

# Law Enforcement and Computer Security Threats and Measures

Mathieu Deflem and J. Eagle Shutt, *University of South Carolina*

Introduction	1	Computer Security, Law Enforcement, and the	
Computer Security, the Internet, and Cybercrimes	1	Balance of Order and Liberty	6
National Laws on Establishing Computer Security		The Coordination of Law and Law	
through National Laws	2	Enforcement	6
The Enforcement of National Laws Concerning		Policing Technology, Maintaining Liberty	7
Computer Security	3	Conclusion	8
Building a Global Legal Order to Protect Computer		Glossary	8
Security	4	Cross References	9
Computer Security and International Policing	5	References	9
Variations of Global Policing	5		
The Role of Interpol and Europol	6		

## INTRODUCTION

In the context of democratic societies, policing always involved a delicate task to provide security while also maintaining liberty. With the rapid expansion of computerized technologies and the Internet, this problem is posed even more acutely, for communication methods have not only expanded sharply, but the development of Internet technology has also brought about increased anonymity and freedom in communications. This situation creates a significant law enforcement problem as the same technologies that guarantee anonymity in legitimate transactions also provide new means to violate laws and to hide the identities of lawbreakers. Because of the cross-border nature of computers linked through networks, also, threats against computer security are often global in nature. By the very nature of the Internet as a border-transcending phenomenon, cybercrimes know no geographic boundaries.

From a legal and law enforcement viewpoint, measures against computer security threats pose problems of jurisdictional authority. National legal systems and their enforcement agencies are formally bound to nationally defined borders, whereas even a single transmission of computerized information over a network may pass through a dozen or more types of carriers, such as telephone companies, satellite networks, and Internet service providers, thereby crossing numerous territorial borders and legal systems (Aldesco, 2002). The cross-border nature of threats to computer security justifies the need for international cooperation and the development of global frameworks of law and law enforcement. In this chapter, we review the most important law enforcement efforts that have been taken at selected national and international levels to respond to the challenges affecting computer security.

## COMPUTER SECURITY, THE INTERNET, AND CYBERCRIMES

With the advent and the exponential growth of the Internet and computerized transactions, the modern world has witnessed not only an expansion of new means of communication and the creation of virtual communities among people in disparate geographical locales, but it has also brought about new and unprecedented opportunities for illegitimate conduct (Ditzion, Geddes, & Rhodes, 2003; Maher & Thompson, 2002; Sinrod & Reilly 2000; Sussman, 1999; Wall 2001a). Cybercrimes have become a permanent factor in the current era of the globalization of information and communications. The negative implications of such crimes can be far-reaching in economic and other respects. The total amount of money involved with credit card theft, for example, is estimated at \$400 million annually, whereas stolen patents and trademarks involve \$250 billion a year (Aldesco, 2002; Baron, 2002).

Cybercrimes are relatively easy to execute and require little technical expertise. Toolkits and handbooks to commit cybercrimes are available on the Internet. Estimates show that nearly 50% of all U.S. companies were attacked by a computer virus, worm, or other Internet-related means in 2001. The computers of the Pentagon are attacked about 22,000 times a year. By 2000, intellectual property theft was already estimated to cause American companies losses in excess of \$ 1 trillion (Barr, Beiting, & Grezeskinski, 2003). The so-called Love Bug worm that spread via e-mails to millions of computers in the spring of 2000 led to an estimated \$8.7 billion in damages and may have cost as much as \$10 billion in lost productivity (Bellia, 2001). The U.S. Defense Department reported that the worm had contaminated at least four classified U.S. military computer systems. The Philippine-based college dropout who caused the havoc could not be prosecuted in

the United States as there was no applicable cybercrime law in the Philippines at that time, for which reasons he could also not be extradited (Cesare, 2001).

At least two types of crimes involving computer security can be distinguished (Goodman & Brenner, 2002). In a first category of offenses, the computer is the target of the crime by means of attacks on network confidentiality, integrity, and availability. Among the examples are unauthorized access to and illicit tampering with systems, programs, or computer data. In a second category of cybercrimes, traditional offenses, such as fraud, theft, and forgery, are committed by means of computers, networks, and other information and communications technology. The latter category of offenses is not novel or unique to the era of the Internet, yet it has qualitatively altered in kind by means of the use of advanced technologies, with important implications for legal policy and law enforcement practices.

Besides the high-tech nature of cybercrimes and the anonymity that the Internet affords, the border-transcending nature of the cyberworld is another outstanding characteristic of computer security since the late 20th century. "An international element is often present, not only when a computer system is the target of a crime," Bellia argues, "but also when a system merely facilitates online forms of traditional crimes or serves as a repository for evidence of a crime" (2001, p. 38). The targets of cybercrime, likewise, can be varied in nature, ranging from illicit gambling to the conveying of threats, the transmission of pornography, and attempts to lure children into sexual conduct to fraud and violations of intellectual property. The Internet has also grown in popularity across the globe and is affecting people of various ages, ethnic backgrounds, and class structures. As a result, the potential impact of cybercrimes can be exploited in a more organized manner that is akin to the existing traditional forms of organized crime, enabling the emergence of so-called cybercrime Mafias (Brenner, 2002). The complexity of cybercrime necessitates the development of new legal frameworks at the national and international levels.

## NATIONAL LAWS ON ESTABLISHING COMPUTER SECURITY THROUGH NATIONAL LAWS

The appearance of new social ills in society will typically invoke the passing of new laws designed to prevent or treat the consequences of such problems. Until recently, the spread of computer crimes was unmatched by the development of proper criminal law statutes (Barr et al., 2003; Rustad, 2001). But the sharp rise in intellectual property crimes over the Internet and other crimes related to information in a highly computerized society has led the governments of many nations across the world to enact new criminal statutes specifically tailored to adequately respond to the changing conditions. This chapter will review these legal developments, focusing primarily on the United States and a selection of other nations.

