I-WAYS, Digest of Electronic Commerce Policy and Regulation 26 (2003) 117–123
IOS Press

In Focus

Cybercrime Laws, Prevention and Enforcement Capacity Builds

1. Introduction

The recurrent theme of national and international cybercrime initiatives, ranging from the United Nations and the Council of Europe, to the 21 Member Economies of the Asia-Pacific Economic Cooperation (APEC) is combating significant incidents of malicious attacks on confidentiality, integrity and availability of computer data and systems. This worldwide consensus of the real threats to the underpinning technologies driving information societies is impressive at a time when global unity seems to be lacking in many other policy areas. This In-Focus section contains highlights from a number of documents and laws with major attention directed to programs of APEC on cybercrime and information security in the Asia-Pacific region.

The United National General Assembly took an early initiative to call for Member States to become aware and prepare necessary legal and administrative procedures to prevent or prosecute cybercrime. Resolution (55/63) on Combating the Criminal Misuse of Information technologies, adopted on January 22, 2001, calls on national governments to respond by adopting the following 10 preventive measures:

1. States should ensure that their laws and practices eliminate safe havens for those who criminally misuse information technologies;
2. Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;
3. Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;
4. Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;
5. Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;
6. Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;
7. Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;
8. The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;
9. To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence;
10. The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of governments to fight such criminal misuse.

To further the objectives of the APEC Action Plan on Cybercrime and Information Security (see I-Ways, Vol. 25 2nd Qtr), the e-Security Task Group sponsored a Conference of Cybercrime Experts and Training Seminar in Bangkok, on July 21–25, 2003. Attended by over 120 delegates from 17 economies, the conference was organized by the US Department of Justice and hosted by the National Electronics and Computer Technology Center (NECTEC) and Ministry of Information and

ISSN 1084-4678/03/$8.00 © 2003 – IOS Press. All rights reserved

Communications Technology, Thailand. Conference Chair, Richard W. Downing Deputy Chair of the eSecurity Group presented an overview of APEC's work on Cybercrime and Cybersecurity and Relevant Work of Other Multilateral Forums.

The conference had three primary goals were targeted: (1) assisting economies to develop legal frameworks necessary to combat computer crime; (2) promoting the development of law enforcement investigative units with training and equipment needed to investigate and deter computer crime; and (3) enhancing understanding and cooperation between industry and law enforcement in order to better address the threat of computer crime. Several experts from across the region made presentations and there was an active exchanges of views among participants. The following is an edited summary of the discussions.

2. Developing a Comprehensive Cybercrime Law

2.1. Strategies for Developing and Amending Laws

Models for legislative drafting. The Council of Europe (COE) Convention on Cybercrime provides a model of the types of conduct that should be prohibited, the types of procedural authorities that law enforcement should have, and the types of mechanisms for international cooperation needed to improve investigation and prosecution of cybercrime. Moreover, because it was developed by countries with widely varying legal systems, it does not dictate the manner in which an economy should carry out its provisions. Instead, it identifies the capabilities that economies should have without suggesting the method or language by which those capabilities should be implemented in domestic law. Due to this format, the Cybercrime Convention can be applied to any legal system.

There was broad agreement among the experts that the Cybercrime Convention provides a valuable model for APEC economies seeking to develop comprehensive legal frameworks to combat cybercrime. Many economies, such as Chinese Taipei, the Philippines, and Hong Kong, China used it as the basis by which to propose legislative amendments, while others, such as Australia and New Zealand, used it as a standard by which to evaluate the completeness of their laws. Moreover, as Japan, Canada, and the United States have already signed the Cybercrime Convention, it will serve as the norm by which their laws will be evaluated (the Cybercrime Convention will later be opened for other economies to sign).

Other models for legislative drafting also were considered. Some economies, such as Malaysia, used the domestic law of the United Kingdom as a model. Unfortunately, as the United Kingdom enacted its law in 1990 before the global spread of the Internet, one expert stated that it did not provide complete coverage of the various computer crimes that have developed in the succeeding years.

Process for the development of laws. The experts examined various methods economies have used to develop laws and legislative amendments. Some economies, such as Japan, surveyed industry, academia, and Internet Service Providers, published reports, and solicited public comment. Others, such as Chinese Taipei, created a committee of judges, prosecutors, and security experts to develop a draft law. Still others, such as Canada, sought the advice of cybercrime legal experts from other countries.

