United Nations A/CONF.187/10

Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders

Vienna, 10-17 April 2000

Distr.: General
3 February 2000

Original: English

Item 5 of the provisional agenda*
Effective crime prevention: keeping pace with new developments

Crimes related to computer networks

Background paper for the workshop on crimes related to the computer network

Summary

Effectively preventing and combating cyber crime requires a coordinated international approach at different levels. At the domestic level, the investigation of cyber crime requires adequate staff, expertise and procedures. States are encouraged to consider mechanisms that enable the timely and accurate securing of data from computer systems and networks, should data be required as evidence in legal proceedings. At the international level, investigating cyber crime requires timely action, facilitated by coordination between national law enforcement agencies and the enactment of appropriate legal authority.

In addition to and in support of the international initiatives already taken, the present paper considers the means for the exchange of technical and forensic expertise between national law enforcement authorities, as well as the need for international deliberations on present and future legal measures for international cooperation in the investigation of cyber crime.

*A/CONF.187/1.

V.99-90954 (E)

Contents

I. Legislative background

1. The General Assembly, in its resolution 52/91 of 12 December 1997, decided that one of four workshops to be held at the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders should be on the issue of crimes related to the computer network. The Assembly, in its resolution 53/110 of 9 December 1998, endorsed the programme of work for the Tenth Congress, which included four technical workshops, one of them dealing with crimes related to the computer network. In the resolution, the Assembly emphasized the importance of the workshops and invited Member States, non-governmental organizations and other relevant entities to support financially, organizationally and technically the preparations for the workshops, including the preparation and circulation of relevant background material.

2. In its resolution 54/125 of 17 December 1999, the Assembly encouraged States, other entities concerned and the Secretary-General to work together in order to ensure that the four workshops to be held during the Tenth Congress focus clearly on the respective issues and achieve practical results, and invited interested Governments to follow up with concrete technical cooperation projects or activities. In response to the resolution, the Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders organized two meetings of experts on crimes related to the computer network, at which most of the substantive preparations for the computer crime workshop were made. The Centre for International Crime Prevention acknowledges the efforts of the Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders and the expert group in making this workshop possible.

II. Aim and scope of the paper

3. The emergence of international computer networks, such as the Internet, enables users to engage in communications, actions and transactions with other users all over the world. Since legitimate and illicit use of computers and networks can go hand in hand, it follows that those exploring the opportunities of the new medium include criminally motivated individuals and groups. Crime control in today's environment of international computer networks is complicated for three major reasons:

(a) Criminal behaviour can take place in an electronic environment. Investigation of cyber crimes, that is, any crime committed in an electronic network, requires particular expertise, investigating procedures and legal powers that may not be available to law enforcement authorities of the State concerned;

(b) International computer networks, such as the Internet, are open environments that enable users to act beyond the borders of the State in which they are located. However, investigative efforts of law enforcement authorities in general should be restricted to the territory of their own State. This means that crime control in open computer networks requires intensified international cooperation;

(c) The open structures of international computer networks offer users the opportunity to choose the legal environment that best suits their purposes. Users may choose a country where certain forms of behaviour capable of being executed in an electronic environment have not been criminalized. This can attract criminal activity by persons from other States where such activities are criminal under their domestic law. The occurrence of "data havens"—States where reducing or preventing the misuse of computer networks is not a priority, or where no effective procedural laws have been developed—may impede the efforts of other countries to control crime in computer networks.

4. The focus of the following discussion is on how to achieve coordinated international action in order to facilitate, enhance and improve current methods of combating cyber crime. Of particular interest is the role that can be played by the United Nations or other international organizations. Background information is provided regarding the workshop on crimes related to the computer network.

5. The following discussion outlines the types of crimes envisaged for international electronic networks and explores why such crimes need international attention and combined efforts. The definition of such crimes should bring a common international understanding and guide national criminal policies in the field.

III. Categories of cyber crime

6. The terms computer systems or computer networks are used in the present paper to refer generally to the electronic environment. Although stand-alone systems still

exist, it is more the norm for one or more computer systems, including personal computers, to be interconnected and form a network. No distinction is made here between private and public networks, or based on whether they have permanent connections. In the present paper, unless stated otherwise, telecommunication systems are grouped in the same category as computer systems and networks.