In the United States, laws to protect computer security are primarily based on two pieces of legislation: the

Economic Espionage Act of 1996 and the National Stolen Property Act, which dates as far back as 1934 (Barr et al., 2003). These laws were invoked with renewed vigor because intellectual property crimes by means of the Internet were rising sharply. As the threat of civil action was an insufficient deterrent to thwart the theft of trade secrets and the infringement of trademarks, patents, and copyrights, U.S. Congress passed the Economic Espionage Act in 1996 to criminalize the theft of trade secrets. Other acts have been passed to adequately respond to specific nature of crimes committed in cyberspace. For instance, in 1997, the No Electronic Theft Act was passed to broaden criminal liability for copyright infringement even when no financial gain is involved (Rustad, 2001). The act was passed after an Massachusetts Institute of Technology student had been acquitted for distributing copyrighted software on the Internet because he had received no financial gain from his distribution activities.

The National Stolen Property Act provides criminal sanctions for the transmission of goods and moneys that are known to have been stolen or taken by fraud. Although the act was not designed to apply to theft by computerized means, U.S. federal courts have held that the act can be applied in this circumstance. Originally, the stolen item had to be physically removed for an offense to be prosecutable under the act, but more recently some courts ruled that electronic transmission may be sufficient.

Legal responses at the national level toward the protection of computer security are sometimes only of limited value, because their application and enforcement is limited to jurisdictional borders (whereas cybercrimes are not). The U.S. Copyright Felony Act, the No Electronic Theft Act, and the Digital Millennium Copyright Act, for example, all distinctly focus on computerized information, but they cannot be applied in an extrajurisdictional context. The Economic Espionage Act, however, also applies to economic espionage that occurs overseas, at least when it involves an offender who is a U.S. citizen or corporation or as long as some part of the illegitimate activity is connected to the United States (Barr et al., 2003, pp. 777-778).

The cross-border nature of many computer crimes need not necessarily be addressed by extending national laws to apply to extrajurisdictional territories. Providing there is some degree of coordination among national legal systems, an option toward effective criminalization is provided by cooperation across nation-state borders (Brenner & Schwerha, 2002). Such cooperation is legally secured through mutual legal assistance treaties among nations. The United States, for example, maintains some 40 bilateral mutual legal assistance treaties with foreign nations. These treaties provide both legal and practical means by which one country can seek or provide legal assistance from or to another country (Department of Justice, 2001). Legal cooperation across nations, however, requires that all participating countries have developed similar statutes.

A discussion of all national legal frameworks on computer security is beyond the scope of this chapter. But reviewing a useful selection, it can be noted that many nations have developed explicit criminal codes against cybercrimes (Schjolberg, 2003). In the Americas, the Mexican

penal code specifies that anyone who destroys or causes loss of information contained in computer systems or computer equipment protected by security measures shall be liable to punishments involving imprisonment or fines. Brazil has since July 2000 criminalized the entry of false data into information systems. Other Latin American countries, such as Venezuela and Chile, have passed similar legislation.

The Canadian Criminal Code criminalizes any attempts to fraudulently obtain a computer service or intercept any function of a computer system. In Australia, federal legislation was enacted with the Cybercrime Act of 2001, which criminalizes unauthorized access to, or modification of, data held in a computer to which access is restricted. Among the first nations to enact new laws to protect computer security, the United Kingdom passed a Computer Misuse Act in 1990 to penalize unauthorized access to computer materials. Also in Europe, the French penal code that went into effect in March 1993 provided for the criminalization of attacks on systems for automated data processing. The code criminalizes fraudulent access to an automated data processing system, as well as hindering the functioning of such systems and the fraudulent introduction or modification of data therein. Italy's penal code includes articles on the unauthorized access into computer or telecommunication systems. Similar regulations to protect data were introduced in Germany, Greece, and other European countries. In Belgium, for example, the national parliament in November 2000 adopted legal articles on computer crimes such as computer forgery, computer fraud, computer hacking, and sabotage.

Outside of Europe, China passed new legislation as early as 1994, when regulations were enacted concerning measures to protect the safety of computer information. India passed the Information Technology Act of 2000 that specifies regulations against the hacking of computer systems. Similarly, Japan introduced an Unauthorized Computer Access Law that went into effect in February 2000. In 2002, South Africa enacted an Electronic Communications and Transactions Act, which penalizes cybercrime as the unauthorized access to, interception of, or interference with computerized data.

## THE ENFORCEMENT OF NATIONAL LAWS CONCERNING COMPUTER SECURITY

Passing appropriate laws is a necessary step to respond to crimes, but without effective police operations, such laws would remain inconsequential (Rustad, 2001). The policing of laws related to computer security poses several special problems, not least of all because of the enormous popularity of the Internet and the widespread use of computers. Already by the late 1990s, it was estimated that a global population of some 19 million computer users would have the necessary skills to mount a cyberattack should they choose to use their proficiency for such illegitimate purposes (Cilluffo, Pattak, & Salmoiraghi, 1999). The expansion of the Internet itself has contributed to the growing availability of the tools and skills necessary

to carry out a cybercrime. Moreover, the relative lack of technological expertise among enforcement agencies—at least until recently—initially posed serious limitations to the adequate implementation of any law enforcement plans (O'Neill, 2000). The technological characteristics of cybercrimes also affect the nature of appropriate police actions. The anonymity of the communicator and the methods used to shield one's true identity create considerable problems for the enforcement of any law concerning information and identity theft (Davis, 2003).

The strategies to police cyberspace that were implemented in recent years in the United States provide a good example of the value and limitations of jurisdictionally confined enforcement (Ditzion et al., 2003). Police actions to enforce laws concerning computer security were first stepped up during the Clinton administration. U.S. Congress expanded the scope of the Computer Fraud and Abuse Act, originally passed in 1986 in response to the so-called war games epidemic, to lower the punishable standard of criminal intent in cases of unauthorized computer access, ensuring that a broad class of hackers would be accountable under the statute and broadening the category of protected computers.

In the United States, a leading role in computer-related law enforcement efforts has been adopted by the Federal Bureau of Investigation (FBI), which established so-called computer crime teams in its various field offices across the U.S. states (Wolf, 2000). The FBI also set up the National Infrastructure Protection Center to function as a national law enforcement investigation and response entity for critical infrastructure threat assessment, warning, and vulnerability (Gravell, 1999). These activities have not been without consequences, as many prosecutions of computer criminals evolved from FBI stings operations (Barr et al., 2003).

