I-WAYS, Digest of Electronic Commerce Policy and Regulation 26 (2003) 137–141
IOS Press

In Focus

Legal Manual for Combating Cybercrime

1. Introduction

With nearly 200 countries connected to the Internet, cybercrime has become a global issue that requires the full participation and cooperation of the public and private sectors in all countries, including the developing countries around the globe. The American Bar Association (ABA) in an extensive 213 page manual published in 2003, has assessed national and international law and practice and found serious deficiencies to deter, detect, investigate, and prosecute cybercriminal activities. In the spirit of approaching cybercrime in a coordinated fashion, the ABA's International Crime Project prepared a major report, International Guide to Combating Cybercrime. The Guide is intended to address "glaring gaps in combating cybercrime to date are (1) inadequate international coordination and (2) woefully deficient legal frameworks and organizational capacity in developing countries". It is also to serve as a manual for developed and developing countries alike to help them (1) create effective cybercrime laws, (2) handle jurisdictional issues, (3) cooperate in international investigations, (4) develop acceptable practices for the search and seizure of electronic evidence, and (5) establish effective public/private sector interaction.

The objectives of the Guide, the ABA reiterates, are to "(1) help developing countries attract foreign direct investment and offshore technology operations, and bring the economic and social benefits of technology to their people; (2) promote international cooperation and coordination in combating cybercrime and encourage the establishment of public and private sector structures necessary to share resources and effectively deal with these issues; and (3) help government officials, industry, citizens, academia, and nongovernmental organizations understand their role in combating cybercrime". Inquiries and orders may be addressed to ABA Book Publishing, 750 North Lake Shore Drive, Chicago Illinois 60611 (www.ababooks.org) ISBN 1-59031-195-7. Following are extracts from the Guide.

2. Cybercrime Laws

Cybercrime laws, the ABA observes, deter cybercriminal activities and make these offenses punishable, but they vary in form as much as cybercrime itself. Industrialized nations have enacted laws protecting computer and communications systems and the data residing in and transiting these systems. Generally, these cybercrime laws apply to:

- Use of computers and the Internet for illegal purposes: viruses, hacking, unauthorized access.
- Crimes against communication systems.
- Crimes facilitated by the use of a computer.
- Wiretap, pen register, and trap-and-trace laws to protect privacy and facilitate investigations.

While some countries, such as the United States, have special provisions for unauthorized actions involving "protected computers" (computers or systems used by financial institutions or the government, or involved in interstate or foreign commerce), other countries do not make this distinction. In most developed countries, cybercrimes are considered criminal offenses and are punishable by prison terms and/or fines. In some instances, civil liability may also be attached.

Industrialized countries have also updated their criminal codes to ensure statutes can be applied by diligent law enforcement authorities and government prosecutors to traditional crimes committed in new ways through computers and the Internet. Nations at the forefront of retooling their criminal legal systems to combat cybercrime have supplemented these efforts with additional laws and policies promoting electronic authentication and the use of encryption and relaxing controls for import and export of encryption devices and software.

One of the challenges countries face is keeping their computer crime laws up to date. Cybercrime laws are constantly evolving with new technological capabili-

ISSN 1084-4678/03/$8.00

ties and criminal innovation to address new forms of computer crime, new types of criminals, and emerging concerns within the law enforcement community. Also, with improvements in information and communications technology (ICT) throughout the world, making computer crime a seemingly borderless crime, crimes by and against foreign computer systems have proliferated. Nations have responded to transborder cybercrime by modifying their criminal codes to allow for jurisdiction over, and prosecution of, individuals and organizations committing crimes from one country against computers located in another. Finally, as the global legal and regulatory framework develops for e-commerce and security issues, it is generally accepted that online conduct should be treated no differently than offline conduct. In other words, laws should be technologically neutral and based upon the act rather than the technology used to commit the act.

Developing countries are making headway. In seeking to demonstrate the integrity of their computing and information infrastructures and to respond to the accelerating concerns of industrialized nations as expressed through the Organization for Economic Cooperation and Development (OECD), the Financial Action Task Force (FATF), and the Bank for International Settlements (BIS), developing nations have increasingly adopted and improved their computer crime laws to emulate the laws of more-developed nations.

