THE CRITICAL CHALLENGES FROM INTERNATIONAL HIGH-TECH AND COMPUTER-RELATED CRIME AT THE MILLENNIUM

MICHAEL A. SUSSMANN*

I consider high-tech crime to be one of the most serious issues demanding my attention, and I am doing everything in my power to ensure that the United States actively responds to these challenges.

U.S. Attorney General Janet Reno, January 21, 1997[1]

I. INTRODUCTION

There is a revolution going on in criminal activity. It creates major problems for law enforcement in almost every part of the world—problems that have rarely been as systemic and pervasive.

The revolution lies in the ways that networked computers and other technologies permit crimes to be committed remotely, via the Internet and wireless communications. A criminal no longer needs to be at the actual scene of the crime (or within 1,000 miles, for that matter) to prey on his victim. The possibility of an international element has been added to almost any crime, which means that cumber-

* Senior Attorney, Computer Crime and Intellectual Property Section, U.S. Department of Justice. From 1993-96, the author was Special Assistant to the Assistant Attorney General for the Criminal Division of the U.S. Department of Justice. The views expressed in this article are those of the author and do not necessarily represent the views of the United States. The author wishes to thank the following individuals for providing materials and editing manuscript drafts: Drew Arena, Scott Charney, Claudia Flynn, James Freund, Sam Hollander, Adam Isles, and Sara Maurizi.

1. U.S. Attorney General Janet Reno, Keynote Address to the Meeting of the G-8 Senior Experts' Group on Transnational Organized Crime, Chantilly, VA (Jan. 21, 1997) (transcript available at <http://www.usdoj.gov/criminal/cybercrime/agfranc.htm>) [hereinafter Reno, Chantilly Keynote Address]. The G-8 is an international multilateral group consisting of Canada, France, Germany, Italy, Japan, Russia, the United Kingdom, and the United States. During the 1990s, there were different names for this group, such as "G-7 plus Russia," "P-8," "The Eight," and "G-8," but all of the different monikers refer to the same group of countries. Use throughout this Article of different G-8 names is for accurate referral to source materials and is not intended to confer any other meaning. The genesis, mandate, and current work of the G-8 are discussed at length, *infra*, at Section IV(C).

some mechanisms for international cooperation can slow or derail many more investigations than ever before.[2] Because everything from banks to phone systems to air traffic control to our military relies so heavily on networked computers, few individuals and institutions are impervious to this new and threatening criminal activity.[3]

Take the case of a criminal sitting in Russia who routes a communication through Sweden and Italy before hacking into a bank in New York. The Federal Bureau of Investigation (FBI) may not be able to solve the crime without the immediate help of Russian, Swedish, and Italian authorities. And the immediacy is critical because a criminal's trail often ends as soon as he disconnects from the Internet. To make matters worse, technical solutions, laws and legal processes, and cooperation among governments and with industry are far behind where they need to be for law enforcement to stay a step ahead of the bad guys. Finally, not enough people realize this threat exists on the scale it does. Commenting recently about the public's awareness of the threat to our nation's computers from invisible attacks, Richard Clarke, the current White House "terrorism czar" said:

> [CEOs of big corporations] think I'm talking about a 14-year-old hacking into their Web sites. I'm talking about people shutting down a city's electricity, shutting down 911 systems, shutting down telephone networks and transportation systems. You black out a city, people die. Black out lots of cities, lots of people die. It's as bad as being attacked by bombs . . . . Imagine a few years from now: A President goes forth and orders troops to move. The lights

2. *See, e.g.*, Scott Charney & Kent Alexander, *Computer Crime*, 45 EMORY L.J. 931, 948 (1996) (stressing the need for an organized international response to the worldwide problem of computer crime).

3. *See Hearings on Infrastructure Protection Before the Subcomm. on Technology, Terrorism and Government Information of the Senate Judiciary Comm.*, 105th Cong. (1998), *available in* 1998 WL 12761104 (statement of Michael A. Vatis, Deputy Assistant Director, Federal Bureau of Investigation and Chief, National Infrastructure Protection Center) [hereinafter Vatis Testimony]. "This Nation depends on the stable, consistent operation of our critical infrastructures for our way of life, our well-being and our security. These include: telecommunications, energy, banking and finance, water systems, and emergency services, both government and private . . . . And the infrastructures are more interdependent than in the past, with the result that debilitation or destruction of one could have cascading, destructive effects on others." *Id*. *See generally* PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS: PROTECTING AMERICA'S INFRASTRUCTURES 3-20 (1997). The President's Commission on Critical Infrastructure Protection was created by President Clinton under Executive Order 13010 to study the problem of infrastructure protection in depth and develop proposed solutions. *See id.* at vii.

> go out, the phones don't ring, the trains don't move. That's what we mean by an electronic Pearl Harbor.[4]

At the dawn of the new millennium, at least some modern-day Paul Reveres are raising the alarm. A growing number of law enforcement officials in the United States and abroad are increasing awareness and calling for enhancement of high-tech crime-fighting abilities.[5] Likewise, the international community is beginning to take important action to address this threat to public safety.[6] But in many ways we are just scratching the surface; the long road ahead is going to require leadership, innovation, and persistence.

This Article will, first, examine the specific challenges posed by criminals who use computers and networked communications to ply their craft; second, discuss what needs to be done to effectively combat high-tech crime; and third, examine what steps are currently being taken in this area by some of the major multilateral organizations, such as the Council of Europe, the European Union, and the G-8. I will offer my assessment of the work being performed by international groups, and will draw specific attention to areas where efforts are inefficient or non-existent.

II. THE CHALLENGES

Imagine this scene out of tomorrow's headlines: A hacker, going on-line through the Internet, breaks into computers that the Federal Aviation Administration (FAA) uses for air traffic control. He dis-

---

4. Tim Weiner, *The Man Who Protects America From Terrorism*, N.Y. TIMES, Feb. 1, 1999, at A3. Mr. Clarke has a sign in his office that reads "Think Globally/Act Globally." *See id.*

5. *See, e.g.*, Paul Boateng, Minister of State for the Home Office (U.K.), Tomorrow's Challenges for Law Enforcement, Keynote Address to the Second International Conference for Criminal Intelligence Analysts (Mar. 1, 1999) (transcript on file with the *Duke Journal of Comparative and International Law*) (announcing the formation of a Ministerial Committee on computer misuse).

> [C]ommercial organisations may find it ever more problematic securely to maintain their business transactions, and . . . criminals and criminal enterprises may find an increasing number of opportunities to manipulate systems to their advantage . . . By virtue of the interconnectivity of computer systems in both the private and the public sectors, there is also the growing danger that a criminal attack on one part of a system could lead to the failure of the rest. Moreover, the perpetrator can now just as easily be a 15 year old 'surfer' in Wigan—tomorrow's cyberwarrior—as a professional gang of 50 year old fraudsters in Wisconsin. We must prevent such people from making these attacks.

Id. at 7. (The Minister of State for the Home Office in the United Kingdom is equivalent in rank to the Deputy Attorney General of the United States.)

6. *See infra* Section IV (discussing work in this area being done by international multilateral organizations).

rupts a regional air traffic network, and the disruption causes the crash of a DC-10 in the Rocky Mountains, killing all aboard. The FAA and the FBI know there has been a hacker intrusion, originating through the Internet, but nothing else. Since anyone can access the Internet from anywhere in the world, the FBI has no idea where the hacker may be located. Moreover, they do not know the motive of the attack or the identity of the attackers. Is it a terrorist group, targeting the United States and likely to strike again at any time, or is it a fourteen-year-old hacker whose prank has spun tragically out of control?

Let us follow this scenario a bit further. Within thirty minutes of the plane crash, the FBI tracks the source of the attack to an Internet Service Provider (ISP) in Germany. Assuming the worst, another attack could occur at any time, and hundreds of planes in flight over the United States are at risk. The next investigative step is to determine whether the ISP in Germany is a mere conduit, or whether the attack actually originated with a subscriber to that service. In either case, the FBI needs the assistance of the German ISP to help identify the source of the attack, but it is now 3:00 a.m. in Germany.

- Does the FBI dare wait until morning in Europe to seek formal legal assistance from Germany or permission from the German government to continue its investigation within their borders?
- Does the Department of Justice authorize the FBI's computer experts to conduct a search, without German consent, on the German ISP from their terminals in Washington?
- Does the FBI agent need a U.S. court order to access private information overseas? What would be the reach of such an order?
- If the FBI agent plows forward and accesses information from computers in Germany, will the German government be sympathetic to the U.S. plight, will the violation of German sovereignty be condemned, or both?
- What are the diplomatic and foreign policy implications of the United States remotely (and without advance notice) conducting a search that may intrude into German sovereignty?

The legal and policy implications of possible "transborder searches," such as the one contemplated in this scenario, are quickly becoming a concern for law enforcement agencies around the globe as they grapple with new challenges posed by networked communica-

tions and new technologies.[7] Traditional investigative procedures—and particularly the often cumbersome procedures that govern investigations at the international level—may not be adequate to meet the need in computer crime cases for immediate law enforcement action reaching beyond national borders.[8] The globalization of criminal activity has created vexing problems that, in some cases, defy simple solutions.[9]

Before we explore some of the challenges that new high-tech and computer-related crimes pose, it is important to describe the three ways that criminals use computers.[10] First, a criminal may target or attack a computer or a system controlled by a computer (e.g., hackers disrupting local phone service). Second, a criminal may use a computer to commit a "traditional" crime such as fraud or theft (e.g., promoting bogus investments on a Web page). Third, a criminal may use a computer in a way that is incidental to the offense, but where the computer nonetheless contains evidence of a crime (e.g., drug dealers using personal computers to store records of drug sales and "clients").[11]

The first two kinds of criminal activity can be carried out remotely, and often from great distances. Likewise, evidence of a crime can be stored at a remote location, either for the purpose of concealing the crime from law enforcement and others, or simply because of the design of the network. "Hackers are not hampered by the existence of international boundaries, since information and property can be transmitted covertly via telephone and data networks. A hacker needs no passport and passes no checkpoints. He simply types a command to gain entry."[12] This element of remoteness takes the investigation and prosecution of these crimes out of the exclusive purview of any single nation, thereby creating challenges and obstacles to crime-solving.[13]

---

7. The topic of transborder search and seizure, under which these issues fall, is discussed *infra* Section III(D)(2).

8. *See* Charney & Alexander, *supra* note 2, at 948.

9. *See, e.g., infra* Section III(D) (discussing difficulties in locating and identifying criminals who commit crimes remotely, via networked communications).

10. *See* Charney & Alexander, *supra* note 2, at 934.

11. *See id.*

12. Reno, Chantilly Keynote Address, *supra* note 1. *See generally* Carolyn P. Meinel, *How Hackers Break in . . . And How They Are Caught*, SCI. AM., Oct. 1998, at 98-107 (offering a fictionalized composite of many actual intrusions, or "hacks," and the attendant countermeasures that took place in cyberspace, all from remote locations).