Besides the operations by the FBI, relevant criminal enforcement strategies in the United States are also undertaken by a host of other agencies. The Central Intelligence Agency (CIA) is involved in securing computer communications through the monitoring of communications (Baron, 2002). In the Justice Department, the Computer and Telecommunication Coordinator (CTC) Program has been set up since 1995 at the recommendation of the Computer Crime Unit, now called the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division (<http://www.cybercrime.org>). Every U.S. attorney's office has designated at least one CTC and over 35 districts have two or more. A total of 137 U.S. attorneys are presently working in the CTC Program. The CTCs have responsibility to prosecute computer crimes, serve as technical advisors to other U.S. attorneys, act in liaison with attorneys in other districts, and provide training and guidance to other attorneys and to federal and local agencies in their districts. More recently, since July 2001, additional Computer Hacking and Intellectual Property (CHIP) units of prosecutors have been established to work in collaboration with the FBI and other agencies. Likewise, the FBI organized a cyberbanking initiative in cooperation with the Departments of Justice and the Treasury as well as financial regulatory agencies to examine the risks associated with electronic banking technology (*Cyber Crime*, 1998).

Also established by the U.S. Department of Justice was the National Cybercrime Training Partnership (NCTP) to collaborate with all levels of law enforcement and develop a long-range strategy for high-tech police work, including interagency cooperation, networking, and training (Williams, 1999). At present, NCTP activities are in hiatus pending the formation and initial meeting of a new body, the Cybercrime Advisory Board, under the direction of the National White Collar Crime Center (NW3C). The latter center also runs the Internet Fraud Complaint Center (IFCC) in partnership with the FBI to address fraud committed over the Internet. The IFCC acts as a central repository of fraud complaints for the law enforcement community and provides an easy-to-use reporting mechanism for fraud victims. Another way for citizens to get involved in computer security is through the Cyber Citizen Partnership, a program set up by the Department of Justice and the Information Technology Association of America that involves a Web site to teach children about the right ways to use the Internet.

As is the case in matters of national legal systems, law enforcement measures on computer security have been implemented in many countries across the world. In Canada, a Tech Crime Unit has been established in the Royal Canadian Mounted Police. The Federal Police in Australia has Electronic Forensic Support Teams in most of the country's major cities. In the United Kingdom, a National Hi-Tech Crime Unit was established in 2001. By 2003, the unit's investigations had led to more than 100 arrests in over 40 operations. Special attention is paid to the unit's collaboration with the cybercrime police in other countries. Other countries in Europe, indeed, have similar specialized units set up in their respective police forces. Outside of Europe, the situation is no different as specialized "cybercop" teams are set up in many countries across the globe. For example, the Central Bureau of Investigation in India has established a unit to police Internet communications and cooperate with Indian portals to safeguard against cyberattacks. Special emphasis is placed on the training of officers to serve in such units, as their skills are very different from those needed in a more traditional police role.

## BUILDING A GLOBAL LEGAL ORDER TO PROTECT COMPUTER SECURITY

Similar to the problems associated with legal frameworks, enforcement activities are especially affected by the cross-border nature of computer security-related activities in cyberspace (Calkins, 2000). Yet, among legal scholars there is disagreement on the value of international legal systems in the case of computer security and related Internet activities (Bellia, 2001; Berman, 2002). Some argue that laws regulating online activities crossing national borders are always ineffective because they are to be implemented in nations with limited jurisdiction. Other, however, suggest that the Internet is no less subject to extraterritorial authority than other forms of international activities that had already been regulated by international law for many years before the advent of the Internet. The reality is that the development of cyberspace

as a decidedly global phenomenon has instigated a host of legal initiatives at the international level. Mirroring the development of international police cooperation from the 19th century onward (Deflem 2002a, 2002b), technological advances are typically addressed at overcoming barriers of space and time, and criminal law and law enforcement respond in kind to internationalize their range and activities.

The history of the regulation of illegitimate conduct in cyberspace shows a steady expansion of applicable laws and an increasing involvement of various international bodies to tackle the cross-border nature of cybercrime (Goodman & Brenner, 2002; Grabosky & Smith, 2001; Norman, 2001; Wall, 2001b). Among the key players are the Organization for Economic Cooperation and Development (OECD), the Council of Europe, the European Union, and the United Nations.

Pertinent activities of the OECD date back to 1983 when the organization was assigned to secure a harmonization of European computer crime legislation. In the mid-1980s, the Select Committee of Experts on Computer-Related Crime of the Council of Europe thereupon drafted a recommendation to provide for an adequate and quick response to cybercrime by harmonizing existing legislation in the EU countries and improving international legal cooperation. By the mid-1990s, the Council of Europe had issued several reports detailing appropriate surveillance activities and methods of investigation in the realm of information technology.

Many international bodies were involved in developing an international regulation of cyberspace. In 1990, the United Nations first addressed some of the international legal issues associated with cybercrime. The U.N. Congress then urged the world's nations to step up their efforts to legally respond to computer crime and promote the development of an international legal framework. Also during the 1990s, international agreements were reached that specifically concerned trade secrets and the manner in which business information is to be protected. In 1994, the Uruguay Round Agreement presented Trade-Related Aspects of Intellectual Property Rights (TRIPs), and the OECD stipulated Guidelines on Security and Information Systems in 1992 and Guidelines for Cryptography Policy in 1997. Under the TRIPs agreement, enforcement of intellectual property rights can be obligated, whereas the OECD agreements are guidelines that do not attach binding obligations.

In 1997, the Justice and Interior Ministers of the Group of Eight (G8) met in Washington, D.C., and adopted a set of principles to combat hightech crimes as well as an Action Plan to Combat High-Tech Crime (Bellia, 2001). The G8 agreement provides for national governments to pass legislation that enables international cooperation to keep pace with the development of technology and its use for illegitimate purposes.