7. At present, the Internet is a well-known example of a public computer network. It has gone through an explosive growth in the last decade. It owes much of its success to the use of common communication protocols. Any system or network operator who applies such protocols can easily become a link in the network as a "provider", referred to in the present paper as an Internet service provider. For commercial and technical reasons, the Internet service providers in some countries organize themselves into associations or societies, developing common positions on certain issues.[1] Estimates show that today over 200 million people in the world use the Internet, of whom 112 million are in North America, 47 million in Europe and 33 million in Asia and the Pacific region.[2] At the end of 1995, statistics showed 26 million users, the majority of whom resided in the United States of America. In 1999, the monthly increase in users was estimated at more than 3 per cent.

8. The core function of a computer system is the processing of data. The term data is defined as facts, instructions or concepts represented in a conventional manner, in a form suitable for human understanding or automated processing.[3] Electronic data are represented by a string of magnetic spots on a permanent or temporary storage medium, or in the form of electric charges when being transferred. When data can be identified and controlled by a particular data carrier, such as data stored on a (set of) floppy disks they can, from a legal point of view, be considered one tangible material object. In general, data processed in a computer system can no longer be qualified and controlled by means of their carrier. Operating systems autonomously move data files from one physical place on a storage medium to another. In computer networks, distributed data processing makes it impossible for those in control of data to establish the physical location of the whole or a part of a file without specific measures. Data as such can be controlled only through logical operations not physical acts, which makes it difficult to treat pure data, in law, as if they were tangible objects.

9. Cyber crime refers to any crime that can be committed by means of a computer system or network, in a computer system or network or against a computer system or network. In principle, it encompasses any crime capable of being committed in an electronic environment. In this paper, "crime" refers to forms of behaviour generally defined as illegal, or likely to be criminalized within a short period of time. Certain conduct may be criminalized in one State where it is not in others but, as explained in paragraph 13, a common understanding has developed in certain international forums about which behaviour in relation to computer systems and networks should be criminalized. This is the starting point for the following discussion.

10. The focus here is the criminal investigation and prosecution of cyber crime. The designation "law enforcement authorities" refers to those charged by law with the investigation and prosecution of crime. Some Member States have set up specialized units to investigate or assist in the investigation of computer-related crime. Internationally, the International Criminal Police Organization (Interpol) is the coordinating organization for registering and distributing police information that concerns issues such as wanted persons and stolen property.

11. In investigating cyber crime, the law enforcement authorities of a State may seek the cooperation of authorities from other States, both in the form of assistance with specific cases and in the sharing of general information about criminal organizations and cases. They may, in the course of a particular investigation, request the use of materials available in other States. The scope of cooperation among national law enforcement authorities is determined by the national law of each State, as well as by international agreements, including agreements on mutual legal assistance.

12. Common examples of abuse of international computer networks include communicating expressions forbidden by law, offers of illegal products or false offers in order to obtain illegal financial profits. Here, the Internet is being used in the same manner as any other instrument or tool that may be used to commit a crime. The network itself is the environment of the crime, rather than an indispensable attribute for its perpetration. The specific qualities of the Internet may induce a perpetrator to use it instead of traditional means: it offers excellent communication facilities and the possibility of hiding one's identity, and the risk of being subjected to criminal

investigation, in any of the jurisdictions involved, is relatively low. Apart from the forms of crime mentioned, some Internet users gain illegal access to connected systems, where they interfere with their functioning or content. Such activity has been termed "computer crime". The perpetrators of computer crime availed themselves of specific technical knowledge, expertise or instruments to carry out illicit activities. Computer systems can be easy targets because sufficient security measures have not been incorporated or taken, or because users are unaware of the risks involved. In addition, factors that make a system user-friendly tend to make it unsecure. In addition, factors that make a system user-friendly tend to make it unsecure. Security flaws in commercially successful system software will often be publicly known.

