UNCTAD/SDTE/ECB/2005/1

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT
Geneva

INFORMATION ECONOMY REPORT 2005

CHAPTER 6

UNITED NATIONS
New York and Geneva, 2005

Chapter 6

PROTECTING THE INFORMATION SOCIETY: ADDRESSING THE PHENOMENON OF CYBERCRIME

A. Introduction

As developing countries embrace, exploit and integrate computer and communications systems at an economic and social level, concerns arise about the vulnerability of such systems to deliberate attack. An attack may target the data being processed by systems, or the integrity, confidentiality and availability of the systems themselves. Most users, for example, will have experienced and suffered from viruses infecting and corrupting their data and the operation of their systems. However, where such attacks are targeted at, or inadvertently impact on, a country's critical national infrastructure, such as power systems or transportation networks, the consequences may be significant and cause substantial damage.

Protecting systems from attacks via the Internet obviously relies primarily on the implementation of appropriate technical, physical and operational security measures. It must therefore be the concern of policymakers that users, whether public sector or private sector, implement such security measures to protect their data and systems. However, a parallel requirement for appropriate security is the establishment of a legal framework that deters such attacks by criminalizing the different forms of activities being carried out against systems and enabling law enforcement agencies to adequately investigate and prosecute such activities.

This chapter examines why countries, and in particular developing countries, need to address the threat of cybercrime and what measures need to be taken to ensure that an adequate legal framework is put in place. In the first section, the phenomenon of cybercrime will be examined in its many manifestations, together with its prevalence and economic cost, particularly for developing nations. In the second section, consideration will be given to the appropriate criminalization of particular types of acts.

Cybercrime can generally be classified into three broad categories: computer-related, content-related and computer integrity offences. Each category raises unique issues, and addressing all forms of cybercrime will generally require amendment of the current criminal code, as well as the adoption of *sui generis* offences.

However, reforming the criminal code is only one step towards the effective legal treatment of cybercrime. Law enforcement agencies also require the necessary powers, expertise and resources to be able to tackle instances of cybercrime. The third section of this chapter will examine what procedural law reforms are needed to adequately equip law enforcement agencies to investigate cybercrime.

Cybercrime is often international in nature, occurring across boundaries and impacting on users in different countries. Developing countries will obviously be both victims and the source of cybercrime. As noted at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, in April 2005, developing countries "have become staging grounds for attacks by cyber criminals" on developed countries, due to the greater prevalence of unprotected systems.[1] To address this interrelated vulnerability, greater harmonization evolves between jurisdictions in order to be able to effectively prevent criminal activities, as well as pursue perpetrators. In recent years, there have been a number of initiatives at the intergovernmental level, including the United Nations, the Council of Europe, the G8 and the Commonwealth. These will be used as a benchmark to consider the needs of developing countries.

While examining the threat of cybercrime and suggesting means of combating it, the chapter will keep its focus on issues addressed in the recommendations of United Nations General Assembly Resolution 55/63 (see excerpts from the resolution in box 6.1).

Box 6.1

United Nations General Assembly Resolution 55/63, Combating the criminal misuse of information technologies

(January 2001)

"... notes the value of, inter alia, the following measures to combat such misuse:

(a) States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

(b) Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

(c) Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

(d) Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies;

(e) Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

(f) Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

(g) 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;

(h) The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;

(i) To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence;

(j) 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;"

B. Addressing the phenomenon

As Gibson's notional "Internet"[2] has materialized as the "network of networks" that constitutes the Internet and the communication and content services made available over it, so there has been an inevitable growth in the criminality associated with this environment. The Internet spawns cybercrime: "Since crime tends to follow opportunity and the Internet provides many new opportunities, then new crimes will certainly emerge".[3]

There is no agreed definition of what constitutes computer crime or cybercrime. The computer may constitute the instrument of the crime, as in murder or fraud; the object of the crime, as in the theft of processor chips; or the subject of the crime, as in hacking and distributing viruses. The latter could be defined narrowly to refer to those activities that are unique to the Internet, such as "hacking" and distributing viruses. However, the impact of computers on criminal law has been much more substantial than this narrow field of activities, both challenging traditional criminal concepts, and facilitating particular types of crime, such as child pornography. In addition, criminal law is not just about whether a particular act should be considered criminal or not. It is also about law enforcement, investigating those that commit criminal acts and prosecuting them, a process often considerably more difficult in a computer environment. This chapter therefore adopts a broad approach to the topic, focusing on crimes involving interconnected computers, which use in whole or part the Internet as a communications platform.

For the purpose of this report, the boundaries of what is considered cybercrime and the categorization used to distinguish between different types of cybercrime are those adopted in the primary international legal instrument in this area, the Council of Europe's Convention on Cybercrime (2001).[4] In the Convention, substantive offences are classified into three

categories. The first category is traditional types of criminal offence that may be committed using computers as the instrument of the crime, referred to as computer-related crime, such as fraud. The second category concerns content-related crimes, primarily involving, for example, the violation of copyright or trademark. These first two categories could perhaps be more accurately described as "information crimes", since the object of the crime is the information processed by computers, whether accounting data or a music file, rather than the computer itself.[5] The third category is offences that have been established to specifically address activities that attack the integrity of computer and communications systems, such as distributing computer viruses. However, it could be argued that the public policy rationale underpinning this category is also the protection of the information being processed rather than of computers and systems for their own sake.

While this tripartite categorization will inform our discussion, it should also be recognized that the adoption and dispersion of Internet technologies are not uniform, particularly between developed and developing nations. Wireless communication technologies, for example, have rapidly eclipsed wireline systems in many developing countries, where the legacy fixed infrastructure was greatly underdeveloped. Thus, it should be recognized that differential technological use may mean different patterns of threats and vulnerabilities in terms of cybercrime.[6]

1. The incidence and cost of cybercrime

While this report is concerned with how legal systems need to evolve to address the phenomenon of computer crime, a preliminary question is why they need to evolve. What is the scale of the problem? Public policy agendas generally respond to a need articulated through one or more channels, such as the media or business. Such needs generally emerge from the experience of victims of cybercrime, often coupled with a real or perceived sense of inadequate protection by the law and the agencies responsible for its enforcement. Therefore, how great is the threat of cybercrime?

Reliable statistics about the scale of crime are notoriously difficult to measure,[7] and cybercrime presents particular challenges. A lack of consensus about what constitutes cybercrime is clearly one obstacle to the collection of data. Such a paucity of empirical data concerning computer crime is generally seen as being due to a range of factors:

- *Under-reporting*

  There is a lack of reporting by victims, since commercial organizations avoid adverse publicity in order to protect their reputation and share price.[8] One approach to addressing this problem has been to impose a legal obligation to report incidents. Since 2003, for example, the State of California has obliged public businesses and government agencies to report if a hacker has gained access to personal information and financial data.[9]

- *Law enforcement experience and resources*

  A lack of experience and resources among law enforcement and prosecuting authorities has often meant that investigations and prosecutions are not considered a priority area, particularly when competing for attention with other public concerns, such as violent crime. This will often be exacerbated by inadequate training of personnel. This second factor obviously contributes to the first, under-reporting, since where victims perceive that they will receive a poor response from law enforcement agencies, they will be less likely to make the effort to report.

- *International nature*

  A third factor is the transnational nature of computer crime and the associated jurisdictional problems that contribute to the complexity of investigating and prosecuting offenders. All law enforcement agencies are under to pressure to perform, either expressly or implicitly, and are short of resources. Tackling international crime is resource-intensive, but there are low clear-up rates, namely successful prosecutions.

- *Statistical recording*

  Law enforcement agencies often fail to specifically collate data in relation to computer crime. This may be due to a lack of resources, but is more likely due to the complexities of recording such events.

- *Forensic and evidential challenges*

  Computers, particularly when networked, create significant forensic challenges to law enforcement agencies when obtaining evidence and subsequently presenting it to the courts.