13. Examples of criminals hop-scotching the globe by merely using a home computer and a phone line abound. Between June and October 1994, a hacker sitting in St. Petersburg, Rus-

Not long ago, most crimes were local. The criminal or criminals, the actual crime, and the victim were all within the same state, if not the same city. Such television crime-stoppers as Tony Baretta, Sergeant Joe Friday, and Steve McGarrett of Five-O seldom had to go far to find their man (or woman).[14] Physical evidence of the crime could be found at or near the crime scene, and these cops rarely needed help from outside their precincts. It was the extraordinary set of facts—bank robbers fleeing across state lines, for example—that brought *The F.B.I.*'s Inspector Lewis Erskine (played by Efrem Zimbalist, Jr.) into the case. From 1965 to 1974, Inspector Erskine, roaming the United States, investigated counterfeiters, extortionists, organized crime figures, and bombings by political radicals. But, with the exception of the occasional Communist spy, the entirety of each case rested within the borders of the United States.[15]

Today, however, characters who seem to come more from Tom Clancy's world are taking advantage of powerful personal computers linked to the Internet and World Wide Web, the explosion of electronic commerce and e-mail, and wireless and satellite communications to bring a global dimension to an increasing amount of criminal activity.[16] Targeting computers with malicious programming codes[17] from thousands of miles away is no longer the fanciful idea of science

---

sia, pilfered $5 million from Citibank accounts worldwide and placed the money into his accomplice's accounts in the United States, Israel, Finland, Germany, the Netherlands, and Switzerland. *See* Saul Hansell, *Citibank Fraud Case Raises Computer Security Questions*, N.Y. TIMES, Aug. 19, 1995, at 31; THE WHITE HOUSE INTERNATIONAL CRIME CONTROL STRATEGY (May 1998). The culprit, Vladimir Levin, was extradited to the United States in 1997, pled guilty to conspiracy to commit bank fraud, and was sentenced to thirty-six months' imprisonment. Approximately $4.5 million of the stolen money was recovered. *Id*.

14. Baretta, Friday, and McGarrett are fictional characters, respectively, from the television police dramas *Baretta* (1975-78), *Dragnet* (1952-70), and *Hawaii Five-O* (1968-80). *See* TIM BROOKS & EARLE MARSH, THE COMPLETE DIRECTORY TO PRIME TIME NETWORK AND CABLE TV SHOWS 77, 289, 442-43 (1995).

15. Inspector Erskine was the lead character in the police drama *The F.B.I.* (1965-74). *See id.* at 326. The program won the commendation of real-life FBI Director J. Edgar Hoover, who gave the show full government cooperation and even allowed filming of some background scenes at FBI Headquarters in Washington, D.C. *See id*.

16. If it is true that art imitates life, then the action-thrillers written by Tom Clancy bear out these trends. Tom Clancy, the author of such Cold War bestsellers as THE HUNT FOR RED OCTOBER (1984), RED STORM RISING (1986), and THE CARDINAL IN THE KREMLIN (1988) is now churning out such titles as RUTHLESS.COM (1998) (co-authored with Martin Greenberg), and NET FORCE (1999) (co-authored with Steve Pieczenik).

17. "Malicious programming code" is code that is designed to cause unauthorized damage to computer systems.

fiction writers.[18] Today, such crimes are becoming the daily workload for some investigators and prosecutors.[19] A computer server running a Web page designed to defraud senior citizens might be located in the Seychelle Islands, and victims of the scam could be scattered throughout twenty-five different countries. Or an extortionist may commit blackmail by sending e-mails that run through the communications networks of five countries before reaching the intended recipient.

As we approach the 21st Century, the irrelevance of borders is making some old crime-solving paradigms and practices obsolete. The power of networks and Pentium-driven PCs makes every computer a potential tool for criminals and gives them the ability to reach across borders with great stealth—and then hang up the phone to disappear without a trace.[20] The globalization of criminal activity and the anonymity with which criminals can cross electronic "borders" is a real problem, with a potential to affect every country, every law enforcement officer, every citizen. So what are we to do?

III. WHAT NEEDS TO BE DONE

On December 9-10, 1997, U.S. Attorney General Janet Reno held the first-ever meeting of her counterparts from the G-8 countries (Canada, France, Germany, Italy, Japan, Russia, and the United Kingdom), with the focus on high-tech and computer-related crime.[21] That the first meeting ever held among the senior law-enforcement officials of the eight countries was centered on computer crime un-

18. *See, e.g.*, WILLIAM GIBSON, NEUROMANCER (1984) (describing futuristic hackers who remotely penetrate corporate security systems using intelligent viruses). Four years after *Neuromancer* was published, in 1988, a Cornell University student named Robert Morris developed a program known as a "worm," which he designed to attack computers through the Internet. A worm is a self-contained computer program (unlike a "virus," which must attach itself to other programs) that duplicates itself and then attempts to penetrate computer systems and cause damage. After Morris's worm penetrated the target computer, it would consume the computer's available memory, resulting in the shutdown of the computer. Before his worm could be neutralized, it had crippled approximately 6,200 computers and caused over $98 million in damage. *See* United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

19. For example, the Computer Crime and Intellectual Property Section at the U.S. Department of Justice in Washington has a staff that includes eighteen attorneys. Likewise, the FBI has Infrastructure Protection/Computer Intrusion Squads in seven U.S. cities, with five more funded and scheduled to be operational by January 1, 2000.

20. *See* Marc D. Goodman, *Why the Police Don't Care About Computer Crime,* 10 HARV. J.L. & TECH. 465, 467 (1997).

21. *See* Janet Reno, On the Meeting of Justice and Interior Ministers of The Eight (Dec. 10, 1997) (visited Apr. 19, 1999) <http://www.usdoj.gov/criminal/cyber crime/commp8pr.htm>. The G-8 and its work on high-tech crime is discussed *infra* at Section IV(C).

derscores the growing concerns that world leaders share about security in cyberspace.[22] In a statement to her colleagues, Attorney General Reno highlighted four areas where progress by the international community is critical if law enforcement is to keep pace with both technology and the criminals who exploit it:

- First, enactment of sufficient laws to appropriately criminalize computer and telecommunications abuses;
- Second, commitment of personnel and resources to combating high-tech and computer-related crime;
- Third, improvement in global abilities to locate and identify those who abuse information technologies; and
- Fourth, development of an improved regime for collecting and sharing evidence of these crimes, so that those responsible can be brought to justice.[23]

The joint Communiqué issued at the conclusion of the meeting by all eight countries[24] as well as the ten Principles and ten-point Action Plan agreed to by the Ministers and Attorney General[25] reflected concern for these issues. Each of these four areas is critical to pro-

---

22. *See* Clifford Krauss, *8 Countries Join in an Effort To Catch Computer Criminals*, N.Y. TIMES, Dec. 11, 1997, at A12 (quoting Jack Straw, the British Home Secretary, as saying, "We're using 19th-Century tools to face a 21st-century problem. One person can stay in the same place and commit crimes in several countries without leaving his armchair.").

23. Telephone Interview with Scott Charney, Chief, Computer Crime and Intellectual Property Section, U.S. Department of Justice and Chair, G-8 Subgroup on High-tech Crime (Dec. 1, 1998).

24. *See* Meeting of the Justice and Interior Ministers of The Eight, Communique´ (Dec. 10, 1997) (visited Apr. 19, 1999) <http://www.usdoj.gov/criminal/cybercrime/communique.htm>.

> National laws apply to the Internet and other global networks. But while the enactment and enforcement of criminal laws have been, and remain, a national responsibility, the nature of modern communications networks makes it impossible for any country acting alone to address this emerging high-tech crime problem. A common approach addressing the unique, borderless nature of global networks is needed and must have several distinct components.
>
> Each country must have in place domestic laws that ensure that the improper use of computer networks is appropriately criminalized and that evidence of high-tech crimes can be preserved and collected in a timely fashion. Countries must also ensure that a sufficient number of technically-literate, appropriately-equipped personnel are available to address high-tech crimes.
>
> Such domestic efforts must be complemented by a new level of international cooperation, especially since global networks facilitate the commission of transborder offenses. Therefore, consistent with principles of sovereignty and the protection of human rights, democratic freedoms and privacy, nations must be able to collect and exchange information internationally, especially within the short time frame so often required when investigating international high-tech crimes.

Id.

25. *See id*. The full text of the Principles and Action Plan are provided *infra* note 135.

tecting public safety and ensuring that users of new technologies are not victimized in new ways. Each area also poses unique challenges to ingenuity, national leadership, and international cooperation. I will take up each of them separately in the following subsections.

A. Needed: Sufficient Laws to Punish Computer Crimes

When Country *A* criminalizes certain conduct and Country *B* does not, a bridge for cooperation in solving a crime committed in Country *A* may not be possible. The United States has entered into bilateral treaties of extradition with over 100 countries.[26] These treaties are either "list treaties," containing a list of offenses for which extradition is available, or they require dual criminality (i.e., require that the conduct under investigation is a crime in both the requesting and requested countries and is punishable by at least one year in prison).[27] With regard to treaties for international legal assistance such as those involving the issuance of subpoenas, interviewing of witnesses, or production of documents, some treaties permit assistance as long as the conduct under investigation is a crime in the requesting state. The United States strongly favors this approach.[28] Other treaties permit assistance only if dual criminality exits and if the offense is extraditable.[29] Therefore, if one country does not criminalize computer misuse (or provide for sufficient punishment), extradition and the collection of certain evidence may be prohibited. Consider the following two examples.

---

26. *See* 18 U.S.C. § 3181 (1998) (listing treaties of extradition).

27. Telephone Interview with Drew C. Arena, Counselor for Criminal Justice Matters, U.S. Mission to the European Union (Mar. 9, 1999). (From 1987 to 1992, Mr. Arena was the Director of the Office of International Affairs at the U.S. Department of Justice in Washington, D.C.).

28. *See id.* However, in the more sensitive area of search and seizure, some U.S. treaties either require dual criminality (e.g., Treaty on Mutual Legal Assistance, June 12, 1981, Neth-U.S., T.I.A.S. No. 10734 art. 6, para. 1) or allow a party to refuse a request "if it relates to conduct in respect of which powers of search and seizure would not be exercisable in the territory of the Requested Party in similar circumstances." Treaty Between the United States of America and the United Kingdom of Great Britain and Northern Ireland on Mutual Assistance in Criminal Matters, Dec. 2, 1996, U.S.-Great Britain, S. TREATY DOC. NO. 104-2 (1996) [hereinafter US/UK MLAT], art. 14, para. 2.

29. *See* Council of Europe Convention on Mutual Assistance in Criminal Matters of 1959, Article 5(1)(a) and (b) (allowing parties to those conventions to limit "coercive measures," e.g., search warrants, to situations of either dual criminality or extractability of the underlying offense); Telephone Interview with Drew C. Arena, Counselor for Criminal Justice Matters, U.S. Mission to the European Union (Mar. 18, 1999).