13. While interested countries have considered the problems arising from transnational cyber crime, there has not been much attention paid to it at the global level. The United Nations, for example, has not yet adopted policy specific to the criminalization of cyber crimes; national laws may apply to cyber crimes in a variety of ways, if they apply at all. Reasons for the lack of attention to cyber crime may include relatively low levels of participation in international electronic communications, low levels of law-enforcement experience and low estimations of the damage to society expected to occur from electronic crimes. In global computer networks, the criminal policy of one State has a direct influence on the international community. Cyber criminals may direct their electronic activities through a particular State where that behaviour is not criminal and thus be protected by the law of that country. Even if a State has no particular national interest in criminalizing certain behaviour, it may consider doing so in order to avoid becoming a data haven and isolating itself internationally. The harmonization of substantive criminal law with regard to cyber crimes is essential if international cooperation is to be achieved between law enforcement and the judicial authorities of different States.

14. Two subcategories of cyber crime exist:

(a) Cyber crime in a narrow sense ("computer crime"): any illegal behaviour directed by means of electronic operations that targets the security of computer systems and the data processed by them;

(b) Cyber crime in a broader sense ("computer-related crime"): any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession, offering or distributing information by means of a computer system or network.

15. As defined in the previous paragraph, computer crime concerns all illegal behaviour directed against system and data security by means of electronic operations. Computer systems and data security can be described by three principles: the assurance of confidentiality, integrity or availability of data and processing functions. According to the 1985 Organisation for Economic Cooperation and Development list,[4] and the more elaborate 1989 Council of Europe Recommendation,[5] the confidentiality, integrity or availability offences include:

(a) Unauthorized access, meaning access without right to a computer system or network by infringing security measures;

(b) Damage to computer data or computer programs, meaning the erasure, corruption, deterioration or suppression of computer data or computer programs without right;

(c) Computer sabotage, meaning the input, alteration, erasure or suppression of computer data or computer programs, or interference with computer systems, with the intent to hinder the functioning of a computer or a telecommunication system;

(d) Unauthorized interception, meaning the interception, made without authorization and by technical means, of communications to, from and within a computer system or network;

(e) Computer espionage, meaning the acquisition, disclosure, transfer or use of a commercial secret without authorization or legal justification, with intent either to cause economic loss to the person entitled to the secret or to obtain an illegal advantage for themselves or a third person.

16. The first crime, unauthorized access, sometimes known as hacking, occurs frequently and often in conjunction with the second, damage to data or computer espionage. A popular modern variant is hacking into a web site and putting offensive or damaging information on it. Effective investigation of hacking offences usually requires cooperation by the victim and some means of catching the perpetrator in the act. Perpetrators are often brilliant young technophiles, who may have little moral understanding of their actions or of the potential to do damage. In addition to hacking offences, some countries have criminalized activities such as trafficking in passwords or hacking devices.

17. Corrupting computer data and programs includes launching "worms" or computer viruses. A worm may eventually cause the computer to stop functioning entirely, while a virus can cause the loss of all data stored in the hard disk. A modern way of distributing viruses is through unsolicited e-mail messages. Internet users may be unaware of the risk connected with open electronic networks and receiving unsolicited messages. For financial reasons, commercially available virus scanning programs may not be applied. Criminal investigators may find it difficult to prove who was responsible for launching a virus that has caused damage. Hackers may also misuse (temporary) security flaws in frequently used system programs and may obtain access to, or (in exceptional cases) control over, the computer systems of others by storing specific program functions in those systems. Internet users may not be adequately informed or up to date about the possible risks and additional security measures offered by system software manufacturers.

18. Computer-related fraud is defined by the Council of Europe (see para. 15 above) as:

> "The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing, thereby causing economic or possessory loss of property of another person with the intent of procuring an unlawful economic gain for himself or for another person."

This provision refers to the situation where a perpetrator interferes with the proper functioning of the data processing of a computer—with or without right—with the effect specified in the definition of fraud. It does not encompass well-known schemes to defraud people that are carried out by means of electronic representations or communications through the Internet, such as offers for the sale of favourably priced shares; investments in real estate in a foreign State; lending money with an exceptionally high interest return; prepayment of vaguely described goods; or enticement to enter a pyramid scheme. It is likely that traditional fraud provisions will apply to such schemes.

19. Computer forgery is defined by the Council of Europe (see para. 15 above) as:

> "The input, alteration, erasure or suppression of computer data or computer programs, or other interference with the course of data processing in a manner or under such conditions which would, according to national law, constitute an offence of forgery if it had been committed with respect to a traditional object of such an offence."