Where figures are published, they are often from commercial entities operating in the data security sector, which clearly have an incentive to overstate the problem, and extrapolate the economic costs of computer crime on the basis of scant real data.[10]

The absence of reliable empirical data to support the frequent public claims made about the growth and impact of computer crime creates problems for policymakers. On the one hand, adopting legislative measures against a phenomenon that is little known may easily result in an inappropriate set of rules, either failing to adequately address the mischief or overextending criminal law to activities that should not be criminalized. On the other hand, the basis for taking any measures at all is weak, and therefore potentially flawed; this undermines the rationale for public policymakers to act and again leads to the overextension of criminal law.

Although the true figures concerning cybercrime may be suspect, certain common characteristics do emerge from the data available, and these provide important insights to help guide policymakers. First, a significant proportion, if not the majority, of cybercrime, is committed by, or with the assistance of, persons within the victim organization, such as employees. A survey from India, for example, reported that two thirds of data theft incidents were attributable to employees (current or former), while the majority of acts of unauthorized access originated within the affected company.[11] Such insider-instigated crime may mean that policymakers see primary responsibility as resting with the victim organizations themselves, rather than Governments. In addition, civil proceedings under employment law may be seen as providing for alternative legal redress against the perpetrators. Second, while cybercrime is most popularly associated with acts of hacking and viruses, its most prevalent form would seem to be computer-related crimes, where computers are simply a tool for the commission of economic and financial crimes[12]

When measuring the incidence of computer crime, the concern is with not only the volume of such activities but also their value, in terms of the damage and loss they cause to the victims themselves as well as the collateral damage incurred by others, including wider society and the nation State.

Clearly, the scale of the loss or damage caused will vary greatly according to which form of cybercrime is involved. In terms of computer-related offences, the nature of the loss and damage will obviously be dictated by the underlying criminal activity for which the computer, as a tool, was being used. Most modern large-scale economic and financial crime, for example, will utilize computers at some point, whether in terms of the inputting, processing or outputting of fraudulent data. In 1994, for example, Citibank suffered a significant breach of security in a case management system for financial institutions. Having hacked, the perpetrator was able to transfer funds out of the accounts of certain Indonesian banks.

For perpetrators of computer integrity crimes, the Internet offers individuals and criminal networks possibilities unparalleled in other environments, in terms of anonymity, mobility, geographical reach and the scope of the damage that can be inflicted. The range and scale of potential loss that may flow from attacks against computers and data are substantial and well reported[13] from individual inconvenience when a virus infects and corrupts a system, to substantial loss of revenue resulting from interruption of business. Where such attacks are targeted at, or inadvertently impact on, a nation's critical national infrastructure, such as power systems or transportation networks, their consequences are obviously of great significance and concern. In 2003, for example, the Port of Houston in the United States was brought to a standstill after a denial-of-service attack crippled the computer system on which the port's operations were dependent.

Box 6.2 sets out the key findings of a survey on the impact of computer-related crimes on major businesses in the United Kingdom.

The scant empirical data from developing countries are obviously fraught with difficulties and are potentially meaningless. The economic activity of developing countries may be viewed as being less dependent on computers and communications networks. Computers are also less integrated into every aspect of people's daily lives. The cost and resources required in order to secure systems against attack and exploitation, whether in terms of organizational, physical or logical measures, may often be beyond the means of those using those systems, the result being that there is greater vulnerability in developing countries than in developed ones.

Box 6.2

The impact on UK business

The following are the findings of a 2004 survey by the United Kingdom's National Hi-Tech Crime Unit:

1. Of 201 respondents, 167 had experienced hi-tech crime in 2003.
2. For those 167 companies, the total estimated cost was over £195 million, with financial fraud taking the lion's share at £121 million.
3. Seventy-seven per cent of all respondents faced virus attacks. Viruses affected all types and sizes of company.
4. Of the 44 financial services organizations which responded, three companies had experienced financial fraud totalling over £60 million.
5. Acts of sabotage and data theft most often originated internally. In addition, over a third of recent incidents of financial fraud were either wholly or partially, perpetrated by employees.
6. Almost three quarters of respondents agreed that the single most important impact of a computer-enabled crime was whether the company could continue to operate, function and do business with its customers.

As with other forms of loss and damage, there may be a range of options available to mitigate the loss suffered by certain categories of victim. The adequate provision of insurance cover, for example, is a standard developed-nation response to the risks of doing business. However, the complex nature and the scale of cybercrime-related losses have created problems in the market for the supply of such products in developed countries, which will only be greater in developing nations.

In terms of legal recourse, while cybercrime is primarily addressed through the criminal or penal code, Governments may adopt supplementary compensatory provisions, offering the possibility of the granting of compensation orders in addition to any punitive fine or jail term. In Singapore, for example, the Computer Misuse Act 1993 expressly grants a court the power to make an order against a person convicted of an offence to pay compensation to any party that has suffered damage from the offending activity. Similarly, in the United States, the Computer Fraud and Abuse Act provides that "any person who suffers damage or loss…may maintain a civil action…to obtain compensatory damage and injunctive relief or other equitable relief."[14]

2. Policy objectives

Law and regulation are about facilitating certain types of behaviour and restraining others. The imposition of criminal sanctions on an activity, particularly where the sanction involves the deprivation of liberty through imprisonment, clearly falls at one end of the spectrum in terms of the enforcement of public law. As such, criminal sanctions are not generally imposed without clear policy objectives being identified and articulated by the legislature through statute. Governments have a traditional role as guardian, but the adoption of protective measures, particularly criminal, can also be viewed as demand-side mechanisms supporting the development of e-commerce.

In terms of the development of a nation's information economy and society, it is widely recognized that engendering trust among users, both as citizens and consumers, is a critical element in facilitating the take-up of such techniques and technologies. Indeed, the need for a "global culture of cyber-security" was recognized as a key principle by the delegates at the World Summit on the Information Society (WSIS)[15] in Geneva in 2003 and, together with cybercrime, is a topic being examined by the UN Working Group on Internet Governance (WGIG).[16]

The policy objectives underpinning the criminalization of computer-related activities are generally unaltered by the use of computer technology. The objectives driving the criminalization of activities specifically targeted at computer systems and networks, particularly hacking and the distribution of viruses, range from concerns about the cost to users, both business and consumers, to a broad recognition of increasing societal dependence on such systems, especially with reference to "critical national infra-

structure", such as power networks and air traffic control systems.

Prevention being better than cure, criminalizing specific activities is not a complete or sufficient response to the threat of hackers, virus writers and cyber-terrorists. The targets or potential victims of attacks are usually best placed to implement the appropriate physical and organizational security measures that will prevent, deter or limit the consequences of such attacks. While the virtuous link between data security and cybercrime should clearly be in the interests of users, there is much evidence that data security measures are not given adequate attention or are not properly understood within many organizations.[17] However, since an interconnected and interdependent environment means significant negative externalities and collateral vulnerabilities resulting from a failure to take measures, policymakers must recognize the need to facilitate data security through a variety of mechanisms, including the imposition of legal obligations to implement "appropriate security measures"[18] and encouraging compliance with internationally recognised security standards such as ISO 17799 and ITU Recommendation X805.[19]

As concern about cybercrime as cyber-terrorism has increased, Governments have expressly addressed the vulnerabilities created by the Internet for so-called critical infrastructures, those "facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments."[20] While the specific scope of what constitutes "critical infrastructure" may vary between countries, computer and communications networks, including the Internet, are always explicitly identified. In South Africa, for example, requirements exist for the identification and management of "critical data", defined as data that the Minister of Communications considers "of importance to the protection of the national security of the Republic or the economic and social well-being of its citizens".[21] Obligations are placed on "critical database administrators" to implement measures to protect databases, and a failure to comply may itself be the commission of an offence. At the G8 level, member States have adopted a set of principles specifically aimed at the protection of "critical information infrastructures".[22]