Modeling cybercrime laws after those put forth by multinational organizations and countries that are leaders in commerce is the correct approach. Developing countries should take a global perspective when creating a legal and regulatory framework regarding ICTs. They are encouraged to participate in United Nations (UN) activities in this regard, to join multinational organizations, and to become global players as these issues are discussed and debated and new global legal structures are formed. Countries in line for accession into the European Union (EU) should, of course, closely monitor EU developments in the cybercrime arena. Likewise, countries in the Asia-Pacific region should be mindful of directions from the Asia-Pacific Economic Cooperation (APEC) forum. The leading multinational organizations involved in the ICT legal arena are the UN, OECD, World Trade Organization (WTO), EU, CoE, and APEC. Although not a multinational entity, the United States is also influential regarding ICT legal/regulatory issues.

3. Jurisdiction

Jurisdictional issues present some of the greatest challenges to combating cybercrime. The Internet has made it possible for a cybercriminal to be physically located in one country, weave an attack through multiple countries and computers, and store the evidence of the crime on servers in yet another country. Victims may be all over the globe. While the Internet is borderless, the investigation and prosecution of electronic crimes is not; the borders of sovereign states and their legal systems must be recognized. One of the most complex jurisdictional issues occurs when substantive or procedural laws of the involved countries conflict.

The international community has developed longstanding methods for obtaining and providing legal assistance. The most common are the Letters Rogatory process and Mutual Legal Assistance Treaties (MLATs), often negotiated on a country-to-country basis. These processes are time-consuming and often contain limitations on what assistance may be obtained. Dual criminality requirements can be especially problematic. Where the goal is to prosecute an accused located abroad, there also needs to be a way to secure that person's extradition. Here, too, countries negotiate extradition treaties that govern how to make and respond to extradition requests. Many countries, however, will not extradite their own citizens. Although most of the jurisdictional issues raised in cybercrime cases are not new, the Internet complicates them and increasingly brings them to the forefront.

A number of international fora have attempted to address the jurisdictional challenges posed by cybercrime. The most extensive is the Council of Europe's Convention on Cybercrime (CoE Convention), which was opened for signature on November 8, 2001, and has been signed by 33 countries. The CoE Convention addresses many of these issues. It creates a minimum list of cybercrime offenses and attempts to harmonize the elements of those offenses, thereby reducing many conflict-of-law and dual-criminality issues. The CoE Convention requires signatories to establish criminal jurisdiction over offenses committed in their territory and to consult on investigations. When more than one signatory claims jurisdiction over an offense, they must consult to determine the most appropriate jurisdiction for prosecution. The CoE Convention makes all cybercrimes extraditable offenses and helps resolve extradition treaty conflicts between two signatory countries. The CoE Convention requires signatories to provide mutual assistance "to the widest extent possible" in the

collection and preservation of requested data, whether real-time or stored.

The G-8 has also taken steps to facilitate mutual assistance and resolve many of the jurisdictional issues associated with cybercrime. Likewise, the EU has launched several initiatives aimed at addressing these matters within the jurisdiction of its member states.

4. Law Enforcement

The rapid escalation of cybercrime has significantly affected law enforcement's ability to investigate and prosecute crimes. In addition to coping with the technological advances associated with cybercrime, law enforcement increasingly has to deal with the role of cyberevidence and ICTs in traditional crimes such as murder, rape, illegal drug sales, and child pornography. Cybercrimes present law enforcement with three main challenges:

- Technical challenges that are caused by (a) rapid changes in technology and the inability of law enforcement to stay current, and (b) technical shortcomings that impair finding and prosecuting cybercriminals.
- Legal challenges that are caused by procedural barriers or hurdles and the inability of legal frameworks around the globe to keep up with technological capabilities and the changing business environment.
- Operational challenges that are caused by (a) a lack of equipment, training, and adequate organizational structures, and (b) the need to work with great speed despite time zone, language, and cultural differences.