The G8 action plan was a significant development in the internationalization of computer security law, for it inspired the Council of Europe to prepare a Convention on Cyber-Crime that has been favorably received in many countries since the convention was complete in 2001 (Aldesco, 2002; Baron, 2002; Davis, 2003; see also Brenner, 2002; Keyser, 2003; Marler, 2002). The primary goal of

the convention is to pursue a cross-national policy against the threat of cybercrime by developing appropriate legislation and enhancing international cooperation (Aldesco, 2002, p. 93). The convention includes a harmonization of laws to prevent and suppress computer(-related) crimes by establishing a common standard of offenses. This legislation should cover a variety of related areas such as the illegal interception of and interference with computer data, computer-related forgery and fraud, child pornography, and violations of copyright.

The Convention on Cyber-Crime was the first formalized international treaty on criminal offenses conducted against or by means of a computer and computer networks. With initial preparations going back to the late 1980s, the convention was formally signed in November 2001 by 26 member states of the Council of Europe as well as by the United States, Canada, Japan, and South Africa. The United States had been involved in the elaboration of the convention in its capacity as an observer at the Council of Europe. Not all of the signing countries ratified the convention, although the convention finds broad support. Heralded as the only multilateral treaty to address the problems of computer-related crime and electronic evidence gathering, U.S. President Bush in November 2003 asked the U.S. Senate to ratify the convention. These and other international legal frameworks have distinct implications for law enforcement.

## COMPUTER SECURITY AND INTERNATIONAL POLICING

From an international policing viewpoint, potential threats against computer security relate intimately to the specific means and object matter of computerized information. Computer security threats often concern multiple national jurisdictions. Police activities, in response, have to concentrate on locating the source of the communication to connect the traces of a cybercrime with a real person in the physical world. The infrastructure of the Internet does not provide a ready mechanism for tracing this "electronic trail" (Aldesco, 2002) that leads from the effects of a crime back to its perpetrator. Special strategies at an international level are needed to police threats against computers in a manner that is both effective and appropriate relative to applicable laws. Three basic models can be identified in the international policing of cybercrime: trans-border police actions involving unilaterally conducted investigations abroad, bilateral agreements among countries or their law enforcement agencies, and the establishment of multilateral regimes (Deflem, 2002a; see also Bellia, 2001).

### Variations of Global Policing

In the case of transnational police activities on foreign soil, it is striking to note that the legal systems of some nations allow for extraterritorial police activities, even without a corresponding legal system in the country in which cross-border activities take place. Such transnational police activities often take place without the knowledge or consent of the host country. Some states assert a legal right to conduct "remote crossborder searches" (Bellia, 2001,

p. 39) by using computers located within their jurisdiction to examine data that are stored outside of their jurisdiction. For example, in 2000, FBI agents downloaded data from Russian computers as part of an investigation of a ring of Russian hackers who had been targeting several U.S. companies.

International cooperation among police agencies can occur without explicit legal agreements, instead relying on an autonomously developed professional police culture among security and intelligence agencies across national borders (Deflem, 2002a). Law enforcement agencies in the United States and other countries can independently cooperate and undertake joint efforts in the policing of cyberspace. For instance, the Cybersmuggling Center operated by the U.S. Customs Service has been involved in cyberinvestigations concerning money laundering and child pornography distribution in cooperation with police from Germany, Indonesia, Italy, Honduras, Thailand, and Russia (President's Working Group, 2000).

When computer security-related crimes are subject to laws in one country but not in another, cooperation to investigate pertinent crimes may be hampered and extradition may be unlikely. Yet this limitation is not always in place, because some mutual legal assistance treaties among countries allow for assistance when illegitimate conduct is considered a crime in the state that requests extradition even though that conduct is not criminalized in the state from which assistance is requested (President's Working Group, 2000). Most often, however, especially in the more sensitive area of searches and seizures, a condition of dual criminality must exist whereby a particular type of conduct is considered a crime in both countries involved in a bilateral cooperation agreement.

Bilateral cooperation among nations is precarious, not only because each country involved in cooperation would have to develop similar laws, but also because each country would have to entertain agreements with all other nations of the world. As a perfect consensus about international policing of computer security among all of the world's nations is unlikely, the planning and implementation of multilateral strategies can be a more effective way to develop adequate global law enforcement. Because the Internet now connects virtually every country in the world, the law enforcement challenges posed by this global communication system also have to respond globally. Thus, the international legal frameworks that have been developed on matters of cybercrime carry implications for international law enforcement, especially at the level of each participating nation state and how its law enforcement agencies cooperate with one another. The Council of Europe's Convention on Cyber-Crime, most clearly, has distinct implications for international policing activities. As the convention seeks to harmonize procedures of mutual assistance among nations, special provisions are accorded to law enforcement to aid the investigation of cybercrimes (Aldesco, 2002). The nations that have signed the convention are required to ensure that special police measures are available, such as the realtime collection of traffic data and the interception of content data. The convention also enables police agencies of one nation to collect evidence related to cybercrimes for the police agency of another country and to establish a permanent

communications network to provide international assistance with ongoing investigations. Under the provisions of the convention, also, police in a country are now authorized to request “that their counterparts abroad collect an individual’s computer data, [and] have the individual arrested and extradited to serve a prison sentence abroad” (Aldesco, 2002, p. 95).

### The Role of Interpol and Europol

The international dimensions of law enforcement also include multilateral organizations that have been set up among police agencies. Such international police organizations enable participating agencies to cooperate in the form of direct police-to-police information exchange, even when no formal intergovernmental accords have been reached (Deflem, 2002a). Among the most important of these organizations are the International Criminal Police Organization, better known under its abbreviation Interpol, and the European Police Office, called Europol.

Interpol is an international organization aimed at providing and promoting mutual assistance among criminal police agencies within the limits of their respective national laws and the Universal Declaration of Human Rights (Deflem, 2002a). Originally formed in Vienna in 1923, Interpol is not a supranational police agency, but a collaborative structure among law enforcement agencies from various nations that are linked via specialized national bureaus with a central headquarters in Lyon, France. Presently, Interpol involves police agencies from 181 national states. Interpol has been involved in efforts to combat information technology-related crime for a number of years through a system of so-called working parties on information technology crime that have been set up in various regions of the world (Goodman & Brenner, 2002; *Interpol’s contribution*, n.d.). The European Working Party on Information Technology Crime was the first to be set up under this provision in 1990. It compiles a computer crime manual, organizes training courses in Internet-related crimes, and has set up a rapid information exchange system to transmit relevant information swiftly among the member agencies. The other working parties, which have been set up in the Americas, Africa, and Southern Asia, similarly work toward increasing the flow of information on computer security-related matters among its various agencies.