While Governments are keen to promote the security of, and trust, in the Internet, as a mechanism for facilitating its development security technologies themselves are a source of vulnerability. Cryptographic products in particular, as the dominant technological solution to the need for authentication, integrity and confidentiality on the Internet, are categorized as "dual-use", having military as well as civil applications, and have been, in the past, subject to export controls. While there has been a relative deregulation of export controls, some regulation is still present at the national level and through international treaties. In the United States, the Department of Commerce's Bureau of Industry and Security controls exports of cryptographic products. Some export restrictions still exist for bespoke or military-grade systems. However, the general prescription is that exports are unrestricted, provided that the software is generally available to the public by being sold in retail outlets, that the cryptographic functionality cannot be easily changed by the user, that the software is designed for installation by the user without further substantial support from the developer, and that the developer agrees to provide the software for inspection in order to ascertain compliance with all requirements.[23] Internationally, the trade in cryptography software is the subject of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.[24] The Wassenaar Arrangement was established after the end of the Cold War and is seen as a successor to the Coordinating Committee for Multilateral Export Controls (CoCom). Its provisions are compatible with the prescription of the US Department of Commerce – namely, that software is not necessarily a restricted technology if it is generally available to the public or in the public domain. This is in recognition of the fact that many important cryptographic technologies are either in the public domain, their patents having expired several years ago, or are available as free and open source software that freely circulates on the Internet.[25]

Therefore, a duality in the nature of the vulnerability created by the Internet can be seen: as a source of vulnerability, the conduit for those that wish to attack State infrastructure; and a vulnerable entity in its own right, as an essential infrastructure.

3. Enforcing the law

Despite continuing public ignorance, it is now widely recognized by experts that the Internet does not suffer from a lack of law, but an excess of law coupled with an enforcement problem.[26] As noted above, one central issue in tackling cybercrime is the availability of law enforcement resources. Law enforcement can

be seen as a two-stage process: the investigation of illegal activities and the prosecution of offenders. Both stages are traditionally perceived as tasks to be carried out by the police, with the intelligence services operating where issues of national security are involved. However, the reality is that the "policing" of cybercrime will involve a diverse range of public and private sector entities.

In most developed-nation jurisdictions, a wide range of regulatory authorities are granted powers to investigate and prosecute persons for offences within their regulatory jurisdiction. These authorities have functions to investigate specific types of conduct, such as financial services authorities (e.g. in an Internet securities fraud) or trading standards bodies (e.g. preventing the sale of unauthorized signal decoders).

In some legal systems, a private person as well as a public authority may be able to pursue a prosecution for certain offences. In the area of criminal copyright infringement, for example, rights holders such as the Business Software Alliance and the International Federation of Phonographic Industries may lead the investigation and prosecution of perpetrators. Most notably, in France, the League Against Racism and Anti-Semitism and the French Union of Jewish Students brought a successful action against Yahoo! for the sale of Nazi memorabilia available via its auction service in breach of French penal code.

In terms of criminal investigations, the private sector is clearly needed to assist public law enforcement and may, through self-regulatory initiatives, establish entities with a specific remit to receive complaints, and investigate and report on illegal activities. The following are some examples:

- In 1999, the International Chamber of Commerce (ICC) established a Cybercrime Unit to provide a mechanism for reporting criminal activity in the area and alerting members.[27]
- Many countries have established Computer Emergency Response Teams (CERTs), with public and private sector funding, which are tasked with warning users of emerging cybercrime activities, as well as developing a core of skilled professionals able to help tackle incidents.[28]
- In December 2004, a group called "Digital PhishNet" was established to tackle online identity theft, comprising financial services companies, ISPs and law enforcement.[29]

The need for a partnership between State authorities and the private sector to enhance enforcement is an inevitable feature of the Internet. However, private sector law enforcement activities also raise concerns in terms of vigilantism, infringement of rights and a blurring of traditional concepts of accountability.

4. International harmonization

Computer crime has an obvious international dimension and policymakers recognize the need to ensure that legal protection is harmonized among nations, so as to prevent the emergence of cybercrime havens. The "I love you" virus, which first emerged in 2000, is the classic example of such a threat. The virus spread rapidly around the world affecting some 45 million Internet users and causing great financial losses.[30] The source was eventually traced to a virus writer named Onel de Guzman based in the Philippines.[31] However, under Philippines law at the time, there was no suitable offence to charge Guzman with, and after the local courts threw out an attempt to proceed against him for theft and credit card fraud, no proceedings were brought.

Attempts have been made within various international organizations and forums, such as the G8 member States' "Principles and Action Plan to Combat High-tec Crime"[32] and the United Nations,[33] to achieve a harmonized approach to legislating against computer crime and thereby try to prevent the appearance of "computer crime havens". The first major attempt was under the auspices of the Organisation for Economic Co-operation and Development (OECD). It published a report in 1986, which listed five categories of offence that it believed should constitute a common approach to computer crime.[34] However, the most significant intergovernmental institution in the field has been the Council of Europe.

The Council of Europe first examined the issue of computer crime in 1985, with the establishment of a committee of experts. The committee produced guidelines for national legislatures on a "Minimum List of Offences Necessary for a Uniform Criminal Policy", which outlined eight offences seen as critical areas of computer misuse requiring criminalization, including damage to computer data and programs. In addition, the report presented an "optional list" of four offences, which failed to achieve consensus among member States, but were thought worthy of consideration, including unauthorized use of a com-

puter. The report was endorsed in a Recommendation by the Council of Ministers urging Governments to review and legislate accordingly (Recommendation No. R(89) 9). A similar instrument, addressing procedural issues (Recommendation No. R(95)13), was adopted in 1995.

Council of Europe Recommendations are not binding legal instruments and, inevitably, had limited effect. However, as the Internet emerged as a new environment for the commission of crime, the attention of policymakers was refocused on the need for a harmonized response. In April 1997, the Council of Europe embarked on the adoption of a Convention, which member States would have a legal obligation to implement. In November 2001, the Council of Ministers adopted the Convention on Cybercrime (Cybercrime Convention), which was opened for signature in Budapest on 23 November 2001, and has since been signed by 34 of the 46 members of the Council of Europe. However, of particular significance to the status of the Convention, four non-members were also involved in the drafting process, the United States, Japan, South Africa and Canada, and became signatories. The Convention also contains a mechanism whereby other non-members can sign and ratify the Convention. The Convention entered into force as of 18 March 2004, when Lithuania became the fifth ratifying State.

Since the adoption of the Convention in 2001, an additional protocol to the Convention was agreed by member States, "concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", in January 2003. The protocol requires the establishment of a range of substantive offences concerning "racist or xenophobic material", including the dissemination of such material, threats and insults, and denial of genocide and crimes against humanity. However, owing to the complexities of legislating against such material, member States have considerable autonomy not to adopt such measures, where, for example, issues of freedom of expression conflict.[35]

The comprehensive nature of the Cybercrime Convention, as well as the geographical spread of its signatories, means that it is likely to remain the most significant international legal instrument in the field for the foreseeable future. The success of the Convention as a spur to harmonization can be measured on the basis not only of the number of signatories, including non-European countries, but also of the fact that it is the source of other harmonization initiatives, such as the Commonwealth Model Computer and Computer-related Crimes Bill (October 2002),[36] which addresses the needs of some 53 developed and developing nations. In 2005, the international police organization, Interpol, adopted a resolution describing the Convention as "providing a minimal international legal and procedural standard" and recommending that its 182 member countries consider joining it.[37] However, concerns have been expressed about the Convention by both human rights groups and providers of communication services, and there have been calls for a treaty to be drafted under the auspices of the United Nations.[38]

C. Reforming the criminal code

To address the threat of cybercrime and to enhance the security of the Internet, Governments have been keen to establish an appropriate legal framework that deters attacks. Such a framework is a question of substantive law, which must appropriately criminalize the different forms of cybercrime.

In general, law reform in respect of computer-related and content-related crime will involve considerations of adaptation designed to ensure that the criminal code is capable of being applied against acts involving the use of computers, rather than wholesale revision of the existing criminal code. The criminal code will generally have been drafted at the time of a modern State's establishment, on the basis of national historical precedents as well as borrowing from colonial and regional sources. As such, the code will often have been drafted using concepts and terminology that reflect the physical world rather than the virtual world.