In addition, economies differed on the question of whether to create a single law that would introduce sweeping changes or to make incremental changes to pre-existing law. For example, in 1997 Chinese Taipei first made limited amendments to its traditional law, such as by making "electronic records" count as records for purposes of the pre-existing forgery, theft, and vandalism statutes. Unsatisfied with these changes, however, Chinese Taipei passed a new law in 2003 to assure that the law penalized all sorts of criminal conduct, such as unauthorized access to computers and the release of computer viruses.

It was made clear that no one process is right for every economy. Lawmakers must evaluate their economy's political, social, and economic milieu to determine the most appropriate strategy. As a Canadian expert pointed out, prudent law makers should consider public and private interests and human rights concerns, research the criminal behavior, consult special interest groups, assess the political environment, and take into consideration the prevailing legal regime.

2.2. Substantive Laws

Unauthorized access to a computer. Several participants commented on the need for comprehensive laws to criminalize various types of harmful conduct. A comprehensive law should include, for example, a prohibition on unauthorized access to a computer. Although some economies prohibit such conduct only when the unauthorized access to the computer seeks to

obtain access to information stored on the computer, the United States pointed out the value of prohibiting the unauthorized access to the computer alone. For example, a criminal can access a computer and cause harms other than obtaining restricted data, such as by installing programs capable of causing a "denial of service attack" (a type of computer attack whereby the victim computer is flooded with unwanted data, preventing it from functioning in its normal way).

Moreover, the experts differed on the value of limiting the scope of the criminal prohibition on unauthorized access only to those acts which circumvent an access control system (such as a password). Some experts suggested that limiting the scope in this way assures that only those with criminal intent to access a non-public computer system will be punished. Other experts suggested, however, that criminal intent can be proved in other ways, and that laws should be flexible enough to punish criminals who knowingly violate the integrity of a victim computer even if the victim has failed to employ security features like password protection.

Damage to computer systems. Participants discussed options for criminalizing conduct that causes computers to crash or modifies or deletes computer data, as well as conduct that makes computers or electronic data unavailable to the authorized users. There was broad agreement that a comprehensive law must cover these sorts of harms.

Unauthorized interception of communications. The need for a law criminalizing the unauthorized interception of others' electronic communications was stressed. Some economies, such as Canada, had long-standing laws that prohibit the interception of communications generally (such as telephone communications), and these laws apply directly to communications carried by computers. Economies should consider how such a prohibition would apply in certain circumstances, however. For example, Canada encountered a difficulty with the application of this law to those computer owners who employ "intrusion detection systems", i.e., software or hardware devices that often intercept communications into and out of a computer network in order to detect unauthorized use. Canada chose to amend its law to assure that developing technologies used to improve computer security do not run afoul of existing criminal laws. In addition, some economies' legislation relating to interception only covers communications using a telecommunications carrier or service provider. The experts discussed problems that have developed with this approach and whether this sort of legislation would apply to new communications media such as wireless networks not operated by traditional carriers.

Production and distribution of devices used to violate the above substantive laws. The need for laws that criminalize the production or distribution of devices, such as software programs, that can be used to damage computers or intercept communications are considered highly needed. Examples of such devices include a virus that damages computer systems and a program that, once installed on a computer network, surreptitiously intercepts email. Certain of these devices, however, have legitimate applications. For example, security professionals often use these devices in order to test the security of computer networks. Also discussed are the ways in which laws can be drafted to allow such legitimate activities. Canada, for example, requires that the production or distribution of the device be "for the purpose of committing a crime". Japan, on the other hand, suggested that laws could include an exception to the criminal prohibition where the device is employed in legitimate security research.

2.3. Procedural Laws

Interception of electronic communications. Key elements of a comprehensive procedural law needed to combat cybercrime were reviewed. One element of such a law is the ability to intercept the electronic communications of criminals. Economies have taken different approaches to such laws and provided different safeguards against abuse by law enforcement authorities. For example, Canada's law includes the requirements that the law enforcement investigators present a significant level of proof to an independent judge, and that the investigators have tried all other options or can show that they are unlikely to succeed (that the court order is a "last resort"). Other economies, such as Malaysia, authorize their police forces to intercept communications only with the approval of a prosecutor. Moreover, New Zealand took an approach that is "neutral" with respect to technology by applying the exact same rules and safeguards to the authority to intercept electronic communications as the ones it already had in place for the authority to intercept voice communications. It appears clear that the exact nature of the restrictions on the use of interception authority may vary based on the economy's legal system, its history of police powers, its political environment, and the perceived scope and nature of its cybercrime problem.