At a global level including all of its member agencies, Interpol has also instigated a number of activities. The Steering Committee for Information Technology Crime has been established to coordinate and harmonize the initiatives of the various regional working parties. Interpol also organizes international conferences on computer crime to share relevant information among its members (Goodman & Brenner, 2002). Initiatives have also been taken to secure coordination with private ventures geared at securing information. In 2000, for instance, Interpol agreed to provide intelligence to the private Web site Atomic Tangerine, which in return would pass on to Interpol information gathered from its monitoring of the Internet. Atomic Tangerine operates a Net Rader service that had on earlier occasions informed police authorities of a Pakistani Internet service provider that had been hacked into as a base to launch other Web site attacks.

Establishment of Europol was agreed upon in the Maastricht Treaty on the European Union in 1992 (Europol website; Rauchs & Koenig, 2001). Based in The Hague, The Netherlands, Europol started limited operations in January 1994 in the form of the Europol Drugs Unit (EDU). After the Europol Convention was ratified by all member states, Europol commenced the full scope of its activities in July 1999. The aim of Europol is to improve the effectiveness and cooperation among the competent authorities of the member states in preventing and combating serious international organized crime. Europol’s areas of investigation include illicit drug trafficking, terrorism, child pornography, financial crimes, and cybercrime.

In matters of computer security and cybercrime in the European Union, Europol is involved only when an organized criminal structure is involved and two or more member states are affected (Computer Fraud and Security 2002; Europol website). Europol has set up a network of cybercrime units among its participating agencies, a centralized monitoring center at Europol headquarters, and a working group to establish cooperation with the private sector. In October 2002, Europol formed a High Tech Crime Center, a task force that has as its mission the coordination of cross-border cybercrime investigations in the European Union. In 2003, Europe’s policing activities against cybercrimes were stepped up by the creation of a European-wide rapid reaction force against attacks on vital computer networks in the form of a single round-the-clock information exchange system against cyberattacks.

## COMPUTER SECURITY, LAW ENFORCEMENT, AND THE BALANCE OF ORDER AND LIBERTY

With respect to the law enforcement aspects of computer security, a number of interesting issues and problems are revealed. The cross-border nature of computerized information exchange highlights the limits of national laws and law enforcement strategies and reveals the need for a coordination of law and law enforcement across jurisdictions. At the same time, continued efforts have to be made to protect liberty, privacy, and other democratic values that are promoted in an open and free society.

### The Coordination of Law and Law Enforcement

A central concern with the existence of diverse national legal systems on computer security is that for national laws to be enforceable, the jurisdictional authority of a nation has to be recognized by other states (Berman, 2002; Speer, 2000). Consensus among the standards of law across nations would alleviate this problem, but there are difficulties with harmonizing various approaches to computer security issues such as copyright infringement and intellectual property theft. International treaties are surely a worthwhile ideal (Weber, 2003), but they cannot be effective unless the participating nations already resemble one another in social, cultural, and economic respects and it is precisely this condition of egalitarianism that is often not

met. The cultures of nations, for instance, differ widely in terms of the emphasis they place on privacy, appropriate law enforcement strategies, and the very notion of jurisdictional sovereignty (Davis, 2003; Fischer-Hubner, 2000; Mayer-Schonberger, 2003).

An ironic consequence of the difficulties to establish a global legal order in matters of computer security (and other important legal issues) is that the lack of formal international agreements increases the likelihood of certain countries trying to exert extraterritorial jurisdiction on other countries (Podgor, 2002). Federal U.S. agencies, in particular, have often sought to assert federal extraterritorial jurisdiction in the prosecution of computer fraud activities that take place or originate from outside the borders of the United States. However, other countries might in turn resist such intrusive attempts that are seen as interfering with the national jurisdictional authority (Deflem, 2001, 2004a). Conflicts over extraterritorial claims cannot aid toward the development of coordinated legal and law enforcement strategies.

Some of the concerns that have been raised surrounding the European Convention on Cyber-Crime nicely illustrate the difficulties that international treaties on computer security face. Some members of the U.S. Congress, for instance, have criticized the European Convention because its widespread implementation would ultimately mean that the European data protection laws, which are considered too strict, might become the world's unitary privacy standard (Davis, 2003). As such, the convention raises resentment from nations on whose support it must ultimately rely. Related concerns have been expressed against the chilling effect the provisions of the convention might have against business enterprises, based in the United States or in other countries, whose commercial interests reach well beyond their respective national home bases.

More countries agreeing to the provisions of the European convention might lead other countries to also join in this international effort (Oddis, 2002). Yet, it can also be argued that adherence to the convention will violate jurisdictional and constitutional authority problems, because the individual states of the United States would not be allowed to create any conflicting or superceding laws to an agreed upon international treaty (Fisher, 2001; Hopkins, 2003). Even if such jurisdictional issues are cleared, there would still be a considerable problem with the fact that the enforcement and prosecution of the agreed upon international laws are left to the various participating states (Mayer-Schonberger, 2003). As Bellia (2001, p. 59) argues, an international agreement still leaves "in the hands of the state where the data is physically stored the power to search or seize the data in question."

### **Policing Technology, Maintaining Liberty**

Some cybercrimes involve criminal offenses that also exist in "realspace" (O'Neill, 2000) but that can now be executed with more speed and efficiency. The technological sophistication of threats to computer security change the nature of appropriate law enforcement activities, as detection and prosecution become considerably more difficult. As such, the policing of computer security relates

intimately to the ever-evolving relationship between technology and law and the continued need to find the most efficient and appropriate way to handle concerns of law and law enforcement in a technologically advanced world. Because of the speed with which technological advances are made and the intrinsic complexity of modern technologies, existing systems of law and law enforcement are often outdated soon after they have been planned and implemented (Skibell, 2003).