Its purpose is to criminalize forgery with respect to computer data, in a manner functionally equivalent to criminalization of the forgery of conventional documents.

20. Two other types of related crime should be mentioned here. The first concerns a number of forms of deceit in relation to telecommunication services. In such cases, to obtain services without payment, the perpetrator attempts by means of technical manipulation of devices or electronic elements of the devices. Such conduct is usually criminalized by means of specific criminal provisions, but it can sometimes be subsumed under the classical provisions for deceit or forgery. The second group relates to the misuse of payment instruments. The perpetrator, by manipulating or forging an electronic banking card, or using false codes, attempts to make an illegal financial gain. This may be covered by specific criminal provisions or by classical fraud and forgery provisions, or amended in the sense described in paragraph 19.

21. Computer-assisted offences include making available, communicating and disseminating certain material, and sometimes merely being in possession of it. Such offences do not require electronic networks; here, networks are used by the perpetrator to increase the effect of the crime and to attempt to elude justice. With regard to content-related offences a distinction should be made between content that is illegal owing to its character or meaning, and content which is not necessarily illegal by itself, but becomes criminal under the circumstances of its distribution. The latter category includes infringement of copyright and sale of forbidden goods or services, such as weapons, drugs, stolen goods, unprescribed medicines and access to gambling facilities. The other category of content-related offences concerns messages that are defamatory, that entice subversion or other illegal activities or are offensive because of their religious or racially discriminatory nature or because of their pornographic nature. The extent to which national legislators have criminalized such behaviour varies considerably. In most cases, the offences have long been part of existing law, raising the question of whether the laws apply to the new electronic environment.

22. There is global agreement in attitudes and rules condemning the distribution of child pornography. International bodies, such as the United Nations Educational, Scientific and Cultural Organization and the European Union, have recommended that countries enact

criminal provisions where the distribution of such material is not already illegal. Many States are preparing or have enacted child pornography laws. National and international police authorities have also given high priority to the investigation of child pornography.

23. As regards offences that involve material relating to the incitement of hate or discrimination, for various reasons, there is less global consensus about whether the criminal laws should be used against expression or distribution. The situation may change as the awareness of the international community is raised about the negative effects of such behaviour.

24. The distribution of illegal materials has caused a discussion about the role and responsibilities of Internet service providers. Apart from a few legislative initiatives to define and to delineate the duties of care of providers, there is a tendency internationally as well as nationally, to give Internet service providers a legal status similar to that of traditional telecom operators. This means that Internet providers generally have no legal obligation to monitor or possibly block traffic that is transferred by means of their computer systems. Nevertheless, an Internet service provider generally is required to take all reasonable steps to prevent further distribution of illegal material once aware of its nature.[6] Other aspects of the application of domestic law to Internet service providers may also be unclear. This includes the extent of possible civil liability for the transmission of illegal content, and the extent to which an Internet service provider has an obligation to cooperate with law enforcement authorities by providing information for a particular criminal investigation or other assistance.

IV. Criminal investigations of cyber crime

25. As stated, cyber crime can be any crime committed by electronic means, or committed in part or entirely in an electronic environment. Criminal investigations in an electronic environment are directed against such crimes. Other crimes, however, can also leave traces or evidence in the electronic environment. Criminal investigations in electronic environments will therefore not be limited to cyber crime in the sense used in the previous chapter, but will encompass the investigation of any crime for which (potential) evidence needs to be secured in an electronic environment.

26. Criminal investigations in an electronic environment require technical expertise, appropriate procedures and sufficient legal authority. The 1989 and 1995 Recommendations of the Council of Europe (R (1989) 9 en R (95) 13) stressed the need for national law enforcement authorities to deploy specialized computer crime units. These units should be adequately staffed and provided with appropriate equipment and software tools. Training programmes should ensure the availability of trained personnel and with up-to-date technical knowledge. Many States have already created computer crime units of this kind. A number have produced manuals with technical, forensic and procedural instructions on how an investigation should be carried out to reduce loss of evidence and to secure its admissibility in court.

27. Some national police units "patrol" the Internet and specific software tools have been developed to detect crimes such as hacking or distributing child pornography. The European Union partly funded the development by Swedish police of software to trace child pornography (see <http://www.techweb.com>). Given the enormous amount of information available in international computer networks, the development of software tools such as those based on pattern recognition seems indispensable.