"Real-time" collection of traffic data. The need for a separate law that allows law enforcement authorities to collect, in "real time", the non-content data associated with electronic communications (sometimes called "traffic data") is considered highly desirable. This authority, for example, would allow a law enforcement official to collect the source and destination of a communication while the communication is still occurring.

The United States emphasized the importance of this sort of legal provision based on its experience in conducting investigations involving the Internet. Although it found that communications can sometimes be traced using stored logging data, it stated that sometimes the only way to identify the criminal was to obtain the source of a communication while it was still occurring.

Economies have implemented this type of provision in varying ways. Some, such as the United States, require a court order (albeit with many fewer restrictions than interception the content of communications); others, such as Australia, allow law enforcement authorities to formally require providers to collect this sort of information without a court order. Still other economies, such as Canada, are in the process of implementing a law that would allow this sort of evidence collection.

Obtaining data from providers. The experts discussed the need for a method of obtaining stored electronic data – both content and non-content information – from providers. Although every economy's law had some method for law enforcement to compel providers to disclose such evidence, the actual implementation of such authorities varied considerably.

Some economies, such as the United States and Australia, have laws that explicitly provide for this kind of evidence collection. Such laws often draw distinctions between the disclosure of the content of communications and the disclosure of the non-content data related to such communications. For example, United States law allows law enforcement to compel the disclosure of non-content information using a "subpoena" (with relatively little prior justification), whereas it requires a search warrant similar to that used to search a home or business to obtain undelivered email messages. Similarly, Australian law allows police officers to formally request traffic information, but they must obtain a court order to compel the disclosure of the content of communications.

Other economies do not have laws that apply specifically to data held by providers but instead employ more traditional "search and seizure" authorities to this situation. For example, under current Philippine law, providers are *permitted* to disclose stored data based upon the request of a police officer, but if the provider refuses, the officer must obtain a traditional search warrant. Japanese law enforcement authorities use a similar strategy to obtain such evidence. The need to collect data from third parties other than traditional service providers, for example from universities and businesses, was also discussed.

Other problems law enforcement authorities face – other than legal ones – in obtaining such data also were described. Law enforcement authorities in Chinese Taipei, for example, have to pay large sums of money to reimburse providers for the disclosure of data. In the United States, providers are entitled to "reasonable costs", which in practice are not exorbitant. Most other economies reported that they do not pay anything for such disclosures.

Preserving data. Laws that enable law enforcement authorities to preserve specific data – such as communication log files or the content of emails – associated with a particular criminal investigation are considered necessary. This authority does not include the disclosure of such information, but it can freeze evidence while investigators obtain the appropriate legal process, such as a court order. While the experts acknowledged the need for a preservation authority, economies take different approaches to effectuating it.

Certain economies, such as Australia and the United States, have legal provisions that allow law enforcement to request preservation without judicial oversight. Others, such as Indonesia and Japan, have less formal relationships between law enforcement and providers that allow law enforcement to request data preservation.

Experts also discussed the need for providers to keep such requests for the preservation or disclosure of records confidential and not notify the customer about the law enforcement investigation. Economies take various approaches to this question. For example, Chinese Taipei's law allows law enforcement to command providers not to disclose the fact that law enforcement has made a request; the United States has a law that precludes providers from notifying its customers, but only following a court order; and Japanese law allows for criminal prosecution of providers if they interfere with a criminal investigation by notifying a customer.

Identifying criminals who access the Internet anonymously. It was acknowledged that by accessing the Internet anonymously – for example using a cybercafe that does not check the identity of its customers – criminals can make it much more difficult for law enforcement to identify and punish them. Some economies

have tried to address this problem by enacting laws that require those who obtain Internet accounts to provide identification. Others, including the Philippines, are considering such legislation.

2.4. Laws and Policies that Allow for International Cooperation

A repeated theme, reiterated by many experts, is the need for international cooperation to address the threat of cybercrime. For example, China emphasized that responding to "denial of service" attacks requires cooperation between economies, and that the only effective way to address such an attack is to cooperate quite quickly. The ability for law enforcement to cooperate in trans-border investigations, however, requires certain legal authorities.

Such legal authorities include the ability for law enforcement to assist foreign investigations, even where the crime does not occur (or the victim is not located) within the economy's borders. If an economy does not have this power to investigate, criminals can route their communications through that economy, and the international investigation to discover the source of the attack will reach a dead end.