The technologically sophisticated nature of computer crimes means that law enforcement must recruit and train computer specialists and place priority on cooperation and intelligence sharing (McFarlane, 2001). But the technological nature of computer security might also imply that a strategy of law enforcement is needed that shifts the burden of protection of the technology to the manufacturer. This burden-shifting approach would target the design flaws that can lead to security-related failures (Katyal, 2003; Pinkney, 2002). Although not everybody will agree with this strategy, it is clear that cooperation between the government and its agencies, on the one hand, and the private sector, on the other, is needed (Coleman & Sapte, 2003). The fact that attacks against computer security also create economic damage provides at least a commercial incentive for active cooperation from the private sector. Strategies of security are not free, but neither are the consequences of insecurity (Hinde, 2003).

Debates surrounding the protection of privacy rights are virtually concomitant with the rise of new technologies. In matters of computer-related crimes, civil libertarians have argued that police actions should always remain mindful of the legitimate transactions that are conducted over the Internet and other technological communication systems (Brenner, 2003; Huie, Larabee, & Hogan 2002; Tountas, 2003). Aldesco (2002), for instance, argues that law enforcement has a legitimate interest in combating computer crimes, but that government agencies should not invade the privacy of legitimate communications. Although the anonymity afforded by the Internet can be abused, it is also an important value in a society committed to the free development of communications (Marx, 2001).

Newly developed law enforcement methods to ensure computer security are often less concerned with protecting the liberties granted in a democratic constitutional state (Kennedy, 2002). The European Convention on Cyber-Crime, for instance, empowers law enforcement agencies with the authority to search and seize information that is stored on computer systems, at least when such activities are part of a particular investigation into a cybercrime. By giving new powers to law enforcement to investigate cybercrimes, even outside of their respective jurisdictions, an imbalance may be created when there are no increasing protections for personal privacy. It is to be noted that such issues of individual rights are also important to consider relative to foreign nationals who commit cybercrimes and who are then subject to computer searches and other investigative procedures by law enforcement (Young, 2003). Given the disparity in the recognition of liberty and civil rights across the world, the inhabitants of some countries will be more likely to face dire consequences than will others (Huie et al., 2002), further enhancing inequality on an international scale.

## CONCLUSION

Law enforcement is an important and necessary component among the efforts to maintain computer security. Because of the rapid and widespread expansion of computerized technologies and because of the border-transcending nature of computers linked through networks, the policing of threats against computer security presents a challenge to traditional means of crime detection and investigation on an international scale. Existing notions of jurisdictional authority have to be redefined to meet the global needs of information security. Trying to avert cybercrimes and the economic and social harm they can cause, many nations across the world have developed new legislation. Extending these legislative efforts are international systems of law, such as the European Convention on Cyber-Crime, to respond to the need for international legal cooperation and more adequately address cybercrimes and related cross-borders threats against computer security.

Without adequate law enforcement, laws remain ineffective. In the case of computer security, law enforcement agencies have instituted specialized computer crime teams to focus on the ways in which crimes can be perpetrated against or with the aid of computers. As with their accompanying legal systems, pertinent law enforcement activities often extend beyond the reach of jurisdictional boundaries, whether via cooperation among the police forces of different nations or through unilaterally enacted police actions abroad. International police operations pose special problems of coordination among the law enforcement agencies of various countries and they also lead us to rethink the need for police to preserve liberty and legitimate computer transactions while seeking to police computer crimes effectively.

Law enforcement efforts against threats to computer security do not respond merely to technological developments, but also take shape in specific sociohistorical circumstances. Since the terrorist attacks of September 11, 2001, many dimensions of law enforcement have undergone considerable changes, not only in terms of counterterrorism strategies but also with respect to other aspects of crime and crime control (Deflem, 2004b). The policing of computer security issues has also been altered since 9/11 because scores of systems relating to security, means of transportation and communication, and other public facilities rely heavily on computerized systems (Birnhack & ElkinKoren, 2003; Brenner & Goodman, 2002; Raghavan, 2003). Given contemporary society's heavy reliance on computers, it is possible, for instance, for a terrorist group or individual to hack into the computers that oversee the subway system of a city or the railway network of a country. Following the attacks of 9/11, interest in and concern for computer security has skyrocketed, especially in connection with cyberterrorism. To be sure, cyberterrorism does not fully equate with cybercrime, but there is some overlap. For example, the initial stages of the offenses may be similar (e.g., sending out a computer virus), so that the response from a law enforcement viewpoint can be similar as well. But cybercrime and cyberterrorism differ in the harm they may cause and the motivation that is involved. In practice, however, the legislative responses—on both

the national level and the international level—often confuse between the two offenses and have thus sped up the development of new means to police cybercrimes.

The strongest indicator of the changes affecting cyber-related matters in the post-9/11 era is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act in the United States (Berkeley Technology Law Journal, 2004; Copeland, 2004). Among other provisions, the act gives authorities new powers by means of expanded options for wiretaps and technological systems of cybersurveillance (Ventura, Miller, & Deflem, in press). Relatedly, also, the National Cyber Security Division was created in the Department of Homeland Security in June 2003 as part of the National Strategy to Secure Cyberspace. Similar such new laws and the means to enforce them are now being set up in many other countries. Cyberlaw and law enforcement are a rapidly expanding reality. Ongoing developments indicate that, after several years of slowly responding to the threat of cybercrime, the events of 9/11 have served as an important catalyst to step up efforts to provide computer security through law and law enforcement. Although most cybercrimes do not relate to terrorism, the terrorist events of 9/11 may have provided the strongest impulse to develop new coordinated means against all types of cybercrime.

## GLOSSARY

**Computer Security Threats** Potential and actual violations of law that either involve attacks on the security of computers or that use a computer to commit an illegal act.

**Convention on Cyber-Crime** An international treaty initiated by the Council of Europe that involves a harmonization of legislation and an enhancing of international cooperation to prevent and suppress computer-related crimes.

**Cross-Border Law Enforcement** Activities of law enforcement agencies that transcend the jurisdictional authority of national states.

**Cybercrimes** Criminal activities involving the use of the Internet, including such criminal acts as fraud, identity theft, and cyberterrorism.

**Cybercop Units** Popular term for specialized units in law enforcement agencies that deal with cybercrimes and criminal activities associated with computerized information systems.

**International Policing** Police activities that involve citizens of other national states by means of international cooperation with foreign police, transnational police operations in foreign countries, or supranational crime developments affecting police in more than one country.