It is beyond the scope of this Report to consider each and every type of computer-related and content-related crime; however, the following highlights some of the areas where jurisdictions have faced issues when applying the traditional criminal code in a cybercrime environment:

- *Information acquisition*: As information has become a more valuable commercial asset, such as intellectual property and personal data, the illegal appropriation of such information may need to be made subject to criminal sanction (e.g. identity theft) or to enhanced penalties (e.g. counterfeiting).

- *Dealing with machines*: Some criminal acts may be cast in terms of doing something to someone, such as deception (fraud). In a cybercrime environment, acts will often involve no human interface, being completely automated. The criminal code must ensure that machine-to-machine criminal acts are fully subject to the law.

- *Intangible damage*: The nature of computer and communication technologies means that damage may be done to a system which is not tangible or directly perceivable by persons, such as altering the magnetic state of a disk to erase data. Such intangible damage should be recognized by the criminal code.

- *Digital manipulation*: Digital information is capable of manipulation to an unprecedented extent. Consequently, statutory provisions based on fixed conceptions of capturing and presenting information (e.g. an indecent photograph) may need to be amended to reflect such flexibility.

- *Digital time*: It is recognized that events can happen on the Internet on a time scale that is different from that of traditional conceptions. The criminal code may need to reconsider the use of terminology such as "recorded" or "stored", which may imply a requirement for something more permanent than the transitory nature of events on the Internet.

- *Determining location*: As in the case of time, traditional criminal-law concepts of location may be challenged on the Internet. The criminal code needs to reflect the potential transnational scope of cybercrime activities.

Policymakers and legislators will therefore need to review the existing criminal code in order to address such issues and to reflect the nature of criminal activities in a Internet environment.

1. Computer integrity offences

In contrast to the other two categories (computer-related and content-related offences), computer integrity offences generally present countries with the need to establish *sui generis* offences, rather than reform the existing code. The computer integrity activities addressed in the international instruments can be broadly classified into four categories:

- Offences concerning access to data and systems;
- Offences relating to interference with data and systems;
- Offences concerning the interception of data in the course of their transmission;
- Offences concerning the use of tools or "devices" to carry out any of the above acts.

The two key elements of all these offences are intention – the traditional criminal-law requirement for the necessary mental element, or *mens rea* – and that the person must be acting "without right", "authorisation" or "lawful excuse".

Interference is generally considered to be of greater seriousness than the "mere" access offence, since the main mischief being addressed is threats against the integrity of data being processed and the operation of systems. Obviously, access may be gained in order to commit any number of further offences, whether fraud or terrorism. In the United Kingdom, for example, a terrorist act is defined as including actions "designed seriously to interfere with or seriously disrupt an electronic system".[39] In such cases, the access offence may be viewed as primarily "facilitative" in terms of the investigation and prosecution of cybercrime activities, since it will rarely be the main charge laid against the accused. [40] However, by criminalizing all forms of computer "trespass", such as access sought simply as an intellectual challenge or out of curiosity, an anomaly can be created with the legal treatment of analogous situations in the physical world.

In terms of interference, whether with data or systems, the concept is elaborated to cover all forms of modification, including deletion and suppression, as well as rendering such data or systems inaccessible or inoperable. The latter would be applicable to activities known as 'denial-of-service' attacks, where a person or persons bombard a system with data requests, thereby overloading the system and leading to its eventual shutdown. In the draft EU Framework Decision, interference which has "affected essential interests", a term presumably designed to encompass "critical infrastructure", is considered an "aggravating circumstance" which should be subject to more substantial penalties.

The interception of data in transmission is carried out in order to compromise the confidentiality of communications. Such espionage or surveillance will gen-

erally be for reasons of political or economic gain. Indeed, the political overtones attaching to interception activities have meant that communications privacy is given statutory or even constitutional protection in most jurisdictions. Historically, legal controls in respect of interception have been directed more towards the manifestations of the State, particularly law enforcement agencies, than towards individuals or networks of cybercriminals or cyber-terrorists.

The provisions in respect of "devices" are intended to address those that supply or possess the tools that are used to access or interfere with data or systems, or intercept communications, such as password "cracking" software and other "hacker tools".[41] These provisions have been controversial, since such tools will often encompass both legitimate and illegitimate purposes. In relation to supply, such offences could also be categorized as "facilitative", to the extent that they address the availability of the tools needed to commit cybercrimes. The possession offence can be categorized as a "preparatory" offence, criminalizing the steps taken prior to the commission of an integrity offence.

Harmonization of substantive offences is a prerequisite intergovernmental response to network-based crime. Identifying and criminalizing specified activities place a common legal framework on decentralized, informal and mobile transnational criminal and terrorist networks. However, concerns about overcriminalization may also be raised in respect of the *sui generis* computer integrity offences, particularly concerning access and devices.

2. Locating cybercrime

Computer crime often inevitably has a transnational aspect to it that can give rise to complex jurisdictional issues, involving persons present and acts carried out in a number of different countries. Even where the perpetrator and the accused are located in the same jurisdiction, relevant evidence may reside on a server located in another jurisdiction, such as a "Hotmail" account.

In terms of general law, as with most aspects of network-based activities, traditional concepts and principles are sometimes challenged by the nature of the technology. The general principle of international criminal law is that a crime committed within a State's territory may be tried there, although the territoriality of criminal law does not coincide with territorial sovereignty.[42]

However, where criminal activity is information-based a jurisdictional distinction between the initiation and termination of an act often results, such as in the case of the release of a virus and its execution within a recipient's system. One consequence of this jurisdictional dissonance, especially in an Internet environment, is that criminal law has had to be amended to extend the territorial reach of certain offences. In addition, the general concern about the growth and societal impact of computer crime has led Governments to apply extraterritorial principles to computer crime.

In terms of ensuring legal certainty, general principles of international criminal law are made concrete through express jurisdictional provisions in the substantive legislation. Such rules generally claim jurisdiction if one of the elements of the offence occurs within the State's territory. Under the United Kingdom's Computer Misuse Act 1990, for example, jurisdiction is asserted through the concept of a "significant link" being present in the domestic jurisdiction, for example if either the computer or the perpetrator is in the United Kingdom. In the United States, the USA Patriot Act of 2001 amended the Computer Fraud and Abuse Act to extend the concept of a "protected computer" to include "a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States".[43] This effectively extends the territorial scope of the domestic offence, when the attacked computer is in another jurisdiction.

While the jurisdictional norm of criminal law is the territorial principle, there are four broadly recognized principles under which extraterritorial jurisdiction is claimed or exercised in cases of international criminal activity:

- The "active personality principle", which is based on the nationality of the perpetrator;
- The "passive personality principle", which is based on the nationality of the victim;
- The "universality principle", for crimes broadly recognized as being crimes against humanity, such as genocide;
- The "protective principle", to safeguard a jurisdiction's national interest, such as the planning of an act of cyber-terrorism.

Both the Convention on Cybercrime and the Commonwealth Model Law address the question of establishing jurisdiction. The Convention states that jurisdiction should exist when the offence is committed:

(*a*) In the Party's territory; or

(*b*) On board a ship flying the flag of that Party; or

(*c*) On board an aircraft registered under the laws of that Party; or

(*d*) By one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. (Article 22).

The fourth scenario, based on the nationality of the offender, is an example of the "active personality" principle referred to above.

However, the adoption of extraterritorial provisions does not necessarily provide an easy solution to transborder cybercrime. First, there are practical difficulties arising from the need to gather evidence overseas and the possibility of bringing witnesses from abroad. Second, there may be potential conflicts with local laws, which may prevent evidence from being gathered or the accused being extradited. Third, doubts may be raised as to whether the public interest is served in the prosecution of cases where there is no impact on the jurisdiction in question.