In 1992, hackers from Switzerland attacked the San Diego Supercomputer Center.[30] The United States sought help from the Swiss, but the investigation was stymied due to lack of dual criminality, (i.e., the two nations did not have similar laws banning the conduct), which became an impediment to official cooperation. Eventually, local police in Zurich did render informal assistance, and they prepared a list of questions for U.S. authorities to answer, transmitted through official channels, so the case could be properly pursued. After the United States answered those questions, but before follow-up questions could be answered through official channels, the hacking stopped, the trail went cold, and the case had to be closed.[31]

Several years later a similar problem arose, when the United States found itself unable to reach a criminal in order to bring him to justice. From August 1995 until February 1996, the Naval Criminal Investigative Service and the FBI investigated a hacker who was stealing password files and altering log files in military, university, and other private computer systems.[32] Many of these systems contained sensitive research on satellites, radiation, and energy-related engineering.[33] U.S. authorities tracked the hacker to Argentina and notified a local Argentine telecommunications carrier.[34] The carrier contacted local law enforcement, which began its own investigation. Subsequently, an Argentine judge authorized the search of the hacker's apartment and the seizure of his computer equipment based on potential violations of Argentine law.[35] Unfortunately, the treaty between Argentina and the United States did not authorize the extradition of individuals for "computer crimes" (although it does for more traditional crimes). The U.S. Attorney's Office in Boston charged the perpetrator with several criminal violations, but it was unclear whether or not the case would ever be resolved due to the

30. Telephone Interview with Scott Charney, Chief, Computer Crime and Intellectual Property Section, U.S. Department of Justice and Chair, G-8 Subgroup on High-tech Crime (Mar. 2, 1999).

31. *See id.*

32. *See* Pierre Thomas & Elizabeth Corcoran, *Argentine, 22, Charged With Hacking Computer Networks*, WASH. POST, Mar. 30, 1996, at A4; Telephone Interview with Stephen P. Heymann, Deputy Chief, Criminal Division, U.S. Attorney's Office (D. Mass.) (Apr. 12, 1999) (Mr. Heymann is the Computer and Telecommunications Coordinator (CTC) for the District of Massachussets and was the lead prosecutor for this case).

33. *See First Internet Wiretap Leads to a Suspect*, N.Y. TIMES, Mar. 31, 1996, at A20.

34. *See* Thomas & Corcoran, *supra* note 32.

35. *See id.*

absence of uniformity between U.S. and Argentine laws.[36] Fortunately, the hacker agreed to a plea bargain wherein he waived extradition and agreed to plead guilty in the United States.[37]

These cases demonstrate how inadequate laws can allow criminals to go unpunished in one country, while they thwart the efforts of other countries to vindicate the rights of the state and protect its citizens. While the United States has amended its criminal code to specifically penalize a wide variety of computer crimes,[38] other countries have been slower to do so.[39] At a meeting of senior law enforcement officials from the G-8 countries in January 1997, Attorney General Reno stated:

---

36. *See id.*; *First Internet Wiretap Leads to a Suspect*, *supra* note 33; Telephone Interview with Stephen P. Heymann, *supra* note 32.

37. *See First Internet Wiretap Leads to a Suspect*, *supra* note 33; Telephone Interview with Stephen P. Heymann, *supra* note 32.

38. *See* The Computer Fraud and Abuse Act of 1984, Pub. L. 101-73, *codified as* U.S.C. § 1030 (1984), *amended by* the National Information Infrastructure Protection Act of 1996, Pub. L. No. 104-294 (1996). The law contains eleven separate provisions designed to protect the confidentiality, integrity, and availability of data and systems. For example, section 1030(a)(2) makes it a crime to access a computer without or in excess of authority and obtain (1) financial information from a financial institution or credit reporting company; (2) any information in the possession of the government; or (3) any private information where the defendant's conduct involves interstate or foreign commerce. Section 1030(a)(5) makes it a crime for anyone to knowingly cause the transmission of a computer program, information, code, or command, that results in unauthorized damage to a protected computer. (A "protected computer" is one used exclusively by the United States or a financial institution; one used partly by the United States or a financial institution, in which the defendant's conduct affects the government's or financial institution's operation of the computer; or any computer that is used in interstate or foreign commerce or communications. 18 U.S.C. § 1030(e)(2)). *See also* The National Information Infrastructure Protection Act of 1996, A Legislative Analysis, by the Computer Crime and Intellectual Property Section of the U.S. Dept. of Justice (visited Apr. 1, 1999) <http:www.usdoj.gov/criminal/cybercrime/1030_anal.html>; Charney & Alexander, *supra* note 2, at 949-54 (providing a summary and explanation of the individual provisions of the Computer Fraud and Abuse Act). The United States also is moving to update statutes concerning "traditional" crimes, where new technologies present new opportunities for criminals. *See, e.g.*, Child Pornography Prevention Act (CPPA), Pub. L. 104-208, 110 Stat. 3009-28. 18 U.S.C. § 2252A (1996) (criminalizing, among other things, the use of computers to create and/or transmit child pornography); United States v. Hilton, 167 F.3d 61 (1st Cir. 1999). "Congress enacted the CPPA to modernize federal law by enhancing its ability to combat child pornography in the cyberspace era . . . . Lawmakers wished to improve law enforcement tools to keep pace with technological improvements that have made it possible for child pornographers to use computers to 'morph' or alter innocent images of actual children to create a composite image showing them in sexually explicit poses." Hilton, 167 F.3d at 65.

39. For example, while unauthorized access to a computer, without further action, is a criminal offense in such countries as France, Canada and the United States, it currently is not a criminal offense in Russia or Japan. *See* Charney, *supra* note 23 (as chair of the G-8 Subgroup on High-tech Crime, Mr. Charney is compiling the results of a survey completed by G-8 law enforcement officials on those countries' legal systems with respect to computer crime).

> [U]ntil recently, computer crime has not received the emphasis that other international crimes have engendered. Even now, not all affected nations recognize the threat it poses to public safety or the need for international cooperation to effectively respond to the problem. Consequently, many countries have weak laws, or no laws, against computer hacking—a major obstacle to solving and to prosecuting computer crimes.[40]

The solution to this problem is simple to state: "[countries] need to reach a consensus as to which computer and technology-related activities should be criminalized, and then commit to taking appropriate domestic actions."[41] But it is not as easy to implement. An international "consensus" concerning the activities that universally should be criminalized may take time to develop. Meanwhile, individual countries that lack this kind of legislation will each have to pass new laws, an often cumbersome and time-consuming process. In the United States, for example, action by both the Congress and the President is required for new legislation.

B. Needed: Personnel and Resources to Combat High-tech Crime

In 1986, an astronomer-turned-systems-manager at the University of California at Berkeley found a seventy-five cent accounting error in the computer's billing program, which led to the discovery that an unauthorized user had penetrated Berkeley's computer system.[42] When the astronomer, Clifford Stoll, began to investigate further, he discovered a hacker identified as "Hunter" was using Berkeley's computer system as a conduit to break into U.S. government systems and steal sensitive military information.[43] The hacker's objective seemed to be to spy on the United States' "Star Wars" missile defense program.

Stoll encountered serious problems as he began to pursue the hacker. To begin with, Stoll was unable to find computer literate law enforcement personnel with an appreciation of the technical nature of the criminal activity. He also found that the legal processes required to locate and identify the hacker while he or she was online and thereby traceable were inadequate.[44] Various local and federal

---

40. Reno, Chantilly Keynote Address, *supra* note 1.

41. *Id*.

42. *See generally* CLIFFORD STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989) (describing the author's ten-month odyssey in search of the hacker).

43. *See id.*

44. *See id*. at 43.

agencies that Stoll contacted, including the FBI and Central Intelligence Agency (CIA), initially expressed little interest in pursuing what at first looked like a computer prank.[45] When local police finally issued a California order to trace a phone call, the trail led to Virginia where the order had no force. When the call was finally traced to Germany, the German telecommunications carrier could not quickly ascertain the source of the attacks because the trace had to be accomplished through mechanical switches. As Stoll and those assisting him moved backwards through the labyrinth of telecommunications to its source, they found a dearth of law enforcement personnel with technical expertise who could help.[46]

Stoll's "investigation" brought to light a number of interdependent "personnel" and "resource" requirements that, unless fulfilled, will impede the success of law enforcement in this burgeoning area. It is critical that the requirements summarized below are met at the international level to eliminate weak links in the chain of an investigation.

1. Experts Dedicated to High-tech Crime. The complex technical and legal issues raised by computer-related crime require that each country have individuals who are dedicated to high-tech crime. These individuals are needed to support domestic law enforcement authorities faced with high-tech issues, and they will be the first point of contact for their international counterparts.[47]

---

45. Until government investigators learned of the potential threat to national security, they had no interest in pursuing a case which appeared to have damages valued at less than $1.00. *See id*. (describing how the FBI in Montgomery, Alabama would investigate a computer crime only after a million dollars was at stake); *see also* Goodman, *supra* note 20 (discussing law enforcement disinterest in pursuing computer crimes).

46. *See generally* STOLL, *supra* note 42. Since Hunter's trail evaporated each time he ended a communication, Stoll had to resort to generating phony official-looking data to keep the hacker interested and online long enough for the trace to be completed. Eventually, the source of the attacks was identified, and the hacker was prosecuted in Germany. Ironically, one of the reasons the investigation was successful is because Stoll worked directly with telephone company personnel, who in turn worked with other telecommunications providers, instead of working with the government. *See id*. at 53, 225.

47. *See* Reno, Chantilly Keynote Address, *supra* note 1 ("[We must ensure] that law enforcement personnel are capable of addressing high-tech crime by understanding two emerging and converging technologies simultaneously: computers and telecommunications. The complexity of these technologies, and their constant and rapid change, suggest that countries need to designate investigators and prosecutors to . . . work these cases on a full-time basis, immersing themselves in computer-related investigations and prosecutions."); Reno, *supra* note 21 ("Countries must also ensure that a sufficient number of technically-literate, appropriately-equipped personnel are available to address high-tech crimes.").

2. *Experts Available on a Twenty-Four Hour Basis.* A unique feature of high-tech and computer-related crime is that it requires immediate action to locate and identify perpetrators. Due to a general lack of historical communications data, the trail of a criminal may be impossible to trace once a communication link is terminated. This lack of data is due, in part, to the fact that businesses no longer bill their customers by individual telephone call or Internet connection but, instead, by bulk billing (e.g., a single rate for one month of usage).[48] When bulk billing is employed, there is no longer a business need to record the transmission information (i.e., connection times or source and destination) for individual connections; therefore, traffic data may not be available at a later date. Thus, investigators and prosecutors with expertise in this field must be available twenty-four hours a day, at home and by pager, so that appropriate steps can be taken in a fast-breaking high-tech case.

3. *Continuous Training.* Because of the phenomenal rate at which computer technologies evolve, and because high-tech criminal techniques and capabilities change more rapidly than those in more traditional areas of criminal activity, experts must receive continuous training in the investigation and prosecution of high-tech cases. In addition to domestic training, countries should participate in coordinated training with other countries, so transnational cases can be pursued quickly and seamlessly.[49]

4. *Up-to-date Equipment.* To keep pace with computer criminals, law enforcement experts in this field must be properly equipped with the latest hardware and software. There was a time when police needed little more than a gun, handcuffs, flashlight, and a notepad. Today, providing them with proper equipment may prove to be one of the more difficult challenges, because the cost of purchasing sophisticated equipment and software to keep pace with

48. *See, e.g.*, James Peltz & Michael Hiltzik, *Takeover Possible at Earthlink*, L.A. TIMES, Jan. 26, 1999, at C7.