**Law Enforcement** The formal institutions of national states, and the functions that are associated with them, to enforce compliance to laws and investigate violations of law.

**Legal Systems** The whole of laws formally enacted by governing bodies, including the governments of national states and international governing agencies. Legal systems are accompanied by enforcement agencies and typically comprise civil and criminal laws.

## CROSS REFERENCES

See *Combating the Cyber Crime Threat: Developments in Global Law Enforcement; Cyberterrorism and Information Security; Law Enforcement and Digital Evidence; Privacy Law and the Internet*.

## REFERENCES

- Aldesco, A. I. (2002). The demise of anonymity: A constitutional challenge to the convention on cyber crime. *Loyola of Los Angeles Entertainment Law Review*, 23, 81–123.
- Baron, R. M. F. (2002). A critique of the international cyber crime treaty. *CommLaw Conspectus*, 10, 263–278.
- Barr, K., Beiting, M., & Grezeskinski, A. (2003). Intellectual property crimes. *American Criminal Law Review*, 40, 771–823.
- Bellia, P. L. (2001). Chasing bits across borders. *University of Chicago Legal Forum*, 2001, 35–101.
- Berkeley Technology Law Journal. (2004). Cyberlaw: additional developments. *Berkeley Technology Law Journal*, 19, 543–553.
- Berman, P. S. (2002). The globalization of jurisdiction. *University of Pennsylvania Law Review*, 151, 311–432.
- Birnhack, M. D., & ElkinKoren, N. (2003). The invisible handshake: The reemergence of the state in the digital environment. *Virginia Journal of Law and Technology*, 8. Retrieved March 24, 2004, from [http://www.vjolt.net/vol8/issue2/v8i2\\_a06-Birnhack-Elkin-Koren.pdf](http://www.vjolt.net/vol8/issue2/v8i2_a06-Birnhack-Elkin-Koren.pdf)
- Brenner, S. W. (2002). Organized cyber crime? How cyberspace may affect the structure of criminal relationships. *North Carolina Journal of Law & Technology*, 4, 1–50.
- Brenner, S. W. (2003). Complicit publication: When should the dissemination of ideas and data be criminalized? *Albany Law Journal of Science & Technology*, 13, 273–429.
- Brenner, S. W., & Goodman, M. D. (2002). In defense of cyberterrorism: An argument for anticipating cyberattacks. *University of Illinois Journal of Law, Technology & Policy*, 2002, 1–57.
- Brenner, S. W., & Schwerha, J. J., IV. (2002). Transnational evidence gathering and local prosecution of international cyber crime. *John Marshall Journal of Computer & Information Law*, 20, 347–395.
- Calkins, M. M. (2000). They shoot Trojan horses, don't they? An economic analysis of anti-hacking regulatory models. *Georgetown Law Journal*, 89, 171–224.
- Cesare, K. (2001). Prosecuting computer virus authors: The need for an adequate and immediate international solution. *Transnational Lawyer*, 14, 135–170.
- Cilluffo, F. J., Pattak, P. B., & Salmoiraghi, G. C. (1999). Bad guys and good stuff: When and where will the cyber threats converge? *DePaul Business Law Journal*, 12, 131–168.
- Coleman, C., & Sapte, D. W. (2003). Securing cyberspace: New laws and developing strategies. *Computer Law and Security Report*, 19, 131–136.
- Copeland, R. A. (2004). War on terrorism or war on constitutional rights? Blurring the lines of intelligence gathering in post-September 11 America. *Texas Tech Law Review*, 35, 1–31.
- Computer Crime & Intellectual Property Section of the Criminal Division, Department of Justice. (n.d.). Retrieved May 14, 2005, from <http://www.cybercrime.gov/compcrime.html>.
- Cyber crime, transnational crime, and intellectual property theft: Testimony before the Joint Economic Committee, United States Congress (1998) (testimony of J. N. Gallagher).
- Cyber Security Research and Development Act, Pub. L. 107–305, 107th Congress (2002).
- Davis, E. S. (2003). A world wide problem on the World Wide Web: International responses to transnational identity theft via the Internet. *Washington University Journal of Law & Policy*, 12, 201–227.
- Deflem, M. (2001). International police cooperation in Northern America: A review of practices, strategies, and goals in the United States, Mexico, and Canada. In D. J. Koenig & D. K. Das (Eds.), *International police cooperation: A world perspective* (pp. 71–98). Lanham, MD: Lexington Books.
- Deflem, M. (2002a). *Policing world society: Historical foundations of international police cooperation*. Oxford, UK: Oxford University Press.
- Deflem, M. (2002b). Technology and the internationalization of policing: A comparative-historical perspective. *Justice Quarterly*, 19, 453–475.
- Deflem, M. (2004a). The boundaries of international cooperation: problems and prospects of U.S.-Mexican police relations. In M. Amir & S. Einstein (Eds.), *Police corruption: Challenges for developed countries—Comparative issues and commissions of inquiry* (pp. 93–122). Huntsville, TX: Office of International Criminal Justice.
- Deflem, M. (Ed.). (2004b). *Terrorism and counterterrorism: Criminological perspectives*. Oxford, UK: Elsevier Science.
- Department of Justice, Computer Crime and Intellectual Property Section (CCIPS). (2001). *Seizing computers and obtaining electronic evidence in criminal investigations*. Washington, DC: U.S. Department of Justice.
- Ditzion, R., Geddes, E., & Rhodes, M. (2003). Computer crimes. *American Criminal Law Review*, 40, 285–336.
- Fisher, J. (2001). The draft convention on cyber crime: potential constitutional conflicts. *UCLA Law Review*, 32, 339–361.
- Fischer-Hubner, S. (2000). Privacy and security at risk in the global information society. In D. Thomas & B. D. Loader (Eds.), *Cyber crime: Law enforcement, security, and surveillance in the information age* (pp. 173–192). New York: Routledge.
- Goodman, M. D., & Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *UCLA Journal of Law & Technology*, 3. Retrieved March 22, 2004, from [http://www.lawtechjournal.com/articles/2002/03\\_020625\\_goodmanbrenner.php](http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php)
- Grabosky, P., & Smith, R. (2001). Telecommunication fraud in the digital age. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 29–43). New York: Routledge.
- Gravell, W. (1999). Some observations along the road to “national information power.” *Duke Journal of Comparative & International Law*, 9, 401–426.