D. Addressing the data problem

Cybercrime investigations and the gathering of appropriate evidence for a prosecution, the science of forensics, can be an extremely difficult and complex issue.[44] Steps will obviously be taken by perpetrators to hide or disguise their activities, such as "communications laundering" routing transmissions through a series of jurisdictions to frustrate attempts to trace the source or the extensive use of cryptographic techniques to render data unintelligible. However, the environment itself also raises significant challenges owing, in part, to the intangible and often transient nature of data involved. The nature of the technologies bestows upon data the duality of being notoriously vulnerable to loss and modification, as well as being surprisingly "sticky" – subject to a thorough inspection, a hard disk will reveal much data that may have been assumed as deleted – at one and the same time. The "stickiness" of data is attributable, in part, to the multiple copies generated by the communications process, as well as to the manner in which data are stored on electronic media. Such technology renders the process of investigation and recording of evidence extremely vulnerable to defence claims of errors, technical malfunction, prejudicial interference or fabrication, which may lead to such evidence being ruled inadmissible.[45]

A lack of adequate training of law enforcement officers, prosecutors and, indeed, the judiciary will often exacerbate the difficulties of computer forensics. In developed countries, substantial efforts have been made over recent years to address this training need and specialized courses and facilities have established. In addition, computer forensics has become a recognised academic discipline and numerous organizations now offer such services on both a commercial and a non-commercial basis. Law enforcement agencies have also formalized their treatment of computer-derived evidence, through the issuance of guidance.

Box 6.3 provides an example of principles designed to ensure good practice when collecting computer-based electronic evidence.

Relevant evidential data may be found in the systems of the victim, the suspect and/or some third party, such as a communications service provider. Alternatively, evidence may be obtained from data in the process of being transmitted across a network, generally referred to as intercepted data. Specific rules of criminal procedure address law enforcement access to both sources of evidence data at rest or data in transmission although the Internet raises a range of issues in relation to the operation of such rules.

Any criminal investigation interferes with the rights of others, whether the person is the subject of an investigation or a related third party. In a democratic society any such interference must be justifiable and proportionate to the needs of society to be protected. However, the growth of cybercrime has raised difficult issues in respect of the appropriate balance between the needs of those investigating and prosecuting such crime, and the rights of data users to privacy. This section considers some of the problems raised by data for law enforcement agencies investigating cybercrime and examines proposals for procedural law reform.

Box 6.3

ACPO Good Practice Guide for Computer Based Evidence[1]

The following principles should guide the practice of all law enforcement agency investigations:

Principle 1: No action taken by law enforcement or their agents should change data held on an electronic device or media which may subsequently be relied upon in Court.

Principle 2: In exceptional circumstances where a person finds it necessary to access original data held on an electronic device or media that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.

Principle 3: An audit trail or other record of all processes applied to electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.

Principle 4: The person in charge of the investigation (case officer) is responsible for ensuring that the law and these principles are adhered to.

[1] Association of Chief Police Officers (ACPO), Good Practice Guide for Computer Based Evidence (3rd edition, 2004), available at www.nhtu.org.uk

1. Data at rest

Communications involve at least two parties the caller and the called. In data communications either party, or both, may be machines or more accurately software or files residing on machines, rather than people. Law enforcement agencies will generally access forensic data once they have been recorded or stored, whether in the systems controlled by the calling or called parties, or during the process of transmission. However, access to stored data has raised a number of issues in relation to criminal procedure, in respect of the seizure of such data, particularly when held remotely, protected data, communications data and the preservation or retention of data.

Seizing data

Data stored in the computer system of the suspect are generally obtained through the execution of a court order for search and seizure. A search and seizure warrant can give rise to problems where the relevant material is held on a computer system being used at the time of the search, since any attempt to seize the material for further examination may result in either the loss or the alteration of the evidence.[46] Another problem for law enforcement is the volume of data that are generally subject to seizure, especially since the cost of data storage has fallen and capacity increased dramatically in recent years. The time and expense involved in shifting and scrutinizing seized data are a serious impediment to the process of investigation.

One aspect of the use of search and seizure warrants in a Internet environment concerns the geographical scope of a warrant, issued by a court and authorizing such acts. The Cybercrime Convention, for example, states that the right to search and access should extend to any other computer system on its territory which "is lawfully accessible from or available to the initial system" (Article 19(2)). Thus, an authorized search at a single site can potentially be extended to interconnected systems located anywhere within the jurisdiction.

However, where the remote computer is based in another jurisdiction, important issues of sovereignty and territoriality may arise. In 2000, for example, as part of an investigation into the activities of two Russian hackers, Vasiliy Gorschkov and Alexey Ivanov, the FBI accessed computers in the Russian Federation via the Internet, using surreptitiously obtained passwords to download data from computers operated by the accused, who were already under arrest in the United States. In retaliation for this breach of sov-

ereignty, the Russian authorities charged the FBI agent responsible for the intrusion.[47]

To address these potential conflicts, member States parties to the Cybercrime Convention accepted that access to data stored in another jurisdiction might be obtained without the authorization of the State in which the data reside in two situations:

> *a.* access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
>
> *b.* access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system. (Article 32)

Article 32 details two circumstances which all parties to the Convention could accept, but does not preclude other situations being authorized under national law. An example of a more aggressive stance to accessing remote data is Australia, where a specific warrant-based procedural mechanism was adopted to enable the Australian Security Intelligence Organisation to access remotely held data. These provisions not only authorize the seizure of data, but also permit the modification of any obstructive access control and/or encryption systems to obtain access to the data. Such proactive policing, utilizing the techniques and tools of the cybercriminal in the course of an investigation, even potentially to launch an attack against a foreign perpetrator, raises serious issues of legitimacy, due process and the potential for sovereignty disputes.[48]

Protected data

As discussed above, evidentially relevant data may be obtained through intercepting a communication session or from a party who has stored the data. However, the data once obtained may be in a form that is designed to protect it from being disclosed to third parties; for example, data could be encrypted in order to ensure its confidentiality. In the United States, for example, when the notorious hacker Kevin Mitnick was finally arrested, many of the files found on his computers were encrypted and investigators were never able to access them.[49]

The nature of data security technologies means that investigating authorities have essentially three options in respect of gaining access to protected data:

- Require the person from whom the data have been obtained to convert them into an intelligible plain-text format;
- Require the person to disclose the necessary information and/or tools to enable the authorities to convert the data into a legible format themselves;
- Utilize technologies and techniques which enable the data to be converted without the active involvement of the person from whom the data were obtained.

The first option represents standard criminal procedure in most countries. Under the second option, proposals have been made in some jurisdictions for specific requirements to deliver up "keys" to render data intelligible. Such an obligation differs from the approach taken in traditional investigations. Criminal procedures do not, generally, contain express requirements to provide, for example, the combination to open a metal safe. However, modern data security techniques have been seen by some policymakers as requiring a specific legislative response.

The viability of the third option, converting the data into an intelligible form by utilizing available techniques, would seem to depend on a number of factors, including the strength of the technology used by the party applying the security technique, the functional design of future technology[50] and the period within which the data realistically need to be converted. However, technological developments may create security mechanisms which are incapable of being overcome, such as quantum cryptography.[51] Some Governments have already established "in-house" technical capabilities to support law enforcement agencies,[52] and although such resource allocation is likely to be beyond the capacity of most developing countries, cross-border forensic services could be made available by such institutions.

Communications data

Establishing the identity of a person suspected of criminal activity is obviously crucial to the commencement of any legal proceedings. However, network users are often not readily identifiable from the naming and addressing information processed in the

course of a communications session. There will often be a need, therefore, for the investigator to map a user's electronic identity to his real world identity. A third party, the user's ISP, generally holds such information, and accessing it interferes with the interests both of that third party and of the person being investigated.

One of the classic aphorisms of the Internet age is Peter Steiner's famous cartoon captioned "On the Internet, nobody knows you are a dog".[53] However, in the course of an investigation, the investigator will need to identify the person carrying out the illegal activity, whether canine or not! The process of establishing a real world person's identity from their Internet-related identity creates a significant forensic and legal hurdle.