49. In the United States, high-tech prosecutors at the federal level attend a one-week training course every year, with training provided by both government and private sector personnel. Likewise, all federal investigative agencies provide high-tech training to their agents. The government's National Cybercrime Training Partnership is developing high-tech training for federal, state, and local law enforcement personnel. *See generally* Martin Kettle & Owen Bowcott, *Computer Crime: The Age of the Digital Sleuth*, THE GUARDIAN, Dec. 12, 1997, at 19.

rapid advances in technology places considerable burdens on the budget process.[50]

To get approval to hire and/or allocate dedicated personnel, to commit time and money to training, and to find millions of dollars for frequent purchases and upgrades of equipment and software, senior policy-makers—often acting under tight budget constraints—must become directly involved and provide strong leadership. In fact, to ensure that high-tech issues receive appropriate attention, the support of officials at the level of Attorney General, or Justice or Interior Minister may be required.[51]

C. Needed: Improved Abilities to Locate and Identify Criminals

When a hacker disrupts the telephone network of a Baby Bell, when the White House receives an e-mail threatening the President, or when the files of a Fortune 500 company are stolen via the Internet, a primary investigative requirement is to locate the source of the attack. To do so requires tracing the "electronic trail" from the victim back to the attacker. As we enter the new millennium, law enforcement personnel chasing a hacker's trail face a landscape dramatically different from the recent pre-Internet era.

In today's communications environment, as a result of corporate divestiture, a single carrier usually does not carry a communication from end-to-end. The days when the police worked alone with "Ma Bell" to solve a crime are over. A hacker's transmission may pass from his or her computer to a local phone company, to an ISP, to a long-distance telephone carrier, to a university computer, across an ocean via satellite, on its way to a foreign corporate victim.[52] Consider that:

---

50. *Cf.* Goodman, *supra* note 20; Jon Bigness, *Dick Tracy Comes to Life*, CHI. TRIB., Dec. 15, 1997, at 1C.

51. Unfortunately, many of the senior policy-makers and budget gurus in government are unfamiliar with new computer and telecommunications technologies, and with the threats posed by computer criminals. If these individuals are not familiar with the technologies at issue and the new threats they pose, they may be hesitant to support law enforcement by seeking appropriate legislative and budgetary changes. *See, e.g.*, Weiner, *supra* note 4 ("In his office, . . . [White House terrorism czar Richard Clarke] spoke passionately about the threat of cyberwar, invisible attacks on the nation's computers, a terror so insidious, so arcane he has trouble convincing corporate chieftains and political commissars that it is real.").

52. *See, e.g.*, *Computer Hacker Sought; European Man Cracked Thousands of Passwords Worldwide*, DALLAS MORNING NEWS, July 29, 1998, at 5A (reporting a hacker detected in the network of the University of California at Berkeley math department after gaining Internet access by way of modem through a Swedish Internet Service Provider and passing his communications through such countries as the United Kingdom, Denmark and South Korea).

- a nefarious communication may pass through a large *number of carriers* (e.g., Sprint PCS to Bell Atlantic to CompuServe to AT&T to MCI to the Microsoft Network to Deutsche Telekom);
- the communication may pass through many different *types of carriers*, each with different technologies (e.g., local telephone companies, long-distance carriers, ISPs, wireless and satellite networks);[53] and
- the communication may pass through carriers in a number of *different countries*, each in different time zones and subject to different legal systems.

And, unfortunately, each of these differentiations may occur within one individual hacker attack.

Because tracing the trail from victim back to attacker may be possible only when the hacker is actually on line (since transmission information is often not recorded and retained), law enforcement officials must work at lightning-fast speed. However, the traditional international legal assistance regime often cannot accommodate requests for assistance that occur during a cyber-attack because responses cannot be handled in real-time.[54] Inefficient and overly bureaucratic instruments for mutual legal assistance need to give way to more practical approaches.

A further set of complications arises with each individual carrier approached by law enforcement. First, in order to be able to assist law enforcement officials, the technical infrastructure (i.e., the communications network and the computers and software that run it) needs to have been designed and configured to generate and preserve

---

53. Locating and identifying a criminal who is using an array of carriers becomes much more challenging when wireless communications are used. Previously, when a telephone was used in a crime, a telephone line physically connected the perpetrator to a specific location. If the call could be traced, police knew exactly where the call originated. At the same time, law enforcement could find out the name of the person who was being billed for the phone line, although that person may not, of course, have been actually using the phone at the time of the offense.

But today, mobile phones allow an individual to commit crimes while roaming around the globe. In certain cases, sophisticated technologies can permit law enforcement to identify the general area where a wireless call is coming from, but such information may not be specific enough to allow an arrest to be made. Even then, however, identifying the owner of a particular mobile phone can be difficult, because mobile phones can be altered to transmit phony identifying information. Moreover, as mobile phones become less expensive, criminals can use them as "disposable phones," so that evidence linking the perpetrator to the communication is destroyed immediately after the commission of the crime.

54. *See generally* STOLL, *supra* note 42.

critical traffic data, such as the information relating to the source and destination of a cyber-attack.[55] In certain instances, technologies to generate and preserve this data simply do not exist. Second, assuming the particular piece of the technical infrastructure is capable of generating and preserving needed data, carriers must in fact actually collect and retain such records.[56] Examples of current industry practices that leave carriers without critical data include offering free anonymous e-mail accounts where subscriber information is not requested or verified; implementing dynamic addressing systems at ISPs (i.e., Internet addresses for computers are re-assigned with each new connection); and deciding against generating or maintaining records for local telephone calls. Third, law enforcement must be allowed timely access to this information by the carrier. Accordingly, listed below are the steps that need to be taken so that law enforcement can navigate through the contours of this dynamic environment to find computer criminals.

1. Technical Standards Must Promote Public Safety. Countries need to reach a consensus as to the technical requirements and industry standards in hardware, software, Internet protocols, and related technologies that are most critical to law enforcement needs. Thereafter, countries must develop a process for encouraging technical specifications that promote public safety.

2. Critical Traffic Data Must be Preserved. Countries should ensure that telecommunications carriers and ISPs routinely store

---

55. The use by many ISPs of "modem banks" or "hunt groups," to address increasing demand for Internet access is an example of a network design that can obfuscate critical traffic data. Where a modem bank is used, an ISP may have hundreds (or thousands) of phone lines, but the ISP gives its customers just one access number (e.g., 555-1234). The ISP's network is configured to automatically route each incoming call to the "next" available line, but without linking a customer with a specific incoming line, it may be impossible to tell through which phone line a cyber-attack is transmitted.

56. In some countries, telecommunications carriers and ISPs are required by law to routinely retain data that later may be critical to a criminal investigation; in other countries, such retention is prohibited. And in the third case, a country's laws may be silent on this topic, leaving companies to weigh public safety concerns, privacy interests, and market forces in developing their practices. Of particular concern to U.S. law enforcement are the EU's 1995 and 1997 directives concerning the processing of personal data, which will require deletion of traffic data. *See* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. 31 (L 281); Directive 97/66/EC of the European Parliament and of the Council of December 15, 1997 Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1997 O.J. 1 (L 24) (Jan. 30, 1998). *See* discussion *infra* Part IV.B. and accompanying footnotes.

access logs and other key traffic data for certain minimum periods of time (e.g., ninety days). Countries also need to adopt legal processes that allow law enforcement to request that a carrier or ISP retain specific traffic data for longer periods of time, should that data be needed for a criminal investigation.[57]

3. Information Must Be Shared Quickly. When a communication travels through several carriers, law enforcement must obtain court orders in each successive jurisdiction through which a signal passes in order to trace the communication to its source.[58] If there are points of origin in different jurisdictions, investigators must go to separate courthouses to obtain necessary court orders. "This consumes valuable time and scarce resources and impedes identification of the perpetrator."[59] Legal processes must be improved to account for new technologies and find ways to remove unwieldy, piecemeal mechanics from domestic and international investigations.[60]

When information is sought from carriers in different countries, applications to obtain critical information currently need to be made separately in each country; the resulting delay can debilitate investigators in hot pursuit. Unfortunately, innovative solutions for expediting international cooperation have not yet been developed. We should consider whether traditional means of legal assistance (i.e., requests under mutual legal assistance treaties and use of letters rogatory) need to be supplemented with procedures that will facilitate the immediate sharing of traffic data, or whether other avenues should be explored.[61]

---

57. *See infra* note 67. *See, e.g.*, 18 U.S.C. 2703(f) (requiring a telecommunications carrier or ISP to retain data for up to 180 days at the request of law enforcement). As law-making bodies take up the issue of data protection and other restrictions on the collection and storage of communications data, law enforcement agencies must work to ensure that new data protection policies do not create safe havens for computer criminals, but instead balance privacy concerns with public safety needs.

58. *See generally* STOLL, *supra* note 42; 18 U.S.C.S. § 3121 (Supp. 1989) ("trap and trace" statute).

59. Statement of Attorney General Janet Reno before the United States Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State, and the Judiciary, *available in* 1999 WL 8084451 (Feb. 4, 1999).

60. In Senate testimony, Attorney General Reno discussed a High-Technology Crime Bill being considered by the Department of Justice that would address "several technical and procedural infirmities that inhibit effective investigation and prosecution of cybercrime." One amendment to existing statutes would "allow federal judges to direct cooperation among successive communications providers that carry a particular communication." *Id.*

61. *See* Reno, Chantilly Keynote Address, *supra* note 1.

4. Government/Industry Cooperation is Imperative. There is broad international consensus that cooperation with industry is integral, and indeed critical, to investigating high-tech crime and thereby protecting public safety.[62] Governments should recognize that the needs of law enforcement may place burdens on industry and thus take reasonable steps to minimize such burdens.[63] At the same time, industry ought to consider the safety of the public when responding to the needs of the market. Cooperation can be enhanced in two ways. First, by establishing investigative points-of-contact with critical communications carriers. Second, by standardizing procedures by which investigators seek assistance from industry. Above all, governments must foster an operational relationship with industry based on trust.[64]

D. Needed: Effective Means for Obtaining Evidence Internationally

Even if all countries have adequate computer crime laws, possess dedicated, well-trained and well-equipped experts who are available twenty-four hours a day, and have the ability to locate and identify criminals who use networked communications, there remains a significant hurdle to overcome. How does law enforcement collect electronic evidence that may be scattered across several different countries, can be deleted or altered with one click of a mouse, may be encrypted, and will ultimately need to be authenticated in another country's court? Again, these are areas where the challenges have been recognized but solutions either may not be apparent or may be difficult to implement.

1. *Protected Seizures or "Quick Freeze/Quick Thaw."* One characteristic of electronic evidence is that it can be altered, transferred or destroyed almost instantaneously, and from remote

62. *See* Reno, *supra* note 21. At their meeting in December 1997, Attorney General Reno and the G-8 Justice and Interior Ministers affirmed their commitment to broad cooperation with industry:

> The development of effective solutions will also require unprecedented cooperation between government and industry. It is the industrial sector that is designing, deploying and maintaining these global networks and is primarily responsible for the development of technical standards. Thus, it is incumbent on the industrial sector to play its part in developing and distributing secure systems that, when accompanied by adherence to good computer and personnel security practices, serve to prevent computer abuse. Such systems should also be designed to help detect computer abuse, preserve electronic evidence, and assist in ascertaining the location and identity of criminals. *Id*.

