes the European situation succinctly: "Consensus has emerged where the more traditional concepts of mutual legal assistance were used for drafting provisions of this [COE] Convention. Agreement could also be reached when it came to defining consensus crimes. Difficulties arise, however, where the Convention tries to widen the traditional concepts and therefore enters into conflict with principles such as national sovereignty and territoriality." Thus, the COE has limited itself to constructing the obligation to cooperate "to the widest extent possible" on procedural matters out of broad formulations. These include the "General principles relating to international cooperation" (Art. 20 of Draft No. 18) together with specific provisions on "Extradition" (Art. 21), "Mutual Assistance" (Art. 22), and provisional measures for the expedited preservation of stored computer data (Art. 24). In the European Union, the Council of the European Union's Common Position of May 27, 1999, took a further extraordinary step of endorsing, in general terms, the need for a provision permitting, in exceptional cases, transborder computer searches with post-search notice to the State Party. However, attempts to ne-

gotiate this point reportedly became ensnared by differing visions regarding the details and conditions of its use.

Outside the European context, the Group of Eight (G-8), and in particular the High-Tech Subgroup of the Senior Experts on Transnational Organized Crime, have been at the forefront of the multilateral effort to improve international cooperation in obtaining evidence of computer-related crimes.[50] In October 1999 the G-8 ministers adopted "Principles on Transborder Access to Stored Computer Data."[51] The first section of this document requires states to react quickly to requests for the preservation of electronic data, "in particular data held by third parties such as service providers, and that is subject to short retention practices or is otherwise particularly vulnerable to loss or modification." The second section concerns expedited handling of requests to search data thus seized. The idea, in Arena's words, is a "quick freeze, slow thaw" arrangement by which law enforcement and judicial bodies can fulfill their procedural obligations under domestic law for release of information to foreign law enforcement or judicial officials without risking the loss of critical data. Although the principles may appear "fairly modest" in terms of resolving the overall problem, Arena maintains that the G-8 principles lay the basis for an effective interim international regime for the preservation of electronic data.

The third section of the G-8 Principles, "Transborder Access to Stored Data Not Requiring Legal Assistance," addresses the question

50. Arena notes that the Subgroup was created in 1997 at the beginning of the U.S. Presidency of the G-8, and was chaired initially by Scott Charney, then chief of the Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice. The group of Senior Experts antedates the Subgroup by only two years. It is often called the "Lyon Group" on the basis of a group of 40 Recommendations on Combating Transnational Organized Crime that were adopted at the group's 1996 summit in Lyon, France. In 1998, a set of Ten Principles and a Plan of Action were announced by the Justice and Interior Ministries of the G-8 members at the Washington meeting, and were subsequently ratified at the 1998 Birmingham Summit.

51. Arena notes that "the Subgroup is currently working on the problem of locating and identifying computer criminals in a global environment, and will hopefully be able to develop principles in this area."

of whether *any* direct penetration of foreign jurisdictions via cyberspace is permitted by outside law enforcement officials in the context of a criminal investigation. The answer in the affirmative specifies that "a State need not obtain authorization from another State when it is acting in accordance with its national law for the purpose of: a) accessing publicly available (open source) data, regardless of where the data is geographically located; b) accessing, searching, copying, or seizing data stored in a computer system located in another State, if acting in accordance with the lawful and voluntary consent of a person who has the lawful authority to disclose to it that data." The sole procedural requirement that attaches to such searches is a post-search notification of the searched State that a search has occurred. In sum, the progress achieved by the G-8 demonstrates that significant steps can be taken to facilitate the investigation of computer-related crimes within the context of traditional mutual legal assistance. At the same time, the third section of the October 1999 G-8 Principles suggests that incremental advances toward a more ambitious transnational investigative regime are possible even now.

3. Toward International Consensus?

The information surveyed in this chapter suggests that a significant degree of consensus exists regarding certain types of prohibited conduct in cyberspace. The roster of prohibited acts enjoying a measure of de facto international consensus runs the gamut from "pure" offenses against the confidentiality, integrity, and availability of computers and computer networks to traditional offenses like fraud and larceny in which computers are a material element. The level of consensus identified in this survey is not particularly "deep" in the sense that, in many instances, it probably does not extend to a detailed specification of computer-related offenses or to common definitions of the "objects" or instruments involved. However, in the opinion of the authors of the Draft International Convention, it is enough to permit formalization on a meaningful level.

The successes and failures apparent in the ongoing efforts of international and regional organizations, considered together with the cyber-crime laws that have been promulgated by concerned states, reveal a great deal about where short-term agreement may be possible, and where it is not. If ratified by a significant number of States, the proposed International Convention to Enhance Protection from Cyber Crime and Terrorism could constitute a meaningful step in coordinating the promulgation and enforcement of existing laws against computer crime and in further closing off legal loopholes and eliminating safe havens for cyber criminals. Indeed, the most persuasive argument in support of a formal, multilateral effort at this juncture is the magnitude of the threats and vulnerabilities against which these measures are directed. In this recognition lie the seeds of effective international action, even as differences in national law and traditional repertoires of transnational law enforcement and judicial cooperation constrain the menu of short-term responses. Experience is showing that national governments are increasingly willing to cooperate in foreign investigations. Director of the National Infrastructure Protection Center Michael A. Vatis reported that in the investigation of the February 2000 e-commerce denial of service attack, "for the first time . . . investigators had sought and received cooperation from foreign governments."[52]

As for the multitude of offenses that fall outside the set of "consensus crimes" identified here, Arena maintains that a lack of consensus may for the present actually be a desirable state of affairs. Absence of consensus lends itself to legal and technical experimentation, which in turn increases the likelihood of happening upon effective solutions that may be foreclosed by premature formalization at the international level. Although this chapter has dealt primarily with proposed short-term steps in the legal sphere, the legal-deterrence approach can and should be reinforced by further developments on the technical side. In the technical realm, harmonization is likely to be helped by the fact

52. Matt Richtel, "Official's Testimony Hints at Slow Progress on Internet Attacks," *New York Times*, March 1, 2000, p. A16.

that the technology of security and enforcement is likely to have its source in only a few states. Arena echoed the arguments of Peter Neumann and Richard Power at the Stanford Conference, in positing that the way through the international political maze will probably be found in the free market. Increasingly reliable measures of how much high-tech crime in electronic commerce is costing at the enterprise level have already begun to drive demands for better IT security. Improved cost measurements will also increase awareness of the costs associated with the inefficiencies of transnational fight against computer crime due to outdated agreements for mutual legal and judicial assistance.

In the meantime, progress on the difficult questions can be helped along by demonstrated successes in areas where consensus already exists. Experimentation in transnational law enforcement and judicial cooperation will undoubtedly proceed by means of bilateral agreements among states with similar interests, and through practical lessons learned from investigating and prosecuting cyber offenses. It is to be expected that the de facto regime of multilateral cooperation and consensus will continue to expand and may, over time, pave the way to more comprehensive international legal solutions.

Understanding cybercrime: Phenomena, challenges and legal response. Purpose.Â Cybercrime often has an international dimension.58 E-mails with illegal content often pass through a number of countries during the transfer from sender to recipient, or illegal content is stored outside the country.59 Within cybercrime investigations, close cooperation between the countries involved is very important.60 The existing mutual legal assistance agreements are based on formal, complex and often time-consuming.Â As these crimes differ in many ways, there is no single criterion that could include all acts mentioned in the different regional and international legal approaches to address the issue, whilst excluding traditional crimes that are just facilitated by using hardware.