To address these challenges, governments must devote ongoing government attention and resources to training personnel in high-tech investigative and forensic techniques, establishing internal organizations, and actively participating on the international front. Combating cybercrime also calls for a new partnership between the public and private sectors to enable law enforcement to meet the challenges of high-tech crime. Such partnerships should be based on information sharing, cooperation, and joint work toward fostering global minimum standards.

The two overarching concerns common to all law enforcement agencies are time sensitivity and resource constraints. There is a grave risk that the ability to keep pace with cybercriminals will be outpaced by advancements in technology. Law enforcement's response must be swift, lest the criminals gain the upper hand. Existing resources must be spent wisely. A centralized, coordinated approach is needed when allocating resources to technical tools, training, onsite assistance, and research. The greatest impact is achieved when this is done through existing structures that have a broad reach and include most key stakeholders.

Ten critical priority needs that can be addressed at the national level to improve law enforcement's ability to combat cybercrime are:

- Increase public awareness of the incidence and impact of cybercrimes.
- Improve data collection, analysis, and reporting on cybercrimes.
- Establish uniform training and certification courses.
- Establish electronic crime task forces with regional or national capabilities.
- Bring legal frameworks up-to-date with technology and international laws.
- Create better cooperation with the high-tech industry.
- Establish a central repository and resource point for cybercrime materials.
- Improve senior management's understanding of cybercrime trends and needs.
- Obtain up-to-date investigative and forensic tools.
- Follow best practices when establishing electronic crime units

The US government's activities in cybercrime are considered a worthy model by many countries. Numerous multinational organizations are addressing cybercrime, with the CoE, G-8, and UN in leadership roles. The CoE Cybercrime Convention is the first multilateral treaty that addresses many of the legal and procedural barriers and hurdles confronted by law enforcement and prosecutors in dealing with cybercrimes. It requires signatories to cooperate and offer timely legal assistance in the collection and preservation of evidence and in the investigation and prosecution of electronic crimes. In the past two years, the EU has also launched a number of cybercrime initiatives that are certain to have a global impact. The EU is currently considering a draft proposal for a Council Framework Decision on attacks against information systems that would help facilitate cooperation with law enforcement and address many of the ten priority areas listed above.

Despite these efforts, however, international activities lack coordination, and law enforcement continues to face barriers and procedural delays caused by inad-

equacies in legal systems and the lack of a global, harmonized legal framework. Industrialized nations and donor organizations can advance this process by helping developing countries enact cybercrime laws, establish needed government entities, and provide critical training. The private sector can also help through assistance provided by the legal community, communication providers, private sector companies, and nongovernmental organizations (NGOs).

5. Search and Seizure

Absent consent or access to public communications, government interceptions of communications (and traffic data) and government seizures or compelled disclosures of data in the hands of businesses and individuals constitute an intrusion on personal privacy. Nearly every country in the world includes a right of privacy in its constitution or other basic law. These provisions normally include rights of inviolability of the home and secrecy of communications. The right to privacy is also widely recognized as a fundamental human right under various human rights instruments, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the American Convention on Human Rights. The provisions of the European Convention on Human Rights are binding on all 44 member states belonging to the Council of Europe. The CoE's Cybercrime Convention explicitly requires that searches and seizures be conducted pursuant to the principles set forth in the European Convention on Human Rights.

Under most legal systems, such search-and-seizure intrusions are permissible, but only in accordance with clear standards in the law, requiring justification and prior independent approval, often by a judge. Legal standards limiting the circumstances and procedures for interception, search, and seizure are evolving, but governments and international human rights bodies are paying increasing attention to the procedures.

Varying legal frameworks around the globe significantly complicate the search and seizure of electronic evidence. Distinctions are made between real-time interceptions and digitally stored evidence. For real-time interceptions, the laws in several countries distinguish between the interception of the content of communications and the interception of only the transactional data, or traffic data, that indicates the origin and destination of communications. Under almost all legal systems, the interception of communications is considered a privacy intrusion of the highest order, requiring strict legal protections.