63. *See id.*

64. *See* Kettle & Bowcott, *supra* note 49.

locations, often with little more than a single keystroke.[65] These changes to evidence may result from a criminal trying to cover his tracks, or a system administrator routinely clearing old e-mails or other data from a company's servers. Whatever the case, critical evidence can be lost—long before an international request for assistance is ever transmitted. Traditional methods of obtaining evidence from foreign governments can include lengthy delays, as foreign legal processes, translations, and diplomacy slowly proceed.[66] Old modalities may not always be practical when considering new technologies.

Therefore, when electronic evidence is sought, there may be a need for mechanisms such as a "preservation of evidence request" or "protected seizure," which would work as follows. Where there is a particularized concern about the loss of electronic evidence, a country would make an informal international request that the data immediately be preserved. This could be accomplished in a number of ways, from having a telecommunications carrier or ISP copy and store a customer's data, to actually seizing a criminal's computer and securing, but not searching, it for a short period of time.[67] Once data is protected from loss, expedited processes would provide the foreign country with formal documentation to authorize the issuance of a domestic search warrant or similar process.[68]

2. *Transborder Search and Seizure*.[69] Since paper documents must be within close proximity to be of use, they are usually located

---

65. *See, e.g.*, STOLL, *supra* note 42; Kettle & Bowcott, *supra* note 49.

66. In addition, immediately after a system intrusion, law enforcement authorities may be certain that a crime has occurred and may have identified a potential source, but they may be days away from providing the particularized information usually required by a foreign government before assistance can be granted. It is in that window, between the detection of the crime and formal request, that there is a great risk of deletion, alteration or destruction of evidence. *See generally* STOLL, *supra* note 42.

67. The U.S. Code provides for a form of "preservation of evidence request." A telecommunications carrier or ISP is required, "at the request of a governmental entity, [to] take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process." 18 U.S.C. § 2703(f)(1) (1994). The government can have these records retained for up to 180 days. 18 U.S.C. § 2703(f)(2). This is an important example of how legal processes can be modernized to account for advances in communications and related technologies; implementation of this process on an international level would greatly enhance existing modalities of international legal assistance. *See infra* note 135, Principle V, Action Item 4-6, 8.

68. *See* Reno, Chantilly Keynote Address, *supra* note 1.

69. The following discussion on transborder search and seizure is based on the substantial work of Scott Charney, Chief, Computer Crime and Intellectual Property Section, U.S. Department of Justice. Telephone Interviews with Scott Charney, Chief, Computer Crime and

in the same country as the person being investigated. By contrast, electronic documents are often stored remotely on computers, sometimes thousands of miles away from their author. This may be done because of the structure of a particular business (where data is maintained at company headquarters) or the architecture of the network.[70] At other times, data may be purposely stored in another country to keep it beyond the reach of law enforcement.

A transborder search occurs when a law enforcement agent in his or her own country accesses a computer in another country to obtain electronic evidence, perhaps in furtherance of the execution of a domestic warrant. For example, in the hypothetical discussed in Section II (where a hacker had broken into FAA computers), U.S. investigators would likely have conducted a transborder search due to exigent circumstances (i.e., the possibility of imminent death or serious injury to air travelers). Also, a law enforcement agent can unknowingly conduct a transborder search, when he is not aware that his search has led him across a border. If an investigator searches the computer of a domestic corporation, it may be difficult to know where data accessed through that domestic terminal is actually stored. One site may have a link to another site, and the investigator may not know his communication was routed from a server in Dallas to one in Toronto. Because searches made under exigent circumstances (including those where it is believed evidence will be destroyed if not seized) and inadvertent searches across borders are likely to occur, it may be wise for countries to consider developing rules and/or guidelines to govern a transborder search (e.g., regarding notice to the searched country).

Governments have three potential solutions at this juncture. First, governments could decide to forego the development of principles, allowing each country to decide for itself whether transborder searches constitute an acceptable law enforcement practice.[71] Sec-

---

Intellectual Property Section, U.S. Department of Justice and Chair, G-8 Subgroup on High-tech Crime (Dec. 1998 to Feb. 1999).

70. For example, while America Online provides service in the United States, Europe and Asia, all of its data is stored on its computers in Reston, Virginia. When two people in Japan use AOL accounts to e-mail one another, all of their data is stored in the United States. Thus, if Japanese law enforcement tries to investigate a local crime involving two people who live within the same square mile in Tokyo, the Japanese must seek the assistance of U.S. law enforcement to get at any e-mail on AOL's server. Perhaps inappropriately, the documents are accessible to the account-holders in Japan, but beyond the reach of Japanese law enforcement.

71. If this approach is taken, the most difficult scenario may arise where the searching country takes the view that a transborder search is, under some theory, permissible, and the

ond, governments could limit transborder searches to cases where production of the data could otherwise be compelled through legal processes.[72] This approach expedites the gathering of certain critical evidence while allowing data outside the traditional reach of a country to remain so. The third solution involves creating principles permitting law enforcement agents to conduct transborder searches under clearly defined circumstances that are more broad than those above. Support for this approach may rest on a consensus that the need for effective law enforcement outweighs concerns over protecting data stored in a particular country.

Unfortunately, the area of transborder searches is one where agreement on a particular approach may represent only a tiny step toward resolving other seemingly intractable issues such as how jurisdiction over stored data should be perceived and defined. One senior British law enforcement official has offered the following:

> Jurisdiction over a database should not now depend only on where it happens to be physically stored. Where the owners of the system have set it up to be accessible from another jurisdiction, it should be regarded as present in that jurisdiction for law enforcement purposes.
>
> I recognise this raises difficult constitutional issues for all of us. I hope it will be clear that this [is] not international Governments acting together in an Orwellian idea of 'Big Brother.' Transborder search principles would need to be accompanied by agreed minimum standards and safeguards. But time is limited.[73]

Because the potential for transborder searches exists in almost every country, progress cannot be put off simply because of the difficult legal and policy issues that litter the path to a comprehensive solution. Although, as discussed in Section IV, debates on this topic

---

searched country responds that the execution of that search is not only prohibited in its country but constitutes unauthorized access to its computers and therefore is a criminal offense.

72. For example, when a foreign corporation is doing business in one of the fifty United States, it is subject to that state's (as well as U.S.) laws, and under certain circumstances the corporation can be compelled to produce documents stored in another country. *See* United States v. Bank of Nova Scotia, 691 F.2d 1384 (11th Cir. 1982) (enforcing grand jury subpoena duces tecum in tax and narcotics investigation of U.S. citizen, where subpoena called for production of records in branch office in the Bahamas and compliance would require bank to violate Bahamian bank secrecy rule).

73. Paul Boateng, *supra* note 5. This philosophy is not unlike that used by the court in United States v. Bank of Nova Scotia, 691 F.2d 1384. *See also* discussion *supra* note 72.

are currently taking place in multilateral fora, any outcome is far from certain.[74]

3. *Encryption*. Encryption is a method of scrambling data to protect its confidentiality. Mathematical algorithms are used in conjunction with "keys" (frequently, the key is a password) to hide content, and the intended recipient of an encrypted e-mail message or the user of an encrypted file can only read the message or file if he or she has access to the key. Encryption is important to protect the confidentiality of e-mail traffic, stored data, and commercial transactions.[75]

When encryption is used by criminals for communications or data storage, investigations can be severely hampered because encryption can prevent timely access to the content of seized or intercepted data. Debates concerning the regulation of encryption, as well as a possible management infrastructure for decryption keys, are underway within governments, between governments, and between governments and industry.[76] There has been a wealth of material already written on regulation, key management, and related topics,[77] and discussion on those points is beyond the scope of this article.

What is worth noting, however, is that whatever the overall regime and the legislative and regulatory framework, mutual legal assistance arrangements between countries must include some manner of decryption support services and governments must have the legal ability to provide such support.[78] Consider the case where French law

---

74. Unfortunately, a thorough discussion of transborder search and seizure issues is beyond the scope of this Article; many of these issues are still being framed and debated within and among governments.

75. *See generally* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C (2d ed. 1996).

76. For information concerning U.S. policy on encryption, see, for example, Department of Justice Frequently Asked Questions on Encryption Policy; Letter from Attorney General Reno and others to Members of Congress regarding law enforcement's concerns related to encryption; Senate Hearings on Privacy in a Digital Age: Encryption and Mandatory Access; and Testimony of Deputy Assistant Attorney General Robert S. Litt Before the Subcommittee on Telecommunications, Trade and Consumer Protection of the House Commerce Committee, Sept. 4, 1997 (visited Apr. 10, 1999) <http://www.usdoj.gov/criminal/cybercrime/crypto.html>.

77. *See, e.g.*, STEPHEN KENT, ET AL., SPECIAL PANEL OF THE ASSOCIATION FOR COMPUTING MACHINERY U.S. POLICY COMMITTEE, CODES, KEYS AND CONFLICTS: ISSUES IN U.S. CRYPTO POLICY (1994); KENNETH DAM & HERBERT LIN, CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION DAM, NATIONAL RESEARCH COUNCIL, COMMITTEE TO STUDY NATIONAL CRYPTOGRAPHY POLICY (1996).

78. The United States has dozens of bilateral mutual legal assistance treaties in effect. The more modern treaties have flexibility to accommodate "newer" forms of assistance, such as decryption support. As an example, the U.S./U.K. MLAT art. 1, para. 2(h) provides for

enforcement requests data from the United States that is needed for a criminal investigation. Assume this request is contemplated under French/U.S. legal assistance practices. If U.S. authorities retrieve the data and it is encrypted, and the decryption key is stored in the United States, the data will be of little use to the French if we supply it to them as is. Further, the United States will be in the best position to have the data decrypted, either by learning the password from the target of the investigation, or by otherwise obtaining the key.[79] While commitments to provide decryption support do not exist as such today, the need for them will become more dire as the use of powerful encryption becomes more widespread.

4. *Computer Forensics*. Imagine that you are handling a case involving two business partners, Sam and Harry. Assume a particular e-mail message is important to your proof. Your witness, Sam, testifies that Harry made false statements when applying for a bank loan. On cross-examination, Harry's lawyer tries to suggest that Sam's testimony is a recent fabrication.

To rebut the charge of recent fabrication, you introduce into evidence an e-mail that Sam sent to another colleague, Bob, at the time of Harry's false statements, that is consistent with Sam's testimony at trial.[80] Harry's lawyer calls Bob as a witness and introduces Bob's copy of the e-mail into evidence—but this one is missing the

"such other assistance as may be agreed between Central Authorities." However, other treaties lacking such provisions could be construed to prohibit assistance that is not explicitly stated in their texts. In those cases, an amending document may be required in order to make decryption support available. *See* U.S./U.K. MLAT, *supra* note 28.