28. There are two methods of obtaining data from a computer system, based on technical and legal criteria. In the first, data are obtained as part of a search of premises or the place where the system is located. The second involves the interception or monitoring of data transmitted from, to or within the system. Legal powers for searching premises are not discussed here. It is assumed that the legal powers will encompass the authority to search a computer system at a given location. Interception may be done by technical means from the outside of a system or by means of elements incorporated within the system for that purpose.

29. Generally, traditional criminal procedural law provides for the seizure and freezing of entire computer systems, as it provides for any other evidence. Where this is not feasible, however, there may not be adequate legal powers to investigate the content of a computer system against the will of the right holder(s). The seizure of an entire computer system may not be technically feasible, or it may be disproportionate owing to a multi-user environment and a multi-user interest in the data content. Attempts to secure data for particular investigations may find traditional powers insufficient owing to: (a) problems related to obtaining access to the computer system; (b) the

intangible nature of data; and (c) the fact that data may be stored in a connected system, located outside the premises searched.

30. If a computer system is found at searched premises, the law generally permits law enforcement authorities to gain access to it and inspect its content. This will be possible if the system is already running, the person concerned opens it voluntarily or a means of access is found on the premises. When none of these circumstances occurs, the question is whether the law provides the right to enable law enforcement authorities to gain access to the system against the will of the individual concerned.

31. Computer systems, programs or data files may be secured in order to prevent unauthorized access. Access is then usually gained by identification and authentication procedures, whereby the user provides a password—manually, embedded in a chip card, or both—or has to allow the checking of biometrical marks. Security of data usually involves encryption, which provides for authentication and protects confidentiality, and which involves the use of an encryption algorithm and one or more keys. It raises the serious risk that, without the voluntary assistance of the system keeper or the entitled person, no access will be obtained to the computer system or the data being sought. Some laws, therefore, require system keepers to allow access to the system or the data, punishing non-compliance by using contempt of court rules. Such laws may not apply where a system operator is also the suspect of the crime, however, because this would violate rules or principles against self-incrimination. Individuals who have other legal reasons not to cooperate, such as being related to the suspect or those who have professional obligations to keep secrets, may also be exempt. In some cases, if there is no one present to whom an order to assist can be given, any other person (usually an external expert) may be ordered to assist. Allowing mere access to the data may not be sufficient if it is encrypted. In such cases, laws may compel further cooperation to transform the data into a readable format.

32. Data as such are intangible, so traditional powers of seizure generally do not apply. In the course of a criminal investigation, tangible objects will either be seized and taken away, or measures will be taken to ensure that no one except the investigating authorities can dispose of the objects. With data, it is usually sufficient to make a copy. Additional steps are required, however, where data are hazardous, illegal or valuable, or where there is a possibility of further harm to victims or to the investigation. To deal with this, laws may provide powers allowing the investigating authority to erase data or prevent their further use. To protect the data, copying may be required in order to restore them to their original state when ordered by a judge. If the person concerned complains about the copying and further use of the data, the law could require the issue of an official statement about the data taken.

33. The search of a computer system will generally take place as part of a search of premises or places. The legal power to search is usually limited to the physical boundaries of the searched place. A computer network may not be located in one single place, but be connected with other parts of the network by means of fixed or switched communication lines. The question in such cases is whether the law allows searches in connected systems, when the systems are not located at the premises searched. Without an extended search, there is a risk that the data will be deleted before an additional search warrant can be obtained for the place where the data are physically located. In large networks, it may be practically impossible to establish the precise physical location of the data.

34. The following outlines the legal basis for an authority to conduct an extensive search. The person who resides at the premises to be searched is entitled to gain access to the connected computer system and to use its functions and storage capacity. He or she can control the data without the necessity of going elsewhere. When searched, this person is put under a legal obligation to submit to a search of the premises that are physically under his or her control. It can be argued that the same rules should apply to the data that the person in question has factual access to, even though they may be located elsewhere. It would follow that the scope of such an extended search would be limited to activities that the person in question is authorized to undertake with regard to the connected system and data, and that the individual's rights are not infringed to any greater degree than permitted by the basic search. It would be possible to restrict such powers to investigations of serious crimes or to cases where immediate action is required in order to prevent the loss of evidence, or both. Other limitations might apply when the connected system or data sought is located in a foreign jurisdiction (see para. 59 below).