When utilizing an Internet-based service such as e-mail, the originator of a message requires an IP address, for example 38.111.64.2. That IP address is then logically linked to the originator's pseudonym and domain name, e.g. john.smith@first.com. However, whilst the IP address is unique, the person to whom it is linked will usually vary. ISPs and corporate networks will generally, for reasons of efficiency, dynamically assign an IP address to a user each time he or she logs onto a service or at the commencement of each communication session.

Identification is often a two-stage process. First, it is necessary to identify the person to whom an IP address has been assigned. This can be relatively straightforward, for example using "whois" software to interrogate one of the regional registry databases, which detail IP address allocation. Where the person has a fixed IP address, the registry will effectively identify the owner of the machine unless the address has been "spoofed"[54]. However, where a block of IP addresses belong to a service provider or organization, the second stage will be to approach the holder in order to match the IP address to a specific user. This will clearly not be possible where the holder either provides anonymous public services, such as cybercafe, or does not maintain a historical log of IP address allocation.

From the investigator's perspective, the first legal issue concerns the second-stage process: what legal obligations does the holder of the IP address have, whether a public communications provider or a corporate entity, to disclose information to an investigator identifying an individual user? Reliance on voluntary mechanisms is likely to result in inconsistent practice, perhaps constrained by conflicting legal obligations such as privacy laws or contractual constraints. It may therefore be necessary for investigating authorities to have specific powers to require the delivery of information upon receipt of a properly authorized request.

Preserved or retained data

The patterns created by the communications attributes of criminal and terrorist networks on the Internet are increasingly valuable to law enforcement agencies for discerning the operational nature of such networks forming, dissolving and reforming according to the logic of the opportunities being pursued. Such evidential data will be generated by the networks that comprise the Internet, as traffic passes into, across and out of each network, and will often be as transient as the communication session itself. To address such transience, Governments have looked to the imposition of express preservation and retention obligations upon the providers of communication services.

The Cybercrime Convention addresses the right of law enforcement agencies to request that stored or transmission data be preserved upon notice for certain periods of time, the so-called fast freeze-quick thaw model. Such an order will normally be made against an ISP. However, in the normal course of business traffic data are generally retained for relatively short periods of time, owing to the cost to the ISP as well as compliance with data protection rules, designed to protect the privacy interests of subscribers and users.

Concerns about security threats from the Internet led to calls for the imposition of a general data retention obligation on ISPs to enable law enforcement to access historical as well as real-time traffic data. Prior to the events of 11 September 2001, most Governments rejected such calls, recognizing that such wholesale retention obligations were a threat to privacy as well as an unnecessary cost burden for ISPs. Only expedited data preservation rules made it into the Cybercrime Convention, not general retention obligations, primarily owing to trenchant opposition from the United States.

In the United Kingdom, for example, provisions were incorporated in the Anti-Terrorism Crime and Security Act 2001, establishing a voluntary regime for the

retention of communications data, with the possibility of imposing mandatory directions. In April 2004, the Governments of the United Kingdom, Ireland, France and Sweden proposed a EU Council Framework decision to harmonize traffic data retention among EU member States.

However, large-scale data retention must itself be seen as vulnerable to abuse a new security risk and considerable concern has been voiced that provisions for retention breach data protection and human rights laws as a disproportionate response to an unmeasured threat.

2. Intercepted data

Evidence may also be obtained during the transmission of data between computers across communication networks. Such evidence may comprise the content of a communication, such as a list of passwords, or the attributes of a communication session, such as the duration of a call or the location of the caller, referred to as "traffic data" in the Cybercrime Convention and Commonwealth Model Law.

The interception of the content of a communication is usually subject to relatively strict procedural controls, designed more to protect against privacy infringements by law enforcement agencies than to deter cybercrime. Interception in the course of a criminal investigation will generally require authorization from a third party, usually in the form of a judicial or executive warrant. The Cybercrime Convention provides that authorization should be available only for "serious offences", which would obviously include cyber-terrorist activities, but not necessarily all forms of computer integrity offences, such as mere unauthorized access.

Historically, national legal systems have distinguished between the interception of the content of a communication and the traffic data related to the communication session itself, such as number called. Access to the latter has generally been subject to less stringent procedural hurdles, such as the need for a warrant. Such a distinction would seem to be based on a widely held perception that access to the content of a communication represents a greater threat to personal privacy than access to the related traffic data. However, developments in communications would seem to have led to a qualitative and quantitative shift in the nature of traffic data, from the generation of location data in mobile telephony to the ever-expanding range of daily activities carried out online. As a consequence, the volume of traffic data potentially available to law enforcement agencies and its value as an investigative tool have increased considerably. It would therefore seem arguable that the threats to individual privacy from accessing traffic data, compared with communications content, are of a similar nature in terms of revealing a person's private life and activities and should therefore be subject to comparable access regimes.

One procedural issue raised by differential legal treatment is that in a Internet environment the distinction between traffic data and content is becoming increasingly blurred. A web-based Uniform Resource Locator (URL), for example, may contain not only details of the IP address of the website being accessed, akin to a traditional telephone number, but also further information in relation to the content of the requested communication, such as a particular item held on the site or a search string containing the embedded parameters of the search, for example:

http://www.google.com/
search?hl=en&q=aliens&btnG=Google+Search

In the URL example above, how should the "traffic data" be separated from the associated content? Reliance on law enforcement agencies to distinguish such data would seem unacceptable, and this therefore requires us to consider the role of the communication service provider, over whose network the data are being sent during the interception process. The relevant service provider would need to be able to identify the relevant data and then automatically separate traffic data for forwarding to the appropriate requesting authority.

The consequences of the blurring between traffic data and content in a Internet context and their differential legal treatment are potentially significant in terms of eroding an individual's traditional privacy rights. In addition, communication service providers face legal, procedural and operational uncertainties with regard to the obligations to obtain and provide data that have been requested by an investigating agency.

3. Communication service providers

In a traditional voice telephony environment, the general principle was that an interception would be carried out as physically close to the suspect as possible,

which usually meant at a local loop or exchange level. In a Internet environment, the principle is no longer necessarily applicable as the proliferation of intermediary service providers within the network hierarchy structure presents a range of alternative points of interception (e.g. a web-based e-mail service and cached web pages).

Historically, in order to enable law enforcement agencies to intercept communications, the incumbent operator, often State-owned, has maintained the technical capability to intercept communications. However, in an environment of multiple networks, of vastly varying size and nature, Governments have had to establish formal obligations and procedures concerning "intercept capability". These generally differentiate between the different types of communication service providers (CSPs) and networks.

CSPs have a number of concerns arising from an obligation to ensure an "intercept capability". First, considerable reservations have been expressed about the feasibility of achieving a stable "intercept capability" solution in a rapidly evolving communications environment. "Intermediary service providers" in particular are concerned that their freedom to design, build and operate innovative data communications networks and services, in accordance with the dictates of newly available technologies and commercial imperatives, would be significantly restrained by the need to meet an ongoing obligation to ensure an "intercept capability". It is generally accepted that a single technological solution to the requirement for "intercept capability" is not going to be available; this will have associated cost implications for CSPs and, potentially, procedural implications for law enforcement agencies.

Second, the costs arising from compliance with an obligation to provide "intercept capability" are an important factor. Such costs can be categorized as fixed costs, in relation to building the "capability" into the network (e.g. switches with intercept functionality), and variable costs, arising from the operational aspects of carrying out an interception (e.g. personnel). It is beyond the remit of this report to suggest the most appropriate division of costs between Governments, as holders of public funds, and the providers of communication networks and services. In many jurisdictions, fixed costs are borne by the CSP, whilst variable costs are covered by the relevant public authority.[55] It is generally accepted that shifting some of the financial cost arising from an investigation to the investigating agency acts as an effective restraint on the use of such techniques.

Significant concerns have been expressed, however, particularly by representatives of newly emerged "intermediary service providers", that the costs involved in implementing "intercept capability" in modern communication networks are likely to be substantial. Such concerns have been reflected in some jurisdictions through express statutory reference to the parties required to bear the costs.