Similarly, criminals often choose to commit crimes against victims located solely in other economies. Unless each economy has the ability to prosecute such domestic offenders or extradite them to the economy where the victims reside, that economy can provide a safe-haven for the criminal activity. To address this problem, economies such as Malaysia and the United States have laws that allow them to prosecute domestic offenders for harm caused to foreign victims.

Finally, experts discussed ways for economies to improve the speed with which international cooperation occurs. One option that was raised is to identify points of contact that can assist in international investigations. The Group of Eight has developed a network of such points of contact. This network began in 1997 with eight countries, but now includes 33 countries around the globe including most of the APEC economies. One expert also suggested that the development of "mutual legal assistance treaties" between economies would ease the burdens of international law enforcement cooperation.

3. Developing Investigative Units Capable of Cooperating Internationally

3.1. Funding and Structuring Units

The participants recognized that in order to enforce cybercrime laws, economies must have investigators capable of detecting and investigating computer related violations. In implementing a cybercrime unit, it was agreed that it is important to dedicate the unit solely to investigating crime on computer networks and collecting and analyzing electronic evidence. Investigators in such a unit must have adequate equipment and training in order to do their jobs. Moreover, because of rapid changes in technology, equipment must be updated regularly and investigators must constantly receive updated training.

It was emphasized two capabilities that cybercrime investigative agencies should possess. First, each agency should have the ability to investigate crimes occurring on computer networks. Second, each agency should have the forensic capability to analyze seized electronic evidence. Some economies, such as the Philippines use a single unit to exercise both functions, while others such as Hong Kong separate these functions into different units.

Funding. One of the most significant problems economies face in developing a cybercrime investigative unit is how to assure adequate funding. Economies have developed differing models on how to address this problem. The United States, Japan, and Canada, for example, employ some form of a "task force" model, in which resources from several law enforcement agencies are pooled together. In this way the funding burden can be shared, creating a more viable cybercrime unit.

For example, the United States developed a "Regional Computer Forensic Laboratory" in 1998 that was comprised of thirteen federal, state, and local law enforcement agencies in the area around San Diego, California. The unit proved successful with only limited funding because it drew personnel, equipment, training, and funding from the various agencies involved.

Alternatively, many economies develop a cybercrime investigative capacity at the national level and use that capacity to assist investigators at the regional or local level who have fewer resources and experience. Malaysia, the Philippines, Japan, and Canada, have law enforcement institutions at the national level that serve this function. The experts agreed that providing adequate funding requires the sustained commitment of resources on an ongoing basis.

Hiring and personnel retention. Participants discussed hiring policies and some of the difficulties faced in retaining qualified investigators. Some economies, such as Hong Kong, China, choose to hire cybercrime investigators only from within the police force and then provide them with training in computer technology. Others, such as the United States, at times seek to hire individuals who already have computer expertise and then provide them with training in investigative skills.

Problems commonly encountered involved retaining qualified personnel. Japan and Hong Kong, China, for example, have strict policies of rotating police employees to different assignments, thereby routinely transferring their cybercrime expertise to other jobs. Other economies, such as the Philippines and the United States have experienced the problem that trained investigators often leave the police force to enter the private sector as security consultants where they can make more money. Administrators for cybercrime units have sought ways to limit the rotation of their experienced investigators and to provide both monetary and non-monetary incentives for investigators to continue working at the law enforcement agency.

Working with prosecutors. The value of having investigators work with prosecutors in pursuing a cybercrime investigation was discussed. Hong Kong, China, for example, supported this idea, and the United States stated that American prosecutors have played a valuable role in such investigations by focusing on the evidence required to be successful at trial. Other economies, however, such as Thailand, have legal systems that do not allow prosecutors to become involved in investigations.

3.2. Training Investigators

The need for proper training for cybercrime investigators was stressed. It was agreed that obtaining adequate training is a significant hurdle for the development of cybercrime units. Since training must occur repeatedly to keep up with technology (the United States recommended four weeks of training per year), it involves a significant resource commitment that raises many of the same budgetary issues summarized in the preceding section.

Economies have taken a variety of approaches to training investigators. Some economies, such as Hong Kong, China, have focused their training on independent academic institutions. Hong Kong investigators generally obtain a professional diploma following six months of study at the Hong Kong University of Science and Technology.

Others, such as Japan and Canada, have developed courses at their national police colleges. Such programs have certain advantages, such as lower cost and greater control over the curriculum. But these economies, as well as the United States, have also relied on outside experts to develop courses and supply training. Still others have utilized their relationships with Computer Emergency Response Teams ("CERTs") or foreign law enforcement agencies to provide training for investigators.