35. The searching and selection of data in a computer system raises a number of additional legal problems. The first is how specific the judicial order needs to be about the nature and format of the data sought in order to be lawful.

National laws may impose different restricting conditions here. In addition, the faithful and precise execution of the judicial order may take a disproportionate amount of time, leading law enforcement authorities to make a copy of as much data as seems relevant for later analysis. National laws may or may not allow such a practice. Another important question is whether the person concerned should be informed about the data that are copied and taken away, how much detailed information should be provided and whether he or she should have a right to challenge the seizure legally. A further problem arises if data are under privilege or other legal protection. The question is how to identify and protect such data in cases where authorities copy large amounts of data for later examination.

36. In addition, it should be noted that data are of a volatile nature. They can be easily moved, erased or altered without clear traces remaining. Distributed data processing is not the only factor that makes data volatile. Electronic data processing involves the processing of large amounts of data of an ephemeral nature that are subject to erasure as soon as they are no longer necessary. Examples of such data are log files and communication traffic data. Without knowledge of the "original" data set (if the term has any meaning in data processing), it is difficult to detect manipulations and restoring deleted files will be impossible unless underlying back-up information was kept. The nature of data raises problems when physical searches are involved:

(a) The search for data, electronically stored or being transferred, in most cases needs to be carried out quickly and in a timely manner in order to prevent interference with the search or tampering with the data;

(b) Special precautions need to be taken in order to enable data to be presented as evidence in court. The integrity of the data must be established from the point of downloading or copying from the searched computer system to use in court.

37. The technical and legal distinctions between the seizure of stored data and the interception of data flowing through the network have also become blurred. Data are processed by means of a computer system, sometimes described as an automated data-processing device. Data processing includes input, transfer to peripheral equipment (e.g. video screen) and intermediate storage media, actual processing, transmission of the results to peripheral devices for storage and output or further transmission to other system components. Intercepting data in a computer system generally comes down to the search for stored data, to be carried out by making use of system functions or specific computer programs. Searching for data in transmission can be done by system facilities (monitoring), if provided for, or by technically intercepting the data flow somewhere in the transmission facilities. Since data are in many cases both stored and in transmission, or move frequently from one status to the other, it will often be possible for investigators to choose between seizure and interception to obtain the same data. This may raise legal concerns, because the standards or safeguards which apply to the interception of communcations and the seizure of stored materials are not the same in many States. The interception of data in transmission is often subject to a stricter standard because interception is a covert operation, it may target data that did not exist when the search was authorized or when it commenced and, in most cases, the parties concerned would not be aware of the interception and might not be informed of it, if at all, until long after it had taken place. The fact that network data can be either seized or intercepted may erode the rights of suspects in some cases, since it would allow law enforcement to apply less restrictive legal search powers to some operations that were more in the nature of interceptions.

38. Electronic data, copied from data files or registered from data flows, usually demand special precautions and measures in order to serve as evidence in court, if it may be used as such at all. In many justice systems, the principle of immediateness, that is, that all evidence should be presented in court, requires that the evidential material meet a very high standard. Some countries may have formal requirements that impede or prevent the use of electronic data as evidence. Some laws require that the material be in writing so that it can be read in court, for example. In some countries, data representing sound or images would not meet this condition and would therefore not be admissible. Any doubt about the reliability of evidential material will also generally make it inadmissible. Since electronic data can easily be modified without leaving traces, this puts a heavy burden on law enforcement authorities to gather such evidence according to transparent and secure procedures that enable them to establish its authenticity. To verify authenticity, the court must be able to review the reliability of the process of copying and registering the evidence from the original data carrier or data channel. It must also be able to test the validity of (a) the preservation procedure and security of the preservation itself; (b) any analysis of the material; and (c) whether the material presented in court matches the material originally seized and secured.