4. Cooperating against cybercrime

Another aspect of the governmental response to Internet crime is improvement of cooperation between national law enforcement agencies. At one level, cooperation will involve mutual assistance in the obtaining and exchange of information, whether as intelligence or evidence. In this regard, agencies have established "network" structures in an attempt to mimic the responsiveness and flexibility of other networks. However, such an approach would not seem appropriate where the cooperation involves the movement of suspected perpetrators, further up the enforcement chain.

Moving evidence

The investigation and prosecution of transnational cybercrime will usually require substantial co-operation between national law enforcement agencies, prosecuting authorities and private sector entities such as ISPs. Obtaining such cooperation, generally referred to mutual legal assistance (MLA), in a timely and efficient manner will often be critical to the success of a cybercrime investigation. Historically, however, MLA procedures have been notoriously slow and bureaucratic.

A request for evidence from another jurisdiction is known as a "letter rogatory", and will generally be issued only where it appears that an offence has been committed and that proceedings have been instituted or an investigation is under way. The request may be sent to a court in the relevant jurisdiction, to a designated authority or, in an urgent case, through the International Criminal Police Organization (Interpol). The evidence, once received by the requesting State, should then be used only for the purpose specified in the request; this principle is known as the "specialty principle", a principle also present in extradition treaties, requiring the requesting State to prosecute the

accused only for the crimes detailed in the extradition request.

Despite the existence of MLA procedures, there is always a time lag created by the need to channel a request through the appropriate authorities. As a consequence, law enforcement agencies have adopted alternative informal approaches to the need for a rapid and flexible exchange of information. In the United States, for example, the extension of the concept of a "protected computer" to include non-US based computers, as noted above, means that when a foreign law enforcement agency contacts the US authorities, they can provide assistance informally on the basis that the perpetrator's activities also constitute an offence under US law, rather than comply with MLA procedures. Such an approach may be seen as an alternative version of the "double criminality" principle, discussed below, where the act is in actuality an offence in both jurisdictions, rather than theoretically. While the US authorities may have no intention of pursuing a domestic prosecution, the possibility provides an informal alternative to the mutual legal assistance route.

Many of the international harmonization initiatives have been designed to address the institutional and procedural obstacles to the investigation of a crime, as much as the substantive offences themselves. One key mechanism is the establishment of a network of designated law enforcement contacts, available 24 hours a day, 7 days a week. In 2003, Interpol established a global police communications system, referred to as "I-24/7", to facilitate a rapid response and information exchange among its 182 member countries. In addition, Interpol has established regional working parties (i.e. European, American, African and Asia-South Pacific) to develop good practice through sharing expertise.[56]

As well as reacting to requests, such networks offer a channel for the proactive exchange of intelligence. The Cybercrime Convention, for example, envisages the provision of "spontaneous information", namely intelligence, where by agencies in one State disclose information uncovered during their investigations to another State for the purpose of initiating or assisting an investigation (Article 26). However, such disclosures should be subject to the domestic law of the disclosing State, such as data protection rules, which may impose restrictions on the transfer of personal data.

Moving people

Clearly, when a system is attacked, the perpetrator may be located anywhere in the world. Therefore, if a prosecution is to be mounted, the accused has to be brought to the prosecuting State. The formal procedure under which persons are transferred between States for prosecution is known as extradition. Either bilateral or multilateral treaties or agreements between states generally govern extradition. In the absence of such a treaty, the State where the perpetrator resides is not required under any rule of public international law to surrender the person. In such situations, informal mechanisms may be used to bring the perpetrator to justice. In the *Levin* case referred to above, for example, the accused was enticed to leave the Russian Federation, with which the United States did not have an extradition treaty, and was arrested as soon as he landed in a country with which the United States did have an extradition arrangement, namely the United Kingdom.[57]

In an action for extradition, the applicant State is generally required to show that the actions of the accused constitute a criminal offence exceeding a minimum level of seriousness in both jurisdictions, the country from which the accused is to be extradited and the country to which the extradition will be made. This is referred to as the "double criminality" principle and is generally a threshold of a minimum of 12 months' imprisonment in both States (Cybercrime Convention, Article 24). Meeting the 'double criminality' standard is clearly an objective of harmonization initiatives in respect of substantive offences. In *Levin*, for example, the defendant was accused of committing wire and bank fraud in the United States. No exact equivalent exists in English law, and therefore Levin was charged with 66 related offences, including unauthorized access and unauthorized modification.

Most countries will not extradite juveniles, although a significant proportion of cybercrime perpetrators fall into this category. In addition, some jurisdictions, such as France, make a distinction between nationals and foreign persons, extradition being only available in respect of non-nationals. To address this potential lacuna, the Cybercrime Convention provides that member States shall establish jurisdiction over and prosecute offenders that they refuse to extradite.[58]

E. Concluding remarks and policy recommendations

The Internet can be viewed as the ultimate transnational communications network, offering an unrivalled capability for accessing data and computer systems on a global level. As economies and society become dependent on the Internet, it becomes a critical information infrastructure over which nearly all Governments have only limited control.

Combating cybercrime is one of the greatest challenges facing society today. Evidence of the scale of the threat from cybercrime and cyber-terrorism remains scant, although Governments and, indeed, the wider general public are convinced of the need for action. The Internet can be used to undermine State control and circumvent State laws; however, law reform can address aspects of cybercrime and enhance security on the Internet: as a spur to action for system controllers, as a deterrent for perpetrators and as a tool for law enforcement agencies

Technologically neutral statutes

It is generally accepted that online conduct should be treated no differently from offline conduct. Laws should be technologically neutral and based on the act rather than the technology used to commit the act. As FBI Director Louis Freeh noted in testimony before the United States Senate, "Statutes need to be rendered technology neutral so that they can be applied regardless of whether a crime is committed with pen and paper, e-mail, telephone, or geosynchronous orbit personal communication devices".[59]

Balance between law enforcement and human rights

Criminalization of computer wrongdoing is a prerequisite for combating cybercrime. Thus, in response to threats to the integrity of computer systems and the data that they process, Governments have pursued the harmonization of legal rules and greater law enforcement cooperation. While public perception of cybercrime revolves around specific types of behaviour, such as "hacking",[60] policymakers have primarily been concerned with reforming the procedural aspects of investigating and pursuing cybercriminals. Since the events of 11 September 2001, law enforcement agencies have been granted substantially enhanced powers of investigation. However, there is a fear that the desire to secure the Internet may result in a concomitant erosion of individual privacy and other fundamental liberties. Thus, it is necessary to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in international human rights treaties, such as the 1966 United Nations International Covenant on Civil and Political Rights.

International cooperation

As cybercrime has become a threat, harmonization and cooperation have gathered pace and re-engaged the attention of legislators. It is acknowledged today that an effective fight against cybercrime requires increased, rapid and well-functioning international cooperation in criminal matters.[61] Initiatives in this connection can be seen as extensions of State authority in the face of the erosion of State control. Despite the early territorial assertions for the Internet, cybercrime activities take place and have effects in and between territories. Consequently, Governments may be prepared to trade a loss of some degree of *de jure* State control, in terms of criminal procedure, reflecting their loss of *de facto* control, in return for extended jurisdictional reach, enhancing State authority.

Capacity development

It is recognized that in many developing countries there is a lack of sound, basic knowledge and experience in investigating cybercrime. Thus, it is recommended that adequate awareness programmes be established for decision makers, cybercrime units, justice departments, the private sector and academic institutions .Moreover, it is important that adequate resources in terms of finance, staff and equipment be devoted to addressing cybercrime.[62]

Recommendations

The following highlights some policy considerations and recommendations that policymakers in developing countries may need to address when considering a comprehensive response to the phenomenon of cybercrime:

- Review the existing legal framework and enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with the provisions of international legal instruments, including UN General Assembly Reso-

lution 55/63 (see box 6.1) and the Council of Europe Convention on Cybercrime.