Stored digital evidence can be obtained through immediate access to stored data by entry into a home or office. Under most legal systems, this is considered a serious intrusion on privacy and requires prior legal approval, often by a judicial officer upon a showing by investigators of need and justification. Disclosure of stored data can also be compelled via a subpoena. These disclosures also intrude upon privacy interests and usually require some form of independent approval and oversight.

Law enforcement officials will increasingly be collecting electronic evidence, not only in cybercrime cases, but also in investigations of other kinds of crime that are facilitated by computers or involve electronic communications. This will require attention to both the practical and legal issues involved in accessing communications and stored data. Developing nations seeking to update their criminal laws for the digital age should address the procedural standards for government access to communications and computer data, while balancing the protection of public safety with protection of privacy and civil liberties. They will also need to ensure that their investigators are adequately trained in the practical considerations surrounding the acquisition and analysis of digital evidence. The emerging body of international experience provides useful guidance and suitable models for both the legal and practical aspects of the search and seizure of digital evidence.

6. Public/Private Cooperation

The security of networks and computers is part of the academic discipline of computer science, and the lack of security of networks and host computers is an important issue for everyone who uses the Internet. Security breaches, therefore, cannot be handled only by governments and law enforcement. The nature of cybercrime requires close cooperation between the public and private sectors. Electronic crimes can be committed by disgruntled or former employees, hackers and "script kiddies," organized crime, domestic and foreign competitors, terrorists, and other nation states. The networks and systems under attack or used in cybercrimes are often operated by private companies. Whether and how a company responds to these attacks often involves a delicate evaluative balance among the potential financial losses or damage caused and the risks (legal, reg-

ulatory, and to business reputation) involved in reporting or failing to report such attacks, including potential lawsuits and/or third party liability.

Public/private cooperation on cyberattacks and cybercriminal activities is important and helps each side better understand how to respond to cybercrime and mitigate its impact. This necessarily involves information sharing, which can mean different things to different people. For some, it is a way to develop or enhance information security ideas cooperatively, collaborate on joint responses, or share resources for detecting, preventing, and responding to security breaches and criminal activities. For others, it can mean divulging competitively sensitive information or proprietary data, essentially giving the government – and potentially their competition – the "keys to their kingdom". Some security researchers and professionals believe that information about security vulnerabilities, whether in networks or in host computers, should not merely be shared within industry or with government, but with academia and the general public as well. In whatever form information sharing takes, trust forms the critical element that facilitates the public/private cooperation necessary for the effective prevention and prosecution of cybercrime.

Neither government nor the private sector can address these problems standing alone. Governments cannot solve the complex and multilayered problem of cybersecurity and critical infrastructure protection without the assistance of private organizations. The government needs a cooperative relationship with the private sector because, in most instances, the government does not own, control, or operate the networks that underpin most critical sectors. The private sector needs the government because, no matter how large the corporation, it cannot by itself defend against attacks from terrorists or economic espionage from nation states. Moreover, the core of any nation state's economy, national security, and public safety is dependent upon the reliability, integrity, and availability of its critical infrastructures: electric power grids, railroad and airlines, oil and gas, banking and financial systems, and communications networks. Each of these is dependent upon ICTs and the global, interconnected network.

The legal frameworks of countries often discourage information sharing because they do not provide adequate protections from disclosure of shared information under freedom of information, antitrust, and privacy laws and other potential liabilities related to disclosure of the information. Information sharing and analysis centers (ISACs), which have been voluntarily formed by private sector members, have been cited around the world as models for cooperation and information sharing between the public and private sectors. The common benefits to ISAC members are early notification of potential cyberrisks; access to relevant information; industry-wide vigilance; increased subject-matter expertise; and access to trending, metrics, and benchmark data.

Information sharing can be facilitated by public sector initiatives that (a) establish centers for sharing information on an anonymous basis or serve as an intermediary where the direct sharing of information among industry is difficult, (b) create a central alert point for technical information and assistance regarding security risks and fixes, and (c) organize a public/private group comprised of all stakeholders (industry, government, academia, NGOs) to begin a dialogue on ICT security risks and develop ways to work together. Activities by private sector entities, such as the insurance, auditing, and high-tech industry sectors, can also advance information sharing and increase information and infrastructure security.