39. In addition to conventional powers to search premises, many national legal systems allow courts to make production orders for tangible objects. In some cases, parallel powers to order the production of specified data may also be provided. Such powers may be subject to restrictions and specific conditions that do not apply to conventional production orders, to prevent them from being used as a means to obtain information other than that specified. Without such controls, for example, an order could oblige an individual to collect, process or select any other kind of data that is not stored and under his or her control. Such an obligation would exceed the scope and meaning of a production order. When seeking and using production orders, it may be useful for law enforcement to include the log files of a computer system along with other data being sought. Such files register all transactions on the system in chronological order, recording information about such things as times, durations and terminals from which data were accessed or altered.

40. Under the traditional laws of many countries, it is possible for a judicial or other authority to order the interception and recording of telecommunications in public networks. Some countries have extended that authority to private networks, to specific new forms of telecommunications such as mobile systems or satellite communication systems and to computer networks. The rationale behind such legislative measures is that if communications can be intercepted in one network and not in another, criminals will use the system with the lowest risk of interception by law enforcement authorities. The lawful interception of specified communications requires particular technical facilities, including a clear legal basis for the installation of the facilities and the prompt execution of a judicial order to intercept.

41. To identify the communications to be intercepted and the persons engaged in an intercepted communication, the cooperation of operators of networks, such as telecom operators and Internet service providers, is indispensable. Only such operators have the necessary subscriber information. Where appropriate, national law may impose a legal obligation on operators and providers to give subscriber data promptly when so ordered by the competent authorities. Clear legal obligations of this kind should also protect individuals and companies from civil liability to their subscribers.

42. Telecom operators and Internet service providers usually have traffic data from past communications, generated by equipment that records details including the time, duration and date of any communication, the parties involved and the type of service or activity. (See the parallel to the example of the log file of a computer system in paragraph 37 above.) Such data are generally kept for a limited period of time, depending on the commercial needs of the operator or provider and legal (in the European Union) or commercial requirements for privacy protection. Many national laws allow law enforcement authorities or judicial authorities to order the collection of traffic data of future communications. In cases where traffic data is part of the communication, such as the "header information" of e-mail messages, however, the collection of such traffic data may be considered an interception of the communication itself and subject to legal restrictions on that basis. In other cases, the collection of traffic data without intercepting the contents of the communication itself may be deemed less intrusive to the privacy of those concerned and therefore subject to a lower legal threshold.

43. Cases of hacking or electronic intrusion raise a particular need for the prompt interception of an electronic communication, as well as prompt availability of traffic and subscriber data in order to track down the source of the communication, preserve the data and eventually catch the perpetrator in the act for evidential reasons. If criminalized, hacking may not be considered under some laws a crime serious enough to justify the application of interception measures. Generally, a hacking scheme involves other more serious acts than can be established at the time of detection of hacker activities. This may be seen as another reason to allow interception for electronic intrusion cases.

44. Interception of electronic communications may be hampered by the fact that the communication is encrypted. Encryption is used to allow the authentication of a message, identifying the sender and establishing the integrity of the message. A second function of encryption is to ensure the confidentiality of the message (by protecting it from third persons). Possible cryptography policies have been the subject of recent debate in a number of international organizations. Those interested in facilitating law enforcement and crime control are concerned about diffculties in gaining legal access to encrypted data, while those concerned about privacy and commercial interests want cryptography to protect personal and commercial information.

45. Much of the debate is beyond the scope of the present paper, but two specific issues do warrant consideration here. Some cryptography-producing countries have

considered controlling the proliferation of cryptography products in order to prevent criminal or terrorist groups from gaining access to them, using such things as licence requirements for products "strong" enough to make law enforcement access difficult. Some countries have also sought to apply practical measures in an attempt to ensure that legal access to electronic communications protected by encryption can still be gained. The measures include the use of special computer chips, key-escrow systems (in which message keys are kept by trusted third parties from whom they can be lawfully seized to gain access) or special efforts to break encrypted messages using technical means. Policies of this kind have encountered some difficulties with the technology and opposition from advocates of privacy rights and commercial interests.

46. Ensuring access to encrypted communications or stored data in the course of criminal investigations is understandably a matter of concern to law enforcement agencies worldwide. Measures that address this problem in part may already exist in some countries. In many cases, telecom and network operators will themselves apply encryption to protect their own systems and their customers' communications. Where those operators are under a legal obligation to cooperate with law enforcement authorities in the interception of a specified communication, it seems reasonable to assume that such an obligation includes (or could include) a duty to undo any encryption they applied to it. This would not extend to encryption applied directly by the customer, however, which would generally be impossible for the operator to decrypt. Another possibility is that national legislators consider obliging persons who participate in an encrypted communication to provide the means of decryption when so ordered by the competent judicial authority. To protect against self-incrimination, such an order could be made unavailable against suspects or other persons to whom a legal exemption applies.