- Hinde, S. (2003). The law, cyber crime, risk assessment and cyber protection. *Computers and Security*, 22, 90–95.
- Hopkins, S. L. (2003). Cyber crime convention: A positive beginning to a long road ahead. *Journal of High Technology Law*, 2, 101–121.
- Huie, M. C., Larabee, S. F., & Hogan, S. D. (2002). The right to privacy in personal data: The EU prods the U.S. and controversy continues. *Tulsa Journal of Comparative & International Law*, 9, 391–469.
- Interpol's contribution to combating information technology crime. (n.d.). Retrieved January 23, 2004, from <http://www.interpol.int/Public/TechnologyCrime/default.asp>
- Jackson, M. (2000). Keeping secrets: International developments to protect undisclosed business information and trade secrets. In D. Thomas & B. D. Loader (Eds.), *Cyber crime: Law enforcement, security, and surveillance in the information age* (pp. 153–172). New York: Routledge.
- Katyal, N. K. (2003). Digital architecture as crime control. *Yale Law Journal*, 112, 2261–2289.
- Keyser, M. (2003). The Council of Europe convention on cyber crime. *Journal of Transnational Law & Policy*, 12, 287–326.
- Kennedy, D. C. (2002). In search of a balance between police power and privacy in the cyber crime treaty. *Richmond Journal of Law & Technology*, 9. Retrieved March 24, 2004, from <http://law.richmond.edu/jolt/v9i1/article3.html>
- Maher, M. K., & Thompson, J. M. (2002). Intellectual property crimes. *American Criminal Law Review*, 39, 763–816.
- Marler, S. L. (2002). The convention on cybercrime: Should the United States ratify? *New England Law Review*, 37, 183–219.
- Marx, G. T. (2001). Identity and anonymity: some conceptual distinctions and issues for research. In J. Caplan & J. Torpey (Eds.), *Documenting individual identity* (pp. 311–327). Princeton, NJ: Princeton University Press.
- Mayer-Schonberger, V. (2003). The shape of governance: Analyzing the world of Internet. *Virginia Journal of International Law Association*, 43, 605–673.
- McFarlane, J. (2001). Transnational crime, corruption, and crony capitalism in the twenty-first century. *Transnational Organized Crime*, 4, 1–30.
- Norman, P. (2001). Policing 'high-tech' crime within the global context: The role of transnational policy networks. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 184–194). New York: Routledge.
- Oddis, D. I. (2002). Combating child pornography on the Internet: The council of Europe's convention on cyber crime. *Temple International and Comparative Law Journal*, 16, 477–518.
- O'Neill, M. E. (2000). Old crimes in new bottles: Sanctioning cyber crime. *George Mason Law Review*, 9, 237–288.
- Pinkney, K. R. (2002). Putting blame where blame is due: Software manufacturer and customer liability for security-related software failure. *Albany Law Journal of Science & Technology*, 13, 43–82.
- Podgor, E. S. (2002). International computer fraud: a paradigm for limiting national jurisdiction. *U.C. Davis Law Review*, 35, 267–317.
- President's Working Group on Unlawful Conduct on the Internet. (2000). *The electronic frontier: the challenge of unlawful conduct involving the use of the Internet*. Washington, DC: U.S. Department of Justice.
- Raghavan, T. M. (2003). In fear of cyberterrorism: an analysis of the congressional response. *University of Illinois Journal of Law, Technology & Policy*, 2003, 297–312.
- Rauchs, G., & Koenig, D. J. (2001). Europol. In D. J. Koenig & D. K. Das (Eds.), *International police cooperation* (pp. 43–62). New York: Lexington.
- Rustad, M. L. (2001). Private enforcement of cyber crime on the electronic frontier. *Southern California Interdisciplinary Law Journal*, 11, 63–116.
- Schjolberg, S. (2003). *The legal framework: Unauthorized access to computer systems: Penal legislation in 44 countries*. Retrieved July 6, 2004, from <http://www.mosstingrett.no/info/legal.html>
- Sinrod, E. J., & Reilly, W. P. (2000). Cyber-crimes: A practical approach to the application of federal computer crime laws. *Santa Clara Computer and High Technology Law Journal*, 16, 177–232.
- Skibell, R. (2003). Cybercrimes & misdemeanors: A reevaluation of the computer fraud and abuse act. *Berkeley Technology Law Journal*, 18, 909–944.
- Speer, D. L. (2000). Redefining borders: The challenges of cyber crime. *Crime, Law and Social Change*, 34, 259–273.
- Sussman, M. A. (1999). The critical challenges from international high-tech and computer-related crime at the millennium. *Duke Journal of Comparative and International Law*, 9, 451–489.
- Tountas, S. W. (2003). Carnivore: Is the regulation of wireless technology a legally viable option to curtail the growth of cyber crime? *Washington University Journal of Law & Policy*, 11, 351–377.
- Ventura, H. E., Miller, J. M., & Deflem, M. (in press). Governmentality and the war on terror: FBI project Carnivore and the diffusion of disciplinary power. *Critical Criminology*.
- Wall, D. S. (2001a). Cybercrimes and the Internet. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 1–17). New York: Routledge.
- Wall, D. S. (2001b). Maintaining order and law on the Internet. In D. S. Wall (Ed.), *Crime and the Internet* (pp. 167–183). New York: Routledge.
- Weber, A. (2003). The Council of Europe's convention on cyber crime. *Berkeley Technology Law Journal*, 18, 425–446.
- Williams, W. P. (1999). The national cybercrime training partnership. *The Police Chief*. Retrieved July 6, 2004, from <http://www.wjin.net/Pubs/3417.htm>
- Wolf, J. B. (2000). War games meets the Internet: Chasing 21st century cybercriminals with old laws and little money. *American Journal of Criminal Law*, 28, 95–117.
- Young, S. M. (2003). Verdugo in cyberspace: boundaries of fourth amendment rights for foreign nationals in cybercrime cases. *Michigan Telecommunication and Technology Law Review*, 10, 139–174.