- Cooperate in the exchange of experience and information about legislation and judicial and law-enforcement procedures applicable to computer crime.
- Promote public awareness of the need to implement appropriate data security measures, at a physical and organizational level, encouraging compliance with international standards and the development of sectoral codes of practice.
- Facilitate training among law enforcement officers, State prosecutors and the judiciary in cybercrime technologies and techniques.
- Identify critical national infrastructure that may be vulnerable and susceptible to deliberate attack or accidental damage, and put in place a risk management strategy designed to deal with such risks.
- Consider the imposition of obligations to report to an appropriate government department any breach of data security experienced by certain categories of commercial entity, such as banks.
- Consider the establishment of specialized law enforcement units, combining personnel who have traditional policing skills with computer professionals.
- Establish mechanisms to facilitate greater liaison and cooperation between public sector law enforcement agencies and the private sector, especially providers of telecommunications services.
- Establish mechanisms to develop computer crime prevention and victim assistance programmes.

Notes

1. See Macan-Markar M, Developing Countries Not Immune From Cyber Crime Ø U.N., Inter Press Service, posted 25 April 2005, available at http://www.ipsnews.net/africa/interna.asp?idnews=28430.
2. Gibson W, *Neuromancer*, Harper Collins, 1984.
3. Wall DS, *Internet Crime,* Dartmouth, Aldershot, 2003, at p. xv.
4. See section 1.5 below.
5. The G8 categorizes computer-related and content-related together as "computer-assisted threats", as distinct from "threats to computer infrastructures".
6. Measures to Combat Computer-related Crime, Workshop 6: Background Paper (A/CONF.203/14), at para. 14 *et seq*. Presented at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, April 2005.
7. See generally The state of crime and criminal justice worldwide (A/CONF.203/3), Report of the Secretary-General, presented at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, April 2005.
8. See Computer Security Institute and Federal Bureau of Investigations, *Computer Crime and Security Survey*, 2004 (CSI-FBI 2004), available at http://www.gocsi.com/.
9. California Senate Bill 1386, available at http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.
10. See Kabay M, Studies and Surveys of Computer Crime, 2001, available from www.securitystats.com/reports/Studies_and_Surveys_of_Computer_Crime.pdf.
11. ASCL Computer Crime & Abuse Report (India) 2001-02, quoted in UNCTAD, *E-Commerce and Development Report*, 2003, p. 54.
12. See Discussion Guide presented at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, Bangkok, April 2005, at para. 103.
13. E.g. CSI-FBI 2004.
14. 18 U.S.C. § 1030(g).
15. WSIS Declaration of Principles (WSIS-03/GENEVA/DOC/4-E), 12 December 2003.
16. See Draft WGIG Issue Paper on Cybersecurity and Cybercrime, available at http://www.wgig.org/docs/WP-cybersec.pdf.
17. See, for example, Schneier B, *Secrets and Lies*, Wiley, 2000.
18. E.g. European data protection laws. Directive 95/46/EC states in Article 17(1): "Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing".
19. WGIG at p. 2. For more details on security issues see chapter 5 of this Report
20. Commission Communication to the Council and the European Parliament on Critical Infrastructure Protection in the Fight against Terrorism, COM(2004) 702 final, Brussels, 20 October 2004.
21. Electronic Communications and Transactions Act 2002, Article 52(1)(a).
22. G8 Principles for Protecting Critical Information Infrastructure, adopted May 2003, available at www.usdoj.gov/ag/events/g82004/g8_CIIP_Principles.pdf.

23. See http://www.access.gpo.gov/bis/ear/txt/ccl5-pt2.txt for the text of the US Department of Commerce's Bureau of Industry and Security regulation on US DoC BIS Category 5 Ø Telecommunications and "information security".

24. The Wassenaar Arrangement signatories are Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, the Republic of Korea, Portugal, Romania, the Russian Federation, Slovakia, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom and the United States. For more details see http://www.wassenaar.org/.

25. See chapter 5, part C, for details of the development of particular cryptographic technologies.

26. Reed C, *Internet Law: Text and Material*, Cambridge University Press, 2004.

27. www.iccwbo.org/ccs/menu_cybercrime_unit.asp.

28. See www.cert,org.

29. See http://www.digitalphishnet.org/.

30. Brenner S, and Goodman M, Cybercrime: The Need to Harmonize National Penal and Procedural Laws, 2002, International Society for the Reform of Criminal Law, 16th Annual Conference Technology and Its Effects on Criminal Responsibility, Security and Criminal Justice.

31. Grossman L, 15 May 2000, Attack of the Love Bug, Time Europe, at http://www.time.com/time/europe/magazine/2000/0515/cover.html.

32. See also the G8 Recommendation on Transnational Crime. The Recommendation was endorsed at the G8 Justice and Interior Ministers' Meeting in Canada, 13–14 May 2002 (http://www.g8j-i.ca). See in particular, Part IV, Section D, "Hi-Tech and Computer-Related Crimes".

33. General Assembly Resolution 55/63, Combating the criminal misuse of information technologies, 22 January 2001. See also the *United Nations Manual on the Prevention and Control of Computer-related Crime,* United Nations publication, Sales No. E.95.IV.5.

34. Computer-Related Criminality: Analysis of Legal Policy in the OECD Area, Report DSTI-ICCP 84.22 of 18 April 1986.

35. Article 3(3).

36. http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/{DA109CD2-5204-4FAB-AA77-86970A639B05}_Computer%20Crime.pdf.

37. www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp.

38. See Discussion Guide, supra n. 14, at para. 190.

39. Terrorism Act 2000, s. 1(2)(e).

40. Smith R, Grabosky P and Urbas G, *Cyber Criminals on Trial*, Cambridge University Press, 2004.

41. Council of Europe Convention on Cybercrime, Explanatory Report, para. 71 *et seq*.

42. Cassese A, *International Criminal Law*, Oxford University Press, 2003, p. 277.

43. § 1030(e)(2)(B).

44. See generally Casey E, *Digital Evidence and Computer Crime*, Academic Press, 2004.

45. Sommer P, Evidence from Internet: Downloads, Logs and Captures, pp. 33–42, *Computer and Telecommunications Law Review*, vol. 8, no. 2, 2002.

46. See, for example, the US Department of Justice Report *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, July 2002: available at http://www.usdoj.gov/criminal/cybercrime).

47. Brenner S and Koops B-J, "Approaches to Cybercrime Jurisdiction", 4 *Journal of High Technology Law,* 1, 2004.

48. Reidenberg J, States and Internet Enforcement, 1 U. Ottawa L. & Tech. J. 1, 18 (2004), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965.

49. See generally www.freekevin.com.

50. US-based hardware and software manufacturers, such as Intel, have been in discussions with law enforcement agencies about the possibilities of "building-in" certain functionalities into their products to assist criminal investigations.

51. See Stix G, Best-kept secrets, *Scientific American*, January 2005.

52 E.g. in the United Kingdom, the Government has established a National Technical Assistance Centre.

53. *New Yorker cartoon*, 5 July 1993.

54. This means that a false IP address is inserted in the packet headers.

55. In Belgium and Finland, the costs involved in a criminal investigation may ultimately be recovered from the perpetrator, if found guilty.

56. See http://www.interpol.int/Public/TechnologyCrime/default.asp.

57. *R v Governor of Brixton Prison and another, ex parte Levin* (1996) 4 All ER 350.

58. Article 22(3).

59. *Foreign Economic and Industrial Espionage Remains a Threat in 1999*, National Center for Counterintelligence, p. 2, http://www.nacic.gov/fv99.htm.

60. Many computer scientists and programmers will refer to the criminal misuse of computer code as "cracking" while reserving the term "hacking" for the more mundane tasks of writing non-infringing computer code. For an example, see http://tlc.discovery.com/convergence/hackers/hackers.html.

61. See Preamble to the Convention on Cybercrime.

62. See 5th Meeting of the Interpol Working Party on IT Crime Africa, Pretoria, 17-19 May 2005, http://www.Interpol.int/Public/TechnologyCrime/WorkingParties/Africa/5thMeeting/.