In addition, Canada developed an innovative program to promote on-the-job training. Each new investigator is paired with a "mentor" for a period of two years. Mentors assist the less experienced investigators and assure that they gain experience in a variety of different skills and procedures.

4. Industry and Law Enforcement Cooperation

Both government and the private sector experts discussed the roles of law enforcement and industry, and they explored ways in which better cooperation can help to combat cybercrime. For example, reporting of security breaches and instances of computer crime is critical to law enforcement's ability to address the problem. Industry can also assist law enforcement by providing technical knowledge and expertise.

Each of these forms of assistance depend on trust between industry and law enforcement. Law enforcement can promote trust (and thereby create an environment conducive for reporting of cybercrime) by:

- establishing relationships and lines of communication before an attack takes place;
- maintaining the confidentiality of information provided by industry to the greatest extent possible;
- being sensitive to business needs, such as the need to continue to conduct business and to have input into the way in which information is disclosed to stockholders and the public.

Trust and information flows can also be enhanced by the establishment of technical exchange forums and programs, such as "InfraGard" in the United States, that bring together law enforcement and industry to exchange information on security issues. CERTs can also provide a vehicle for opening lines of communication between industry and law enforcement by encouraging industry to report serious incidents to law enforcement,

Council of Europe Cybercrime Convention Strengthens National Legal Systems

Responding to the challenge of Cybercrime, the Council of Europe (CoE) adopted a Convention on Cybercrime on November 23, 2001. This action was taken because "cybercrime and cyber-terrorism represent a serious challenge to society as a whole and this is the first coordinated and international response," CoE leaders announced in Budapest as the Convention was opened for signature. Participating in the preparation of the Convention were 26 member States of the CoE and four non-members, Japan, Canada, South Africa and the United States. This binding treaty has been opened for signature by other non-member States. It came into force after being ratified by 5 States.
The treaty has a threefold aim: to lay down common definitions of certain criminal offenses relating to the use of the new technologies, to define methods for criminal investigations and prosecution, and to define methods for international communication. The criminal offenses are:

– Those committed against the confidentiality, integrity and availability of computer data or systems (such as the spreading of viruses);
– Computer-related offenses (such as virtual fraud and forgery);
– Content-related offenses (such as the possession and intentional distribution of child pornography; and
– Offenses related to infringements of intellectual property and related rights.

Another objective is to facilitate the conduct of criminal investigations in cyberspace, thanks to a number of procedural powers, such as the power to preserve data, to search and seize, and collect traffic data and to intercept communications.
It was announced at the signing ceremony that the Convention would evolve and would soon have protocols added to enable it to be adapted to new challenges arising in the international context. An example suggested was to criminalize terrorist messages sent via the Internet and their decoding. A new committee of experts has been set up to prepare, within a year, a draft protocol to be added to the Convention which will make racist and xenophobic propaganda via computer networks an offense.
During the preparatory stage of the Convention, concerns were expressed as to whether government authorities, the police in particular, in newly democratic States, could effectively balance the pursuit of cybercrime with individual rights. Drafters of the Convention addressed such concerns in the Preamble with the following: "Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 UN International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy".

providing law enforcement contacts to industry, and acting as a liaison or coordinator between law enforcement and industry.

Obtaining evidence from providers. Procedural laws provide law enforcement with the authority to access information collected or stored by third parties. These laws may create burdens on industry, however, such as expenses incurred in storing and producing data and potential conflicts with customer privacy rights. In order to establish a cooperative working environment, Internet Service Providers and law enforcement agencies should collaborate and develop effective measures to reduce industry compliance costs. An example was the Australian Internet Industry Association's code of conduct that was negotiated between law enforcement and industry. In addition, companies should be aware of the need to create a global legal compliance policy for responding to law enforcement requests from other economies, especially where the company has operations in more than one economy. Such a policy should be consistent with applicable law and implemented globally while recognizing differences among jurisdictions.

5. Conclusion

Over the course of the week, experts exchanged a tremendous amount of information about their experiences, laws, and practices in fighting cybercrime. In addition, the conference served as an important basis from which to continue APEC work. First, it served as an important foundation for the second phase of the Cybercrime Legislation and Enforcement Capacity Building Project. It publicized the opportunities for follow-on training, developed ideas for the form that such training might take, and energized economies to make use of the training opportunities. Second, the delegates to the conference universally praised the conference as a valuable opportunity to exchange views and to promote better cooperation in fighting cybercrime. The delegates called for more meetings of the group in order to continue to further these important goals.