79. For an interesting examination of the legal issues raised by law enforcement's attempts to gain access to plaintext (i.e., unencrypted or decrypted text) and keys, see Phillip Reitinger, *Compelled Production of Plaintext and Keys, The Law of Cyberspace,* U. CHI. LEGAL. F. 171 (1996). The author determines the principal legal obstacle to law enforcement access to be the Fifth Amendment privilege against self-incrimination, and he concludes that a grand jury subpoena can direct the production of the plaintext of encrypted documents, although a limited form of immunity may be required; and a grand jury subpoena may direct the production of documents that reveal keys. Whether law enforcement can compel production of keys that are only known, rather than recorded, is an open question. *See id*. at 173.

80. The document would fall outside the definition of hearsay and therefore be admissible after a sufficient foundation is laid. *See* FED. R. EVID. 801(d)(1)(B) ("A statement is not hearsay if . . . [t]he declarant testifies at the trial or hearing and is subject to cross-examination concerning the statement, and the statement is . . . consistent with the declarant's testimony and is offered to rebut an express or implied charge against the declarant of recent fabrication or improper influence or motive.").

paragraph which refers to Harry having lied.[81] So there are two copies of the "same" e-mail; one, however, contains text that is not contained in the other. What do you do?

Similar problems concerning authenticity of evidence can arise with digital images. By now we have all probably seen (but possibly not known we did) magazine covers with a celebrity's head seamlessly attached to a younger and more fit body.[82] Today, if a photo is being used as evidence, you have to ask: is it real, or was it created (or altered) by merely rearranging binary digits? Further, when information incidental to a document's content, such as the date it was created or last "saved," is important to your proof, how are you going to assure the judge (and jury) that this information was not inadvertently altered when your witness retrieved it from his computer? Put another way, how is the integrity of an electronic medium maintained when it is brought into the courtroom?

The emerging field which addresses these issues is known as "computer forensics."[83] It encompasses the development and use of scientific protocols and procedures for searching computers, analyzing data, and maintaining the authenticity of data that has been retrieved.[84] From a practical standpoint, there are two tasks that experts in this field perform, although the line between the two often can blur. First, they retrieve electronic evidence. Any lawyer can list and print the document files on a hard drive (e.g., the Word or WordPerfect documents on the "C" drive), but it may take an expert to gather evidence that has been deleted (sometimes with powerful programs or devices), hidden, encrypted, or protected with passwords, software time bombs, or other devices that could destroy the

---

81. This document, again, is not hearsay, because it is not being offered for the truth of the statement contained therein, but instead to show that Sam's copy of the e-mail has been doctored. *See* FED. R. EVID. 801(c).

82. *See, e.g.*, Mark Kennedy, *When Seeing Isn't Believing: Digital Altering of Celebrity Photos is Becoming the Norm*, THE STAR LEDGER, Sept. 1, 1997 (discussing such digital alterations as a TV Guide cover in 1989 featuring Oprah Winfrey's face superimposed on Ann Margaret's body; Time magazine having darkened O.J. Simpson's mug shot for its cover; and Premiere magazine having removed Harrison Ford's facial scar for its cover; and stating, "Now it's possible for anyone with a few hours on a mid-priced desktop computer . . . to alter the content of photos.")

83. *See generally* Joan E. Feldman & Roger I. Kohn, *The Essentials of Computer Discovery*, LW GLASS CLE 297 (1998); Gregory S. Johnson, *A Practitioner's Overview of Digital Discovery*, 1997-98 GONZ. L. REV. 347.

84. *See* FEDERAL BUREAU OF INVESTIGATION, U.S. DEPT. OF JUSTICE, FBI LABORATORY ANNUAL REPORT '98 6, 15 (1999); Michael G. Noblett, *Computer Analysis and Response Team (CART): The Microcomputer as Evidence*, 19 CRIME LABORATORY DIG. 10, 10 (Jan. 1992).

evidence. The other aspect of this field is maintaining the authenticity of electronic data such that it can be probative in grand jury or courtroom proceedings.

In the United States, generally accepted protocols and procedures have been established so that (1) investigators searching computers have great success retrieving stored data, and (2) proof of authenticity and associated challenges are in keeping with those associated with physical evidence.[85] Outside of the United States, some countries have the same (or possibly greater) capabilities, but a significant number of others find themselves lacking in such proficiency.[86] The remedy to this disparity in abilities lies in international training and sharing of information and forensic tools. Organized efforts are currently underway to effect these changes.[87] With regard to authenticity, internationally recognized standards in computer forensics need to be adopted and implemented so that evidence gathered in one country can be introduced in proceedings in another country as a matter of course.

IV. WHAT IS BEING DONE BY MULTI-LATERAL ORGANIZATIONS?

To date, three multilateral organizations (i.e., groups with multiple-nation membership) are doing the bulk of the international policy work on high-tech and computer-related crime: the Council of Europe (COE), the European Union (EU) and its related institutions, and the G-8. To a lesser degree, some work in this area has been done by the Organization for Economic Cooperation and Development (OECD), and the United Nations.[88]

Of the three main groups, the G-8 has been particularly effective in making progress on several fronts. While the EU and COE have large European memberships, the G-8 has broader representation, with members from Europe, Russia, North America, and Japan.[89]

---

85. *See id.*; PROCEEDINGS OF THE 12TH INTERPOL FORENSIC SCIENCE SYMPOSIUM 14-51 (Richard Frank & Harold Peel eds. 1998).

86. *See* PROCEEDINGS OF THE 12TH INTERPOL FORENSIC SCIENCE SYMPOSIUM, *supra* note 85, at 8-43 (containing survey responses concerning specific aspects of computer forensics for fifteen countries, such as Australia, China, and Spain).

87. *See* discussion, *infra* Section IV.

88. *See* discussion of these multilateral groups *infra* Section IV.A-E. Work is being done in some instances on a bilateral (two-country) basis. But the broad international policy in this area is being done in the multilateral fora, and an examination of bilateral efforts underway is beyond the scope of this article.

89. *See infra* Section IV.C.

Because networked communications traverse every continent, and because leading communications and computer technology is developed in areas besides Europe (such as Asia and North America), regional efforts to solve universal crime problems will inevitably be either slower or less effective than similar efforts by policy-making bodies with a broad geographic base.

The heads of state of the G-8 countries meet annually. At their 1998 Summit, they adopted a comprehensive plan to fight high-tech and computer-related crime.[90] While the COE started addressing computer crime at the technical level in 1988, its heads of state have only met twice since 1949 when the COE was created, and have never addressed computer crime.[91] While EU heads of state called for a study of the subject and development of relevant policies, the heads of state from its member countries have not settled on a specific plan of action to combat computer crime.[92] Finally, unlike the COE and EU, the G-8 is neither governed by international convention nor constrained by a convention-created bureaucracy. It can therefore move faster and address new and emerging areas as the will of its leaders dictates.

A. The Council of Europe

The Council of Europe (COE) is an international organization based in Strasbourg, France.[93] It was established by ten Western European countries in the wake of the Second World War, with the signing of its founding treaty, known as the Statute of the Council of Europe, in 1949.[94] Today, it has a pan-European membership of forty countries, which include the Baltic states, Russia and Turkey.[95] It defines its main role as strengthening democracy, human rights, and the rule of law throughout its member states.[96] In the area of criminal law, twenty conventions and over eighty recommendations have been adopted, as well as a number of reports on crime issues.[97]

---

90. *See infra* Section IV.C.2 & note 135.

91. *See* Arena, *supra* note 29.

92. *See infra* Section IV.B.

93. *See About the Council of Europe* (last modified Jan. 27, 1999) <http://www.coe.fr/eng/present/about.htm>.

94. *See A Brief History of the Council of Europe* (last modified Jan. 28, 1998) <http://www.coe.fr/eng/present/history.htm>.

95. *See About the Council of Europe*, supra note 93.

96. *See id.*

97. *See* Peter Csonka, *Council of Europe Activities Related to Information Technology, Data Protection and Computer Crime*, 5 INFO. & COMM. TECH. LAW 177, 178 (1996).

In 1989, the Committee of Ministers[98] adopted a recommendation and report on computer-related crime, Recommendation No. R. (89) 9.[99] The recommendation called on member states to consider computer crimes when either reviewing or proposing domestic legislation, and the report contained guidelines in this area for legislators.[100] In 1995, the Committee adopted Recommendation No. R. (95) 13, which provided procedures for implementing Recommendation (89) 9, and contained principles "concerning problems of criminal procedure law connected with information technology" on such topics as search and seizure, technical surveillance, electronic evidence, encryption, and international cooperation.[101]

In February 1997, a Committee of Experts on Crime in Cyberspace (PC-CY) was formed to examine computer crime and related problems in criminal procedure law.[102] Its work is aimed at drafting a binding legal instrument (i.e., a "Cybercrime Convention") which defines cybercrime offenses, and addresses such topics as jurisdiction, international cooperation, search and seizure, data protection, and liability of ISPs.[103] The PC-CY first met in April 1997, and has had several additional meetings.[104] The PC-CY expects to have a draft Convention completed by December 31, 2000, at which time the draft will be forwarded to the Steering Committee on European Crime Problems (CDPC) (a committee of senior career bureaucrats). If the CDPC approves the draft, it will be forwarded to the Committee of Ministers for their approval. After approval by the Committee of

98. The Committee of Ministers is the decision-making organ of the Council of Europe, which comprises the foreign ministers from the member countries. (A European Foreign Minister is equivalent in rank to the U.S. Secretary of State.) *See Introduction to the Committee of Ministers of the Council of Europe* (last modified Mar. 22, 1999) <http://www.coe.fr/cm/intro/intro.0.html>.

99. *See* Csonka, *supra* note 97, at 179-80.

100. *See id.*

101. *Id.* at 186; *Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology* (last modified Dec. 3, 1998) <http://www.usdoj.gov/criminal/cybercrime/crycoe.htm> (adopted Sept. 11, 1995).

102. While membership of the PC-CY is limited to experts from fourteen European countries, representatives from the Canada, Japan, and the United States may attend meetings, but may not vote on any matter. *See Council of Europe's Fight Against Corruption and Organised Crime* (last modified June 10, 1997) <http://www.coe.fr/corrupt/epccy.htm> (Specific Terms of Reference, Committee of Experts on Crime in Cyberspace, 583rd Meeting, Feb. 4, 1997).

103. *See id.*; Telephone Interview with Drew C. Arena, *supra* note 29.

104. *See* THE WHITE HOUSE, INTERNATIONAL CRIME CONTROL STRATEGY 69 (May 1998).

Ministers, the Convention will be open for signature by COE members and non-member states which participated in its drafting.[105]

B. The European Union

The European Union (EU) has its roots in three organizations formed in the 1950s by Belgium, West Germany, France, Italy, Luxembourg, and the Netherlands: the European Coal and Steel Community (ECSC); the European Atomic Energy Community (Euratom); and the European Economic Community (EEC).[106] These three communities are still at the heart of the EU, and the treaties which founded them have since been revised and extended.[107] The Treaty on European Union, generally called the Maastricht Treaty, gives a single legal framework to the three European Communities.[108]

The EU now has fifteen member states, and its own flag, anthem and currency (the Euro).[109] The EU's objective is to "promote economic and social progress which is balanced and sustainable, assert the European identity on the international scene, and introduce a European citizenship for the nationals of the Member States."[110]

In the area of high-tech crime, the EU has issued several texts. In 1995, it promulgated a directive which established certain rights and protections for citizens concerning electronically processed data.[111] For example, the directive establishes the right of a citizen to know what electronic data a corporation maintains on that person, and provides protection against personal data being transferred to a

105. *See Council of Europe's Fight Against Corruption and Organised Crime*, *supra* note 102. If the United States were to become a signatory to the Convention (which is impossible to predict at this point), the U.S. Senate would have to ratify the Convention, as with any international treaty.

106. *See* DIRECTORATE-GENERAL FOR INFORMATION, COMMUNICATION, CULTURE AND AUDIOVISUAL MEDIA, EUROPEAN COMMUNITIES, HOW DOES THE EUROPEAN UNION WORK? 6-7 (2d ed. 1998). The founding treaties have been revised three times: in 1987 (the Single Act); in 1992 (the Treaty on European Union); and in 1997 (the draft Treaty of Amsterdam). *See The abc of the European Union - citizenship* (last modified Feb. 23, 1999) <http://europa.eu.int/abc-en.htm>.

107. *See The abc of the European Union - citizenship*, *supra* note 106.

108. *See id.*

109. *See id.* The member states are: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom. *See What is the European Union? 15 Member States and Maps* (last modified Feb. 3, 1998) <http://europa.eu.int/en/eu/states.htm>.

110. *The abc of the European Union - citizenship*, *supra* note 106.

111. *See* Directive 95/46/EC *supra* note 56.

non-EU country if that country has inadequate privacy protections.[112] Member states are required to establish mechanisms to enforce these rights.[113] In 1997, the EU issued a directive designed to ensure privacy relating to telecommunications data.[114] That directive requires telecommunications carriers to delete traffic data at the end of each transmission (with exceptions for billing purposes and for law enforcement and national security needs).[115] In light of these Directives, it is imperative that government policy decisions concerning electronic commerce and privacy be made in concert with decisions concerning public safety.

In 1997, the European Council[116] endorsed an action plan to combat organized crime, and assembled a Multidisciplinary Group on Organized Crime (MDG) to implement the action plan.[117] Recommendation Five of the action plan calls for a study on high-tech crime, and development of a policy addressing public safety which provides law enforcement and judicial authorities with the means to prevent and combat the misuse of new technologies.[118] Since its inception, the MDG has adopted the study of Dr. Ulrich Sieber on legal aspects of computer related crime,[119] and it is exploring what role Europol might play in combating computer crime.[120]

---

112. *See id.*

113. *See id.*

114. *See id.*

115. *See id.* The EU has issued a number of other documents relating to crime in cyberspace. *See, e.g.,* Decision No. 276/1999/EC of the European Parliament and of the Council of January 25, 1999, Official Journal of the European Communities, L33/1 (Feb. 6, 1999) (adopting an action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks).

116. The European Council is comprised of the heads of state of the fifteen member countries of the EU. *See The Council of the European Union* (last modified Mar. 31, 1998) <http://europa.eu.int/inst/en/cl.htm#council>. The Council meets twice a year to provide input to the European Parlaiment about policy and development of the European Union. *See id.*

117. *See 2146.Council - Justice and Home Affairs Press Release, Brussels, 03-12-1998, Nr. 13673/98, Presse 427* (visited Mar. 27, 1999) <http://ue.eu.int/newsroom/main.cfm?LANG=1> (Press Release from the 2146th Council Meeting, Council of the European Union, General Secretariat, Justice and Home Affairs Report on the Follow-Up of the 1997 Action Plan on the Fight Against Organized Crime).

118. *See id.*; Telephone Interview with Drew C. Arena, *supra* note 29.

119. *See generally* Prof. Dr. Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society—COMCRIME Study*, *in* SPECIAL LAW AND COUNTRY REPORTS (1998).

120. Europol is a European police office created by convention in 1998. Located at The Hague, Europol is an information clearing house and analysis center with law enforcement liaison officers from the member states. Europol is not a European police force; its mandate is to increase cooperation and communication between and among law enforcement agencies in the member states. *See* Telephone Interview with Drew C. Arena, *supra* note 29.

C. The G-8

1. *Background*. The present G-8 (or "Group of Eight") leading industrialized democracies originated in 1975 at an Economic Summit convened by President Valery Giscard d'Estaing of France and attended by leaders from Germany, Japan, the United Kingdom and the United States.[121] President Giscard and Chancellor Schmidt of Germany wanted to establish an informal forum for world leaders to discuss world economic issues.[122] Italy and Canada joined this original "Group of Five" in 1976-77 and the configuration became known as the Group of Seven, or "G-7."[123] G-7 meetings followed a limited agenda of economic issues, and were intended to provide an informal consultation forum.[124] In the 1980s, these annual meetings became more formalized, with an agreed statement, or communique, issued by the leaders at the conclusion of each summit.[125] Leaders such as President Reagan, French President Mitterand, German Chancellor Kohl, and British Prime Minister Thatcher brought increasingly broader agendas to the table.[126] At the end of the cold war, as democratic and economic reform got underway in Russia, Russian leaders were gradually integrated into the G-7.[127] In 1998, the group's name was formally changed to the "G-8," and the first full G-8 Summit was held in Birmingham in June of that year.[128]

In its current configuration, the G-8's membership includes the majority of the world's most powerful democracies—countries that are global leaders economically, technologically, legally, and politically. This small but powerful membership gives the G-8 certain ad-

---

121. *See What is G8?* (visited Mar. 27, 1999) <http://birmingham.g8summit.gov.uk/brief 0398/what.is.g8.shtml> (the British Foreign and Commonwealth Office web page for the 1998 Birmingham Summit).

122. *See id*.

123. *See id*.

124. *See id*.

125. *See id*. For example, the 1983 Williamsburg Summit, hosted by President Reagan, produced a G-7 agreement to support the deployment of U.S. Cruise and Pershing missiles to Europe to confront new Soviet SS20 missiles. Agreement on common opposition to global terrorism followed at the Tokyo Summit in 1986. *See id*.

126. *See What is G8?*, *supra* note 121.

127. *See id*. Former President Gorbachev attended a meeting in the margins of the London Summit in 1991. Likewise, in 1992 and 1993, President Yeltsin was invited to Summits to discuss financial assistance to the Russian economy, and in 1994 President Yeltsin first took part in foreign policy discussions. The Denver Summit in 1997 was called the "Summit of the Eight," in recognition of broader Russian involvement. *See id*.

128. *See id*.; Richard W. Stevenson, *Rich Leaders Turn Eye to Crime and Debt*, N.Y. TIMES, May 17, 1998, at A11.

vantages over more bureaucratic or cumbersome multilateral organizations.[129]

2. *Focus on High-tech Crime*. After the 1995 Summit in Halifax, Nova Scotia, a group of experts was brought together to look for better ways to fight international crime. In 1996 this group (which became known as the "Lyon Group") produced forty recommendations to combat international crime[130] that were endorsed by the G-8 heads of state at the Lyon Summit in June 1996. Recommendation Sixteen, in part, called for countries to "review their laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalized and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention and international cooperation in respect of such abuses are effectively addressed."[131]

To implement Recommendation Sixteen and otherwise enhance the abilities of law enforcement in combating high-tech and computer-related crime, a subgroup of the Lyon Group was formed in January 1997 ("G-8 Subgroup on High-tech Crime"), and it held its first five meetings during that year.[132] In December 1997, Attorney General Reno hosted the first-ever meeting of her counterparts from the G-8 countries, and the meeting centered on computer crime.[133] At the conclusion of the meeting, the Ministers[134] adopted ten Principles and a ten-point Action Plan to combat high-tech crime, and issued a Communiqué.[135] At the 1998 G-8 Summit in Birmingham,

---

129. "Our small number allows us to act quickly, and our unique membership offers an opportunity to lead the world community that is rarely found in our history. And we are often on the cutting edge for example in responding to international terrorism, to international money laundering, to precursor chemicals." Reno, Chantilly Keynote Address, *supra* note 1.

130. *See G8 and International Crime* (visited Mar. 27, 1999) <http://birmingham.g8summit.gov.uk/crime/>.

131. P8 Senior Experts Group on Transnational Organized Crime, P8 Senior Experts Group Recommendations 3 (Apr. 12, 1996) (on file with the *Duke Journal of Comparative & International Law*) (the P8 Senior Experts Group is also known as the Lyon Group).

132. *See Computer Crime and Intellectual Property Section (CCIPS)* (last modified Nov. 24, 1998) <http://www.usdoj.gov/criminal/cybercrime/intl.html>.

133. *See id.*

134. "Ministers" is a convention that refers to the law enforcement heads from the G-8 countries, the majority of which are either Ministers of Justice or Ministers of the Interior.

135. The full text of the Principles and Action Plan adopted by the Ministers follows:

PRINCIPLES AND ACTION PLAN TO COMBAT HIGH-TECH CRIME

Statement of Principles

We hereby endorse the following PRINCIPLES, which should be supported by all countries:

I. There must be no safe havens for those who abuse information technologies.

II. Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred.

III. Law enforcement personnel must be trained and equipped to address high-tech crimes.

IV. Legal systems must protect the confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.

V. Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime.

VI. Mutual assistance regimes must ensure the timely gathering and exchange of evidence in cases involving international high-tech crime.

VII. Transborder electronic access by law enforcement to publicly available (open source) information does not require authorization from the State where the data resides.

VIII. Forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions must be developed and employed.

IX. To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.

X. Work in this area should be coordinated with the work of other relevant international fora to ensure against duplication of efforts.

Communique Annex: Principles to Combat High-Tech Crime (last modified Mar. 30, 1998) <http://www.usdoj.gov/criminal/cybercrime/principles.htm>.

Action Plan

In support of these PRINCIPLES, we are directing our officials to:

1. Use our established network of knowledgeable personnel to ensure a timely, effective response to transnational high-tech cases and designate a point-of-contact who is available on a twenty-four hour basis.

2. Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.

3. Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes.

4. Consider issues raised by high-tech crimes, where relevant, when negotiating mutual assistance agreements or arrangements.

5. Continue to examine and develop workable solutions regarding: the preservation of evidence prior to the execution of a request for mutual assistance; transborder searches; and computer searches of data where the location of that data is unknown.

6. Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and to study ways to expedite the passing of this data internationally.

7. Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime by preserving and collecting critical evidence.

8. Ensure that we can, in urgent and appropriate cases, accept and respond to mutual assistance requests relating to high-tech crime by expedited but reliable means of communications, including voice, fax, or e-mail, with written confirmation to follow where required.

9. Encourage internationally-recognized standards-making bodies in the fields of telecommunications and information technologies to continue providing the public and private sectors with standards for reliable and secure telecommunications and data processing technologies.

10. Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions.

England, the Heads of State endorsed and agreed to implement their Ministers' Principles and Action Plan.[136] Essentially an international template for fighting high-tech crime, the Principles and Action Plan have been adopted by President Clinton, British Prime Minister Tony Blair, French President Jacques Chirac, Russian President Boris Yeltsin, and the other G-8 leaders. This is quite significant. It is the first time a group of powerful world leaders have jointly adopted a detailed plan for fighting computer crime.[137] Additionally, instead of referring the plan back to member countries for individual action, a subgroup of G-8 experts meets regularly to work cooperatively toward implementation of the Action Plan.

3. *High-tech Crime Subgroup*. As of May 1999, the G-8 Subgroup on High-tech Crime had met fourteen times.[138] Its focus has been on enhancing the abilities of law enforcement to investigate and prosecute high-tech and computer-related crime. The Subgroup's progress and accomplishments include the following:

a. High-tech Points of Contact. In March 1998, a network of high-tech points of contact for law enforcement in each of the G-8 countries was established.[139] These contacts are available twenty-four hours a day to respond to urgent requests for assistance in international high-tech crime investigations or cases involving electronic evidence.[140] Recruitment and education efforts are currently underway to expand this network to include many more Internet-connected countries. The hope is that in the near future, international investigations in this area will not be delayed because of the inability to locate the proper computer crime expert or because of differences in time zones.[141]

b. International Training Conference. In November 1998, the Subgroup hosted an international computer crime training conference for G-8 law enforcement officials.[142] The conference,

---

Communique Annex: Action Plan to Combat High-Tech Crime (last modified Mar. 30, 1998) <http://www.usdoj.gov/criminal/cybercrime/action.htm>.

136. *See The Birmingham Summit: Final Communique*, ¶ 21 (visited Mar. 30, 1999) <http://birmingham. g8summit.gov.uk/docs/final.shtml>. The *Final Communique* was established May 17, 1998. *See id.*; *see also* Stevenson, *supra* note 128; Susan Page, *Trade and Crime Were Also on Agenda*, USA TODAY, May 18, 1998, at 15A.

137. The forty recommendations and the principles on high-tech crime agreed to in 1997 have recently been endorsed by the EU. In addition, the UN is considering changes to its model treaty on mutual legal assistance reflecting the work being carried out by the G-8. *See G8 and International Crime*, *supra* note 130.

which focused on technical and operational issues, allowed cybercrime experts to share knowledge regarding the latest trends and techniques of high-tech criminals, the technical problems encountered in high-tech investigations, and law enforcement solutions. This was the first such conference, and the participants expressed unanimous support for similar future conferences.[143]

c. Review of Legal Systems. The Subgroup is in the process of comparing each country's legal system as it relates to high-tech crime.[144] The project covers substantive and procedural laws, data protection and privacy, search and seizure law, extradition, electronic surveillance (wiretapping), and abilities to secure traffic data (connection information) and subscriber information.[145] This is an important step for the G-8 to take to ensure that the member countries' legal systems appropriately criminalize computer crimes and promote their investigation.

d. Locating and Identifying Computer Criminals ("Preservation of Traffic Data"). Substantial energy has been devoted to this critical topic, which includes access to historical traffic data and future ("real-time") traffic data. As a first step in this area, principles for transborder access to stored computer data have been adopted.[146]

e. Principles for Transborder Searches and Seizures. The Subgroup reached a consensus on principles for transborder access to stored computer data.[147] Among other things, the principles include "fast freeze" recommendations on preserving data in anticipation of a formal request for mutual legal assistance, as well as on expedited processing of formal legal assistance requests. The principles also obligate states to ensure that their national laws and procedures permit them to secure rapid preservation of stored data in a

138. Telephone Interview with Scott Charney, Chief, Computer Crime and Intellectual Property Section, U.S. Department of Justice and Chair, G-8 Subgroup on High-tech Crime (May 7, 1999).

139. *See id.*

140. *See id.*

141. *See id.*

142. Telephone Interview with Scott Charney, *supra* note 138.

143. *See id.*

144. *See id.*

145. *See id.*

146. *See* discussion *infra* Part IV.C.3.e.

147. Telephone Interview with Scott Charney, *supra* note 138.

computer system, even where necessary only to assist a foreign state; endorse some forms of consensual access; and affirm that no authorization from a searched state is required for transborder access to publicly available data.[148] These principles are only recommendations on interim measures, and it is too early in the process to know if complicated issues concerning transborder searches and seizures can be resolved sufficiently to allow for their implementation.[149]

f. Computer Forensics. In recognition of the fact that the International Organization of Computer Evidence (IOCE) has broad representation that includes most of the G-8 countries, the Subgroup, through its Chair, referred to the IOCE the task of developing recommendations for international standards on the retrieval and authentication of electronic evidence.[150] The first step for the IOCE will be defining common terms, identifying methods and techniques to be used, and establishing a common format for forensics requests.[151]

g. Cooperation with Industry. The Subgroup has followed the instruction of the G-8 Heads of State at their Summit in May 1998 for close cooperation with industry.[152] Representatives from hardware manufacturers, telecommunications carriers, and ISPs have made presentations at meetings, and have discussed concrete steps law enforcement and industry can take together to accelerate cooperation between the two.[153]

On going Subgroup work concerning industry includes the following: adopting a process that allows the companies that are developing technical standards, including next-generation Internet technologies, to take into account public safety needs; consulting within governments to ensure that new data protection policies do not provide havens for criminals; standardizing law enforcement requests for assistance to industry, in order to allow industry to respond more quickly and with less expense; and developing twenty-four-hour points-of-contact with critical ISPs. In addition, plans are underway

148. *See id.*

149. *See id.*

150. *See id.*

151. *See id.*

152. *See The Birmingham Summit: Final Communique*, *supra* note 136.

153. These representatives have included America Online (American ISP), NiftyServe (Japanese ISP), and Deutsche Telekom (German telecommunications carrier and ISP).

for a G-8 industry conference on high-tech crime which would bring together high-tech crime-fighters and private sector representatives from the G-8 countries.[154]

D. Organization for Economic Cooperation and Development (OECD)

The OECD is an organization of twenty-nine countries that provides member-governments with a forum to develop economic and social policy.[155] It was formed by convention in 1961 by twenty countries in North America and Western Europe, and since then its membership has been joined by Japan, Australia, New Zealand, Finland, Mexico, the Czech Republic, Hungary, Poland and Korea.[156] Membership is limited to countries which are committed to a market economy and pluralistic democracy.[157] Most work is done in one of the OECD's 200 committees, working groups, and expert groups, and over 40,000 government officials participate in OECD meetings each year. The OECD has a permanent secretariat in Paris, and the United States (like other nations) has an ambassador posted to the OECD.[158]

The OECD has developed and issued a number of documents related to computers and cyberspace. "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" were adopted in 1980.[159] The Guidelines were intended "to harmonise national privacy legislation and . . . to prevent at the same time interruptions in international flows of data."[160] "Guidelines for the Security of Information Systems" were adopted in 1992.[161] These guidelines were intended to raise awareness of risks to information systems and to provide reassurance as to the reliability of information systems. Governments and the private sector were urged to cooperate to cre-

---

154. Telephone Interview with Scott Charney, *supra* note 138.

155. *See About OECD: What is OECD?* (last modified Mar. 26, 1999) <http://www.oecd.org/about/general/ index.htm>.

156. *See About OECD: Membership* (last modified Mar. 26, 1999) <http://www.oecd.org/about/general/member-countries.htm>.

157. *See About OECD: What is OECD?*, *supra* note 155.

158. *See id.*

159. *See Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (last modified Mar. 26, 1999) <http://www.oecd.org//dsti/sti/it/secur/prod/PRIV-EN.HTM>.

160. *Id.*

161. *See Guidelines for the Security of Information Systems* (last modified Mar. 26, 1999) <http://www.oecd.org//dsti/sti/it/secur/prod/e_secur.htm>.

ate an international framework for security of information systems.[162] In 1997, the OECD issued Cryptography Policy Guidelines and the Report on Background and Issues of Cryptography Policy.[163]

E. The United Nations

The United Nations is planning to increase awareness of computer crime issues by sponsoring a workshop on "Crimes Related to the Computer Network" at the Tenth United Congress on Crime Prevention and the Treatment of Offenders, scheduled to be held in Vienna in April 2000.[164] At the request of the Centre for International Crime Prevention in Vienna, the United Nations Asia Far Eastern Institute (UNAFEI) has assumed responsibility for coordinating the workshop.

In October 1998, UNAFEI hosted an experts meeting in Fuchu, Tokyo to begin preparations for this workshop. The group of experts, including representatives from Australia, Canada, India, the Netherlands, Japan, Korea, South Africa and the United States, are planning a workshop program that will demonstrate the legal and technical difficulties of tracking criminal activities over computer networks as well as the problems associated with searching and seizing evidence stored on computer networks. In addition, negotiations are currently underway on a UN Convention on transnational organized crime. It is likely that certain aspects of cybercrime will be addressed by the Convention.[165]

V. CONCLUSION

Criminality deriving from new technologies such as computers, the Internet, and wireless communications provides daunting challenges for law enforcement around the globe. Crimes can be committed remotely, without the criminal ever setting foot in the country where the misdeed occurs or the victim is located. Critical evidence may vanish the moment the culprit ends his transmission. And any hacker can route his communication through a foreign country, thereby adding an international element to his crime which may create insurmountable obstacles for law enforcement. Since the United

---

162. *See id.*

163. *See Cryptography Policy: The Guidelines and the Issues* (last modified Mar. 26, 1999) <http://www.oecd.org//dsti/sti/it/secur/prod/e-crypto.htm>.

164. *See* United Nations General Assembly Resolution 1997/52 of December 1997.

165. Telephone Interview with Greg Schaffer, Trial Attorney, Computer Crime and Intellectual Property Section, U.S. Dept. of Justice (March 8, 1999).

States depends on the stable, consistent operation of such critical infrastructures as banking, telecommunications, and emergency services—all of which have become increasingly automated—the stakes facing the public are quite high indeed.

Although law enforcement officials are loath to admit that any criminal has the upper hand, candid professionals acknowledge that they face an uphill battle in this arena. As technologies evolve, laws need updating so that international legal assistance can be provided, and criminals can be extradited and brought to justice. Countries must dedicate more experts to high-tech crime-fighting, and then provide them with the sophisticated and expensive equipment required for their tasks. The ability to locate and identify criminals must be improved dramatically, although it sometimes seems beyond the limits of existing technologies. And various issues posed by the need to gather electronic evidence of a crime from several countries—often in real-time—must be resolved. As a result, the ultimate outcome of this struggle to maintain public safety in our increasingly automated way of life is far from certain.

Many important steps have been taken in this regard by individual governments, and ambitious efforts are also underway in the international community. But so much more needs to be done. At every level, there must be a heightened appreciation of the threat posed by international high-tech and computer-related crime. Senior government officials have to provide leadership, be receptive to new ways of thinking, and come to understand that many of the old paradigms for crime-fighting no longer suffice.

Finally, these challenges cannot be met unless a true partnership between governments and the private sector comes into being. Policy-makers and law enforcement officials must recognize that law enforcement needs may place burdens on industry, which they should take reasonable steps to minimize. At the same time, industry ought to consider the safety of the public when responding to the needs of the market.

As we begin a new millennium, governments must work together to stay ahead of this next generation of criminal activity. They cannot allow cyberspace to become the new Wild West—a frontier bereft of the rule of law, where criminals prey on citizens with impunity. We must not permit the many benefits of the information age—such as electronic commerce and enhanced communications—to be seriously diminished by their vulnerability to illegal activity.