47. As noted in paragraph 37 above, most countries make a distinction between the interception of flowing data and the seizure of stored data, but e-mail challenges this distinction, because it combines both data transfer and storage. When a message is sent, it is transmitted by the sender's service provider to the service provider of the addressee. Upon receipt, the latter stores the message in the mailbox of the addressee until it is opened. The addressee has access to the message and determines how long it will be preserved in the mailbox. Messages in the mailbox are thus under the control of both the addressee and the provider, and law enforcement could generally obtain access by applying coercive powers against either of them. Usually, they will prefer to do so against the Internet service provider, since this could be done without alerting the addressee to the existence of the investigation. In such cases, the legal powers to intercept a communication and to effect a physical search of premises and any computers located therein may effectively become interchangeable. In this context, the legality of a production order to hand over existing messages and messages that arrive within a certain period of time could be questioned unless it met the (usually higher) legal standards for interception. The fact that the data are under the control of the provider and customer simultaneously may also raise questions about whose privacy, property or other rights or interests must be addressed in gaining legal authorization to conduct a search or interception.

V. International cooperation among national law enforcement authorities

A. Forms of cooperation and international initiatives

48. Given the international dimension of electronic networks, it is becoming less likely that all elements of a cyber crime will be restricted to a single national territory. In investigations, law enforcement authorities of different States will need to cooperate, both formally, using mutual legal assistance frameworks and structures such as Interpol, and informally, by providing potentially useful information directly to the authorities of another State. In general, international police cooperation presupposes the consent of the authorities of the States involved. Depending on the relationship of the States involved, the nature of the information in question—or other factors—it may also require authorities and procedures set out in an international agreement.

49. In 1997, the Group of Eight, consisting of the heads of State or Government of the Group of Seven major industrialized countries and of the Russian Federation, adopted a number of legal principles and a common action plan against what it described as "high-tech crime".[7] They contain some proposals for practical cooperation among law enforcement authorities, as well as the development of legal principles concerning mutual legal assistance. Elements of practical cooperation discussed included:

(a) Measures to ensure the availability of a sufficient number of trained personnel with sufficient expertise by cooperation in the equipping and training of law enforcement personnel;

(b) Cooperation in developing forensic standards for the retrieval and authentication of electronic data.

50. In order to facilitate timely responses to a request for assistance from another State, the Group of Eight agreed to establish a system of contact points, available 24 hours a day and for 7 days a week ("24/7") which is now in place. The tasks of the contact points are very diverse. When requested, a contact point will provide factual information that may help expand the investigation to the other State or invoke its assistance, and take all other necessary measures in order to respond without delay to a formal request for legal assistance or take the preliminary measures, as permitted by national law, in awaiting such a request. The "24/7" contact points are not confined to the Group of Eight, but have also been established on a voluntary basis in many other States. In some countries, the creation of such specialist units may not be practicable because of lack of expertise or financial means. In other States, the fighting of cyber crime may have a lower priority. Obviously, the more States that train and equip personnel and make them available on the "24/7" basis, the more effective the system will become.

51. Within the framework of Interpol, several expert working groups on information technology crime have been established. The European Working Party on Information Technology Crime has developed a computer crime manual (available on CD-ROM). It contains instructions on how to investigate computer crime cases, a description of tools and techniques for searching and securing electronic material and information about the relevant substantive and procedural laws of different countries. Working parties are active in the development of specific software tools in order to detect specific crimes on the Internet. Several training courses for computer crime investigators have been held.

52. The United Nations manual on the prevention and control of computer-related crime aims at the harmonization of both substantive and procedural law, as well as international cooperation in combating computer-related crime. The manual contains a chapter on information security and prevention of cyber crime.[8]

53. Both coordinated approaches and those based on initiatives taken by an individual State have merit, and it is important to maximize the benefits of both. In this context, it is important that international meetings are organized on a regular basis for cyber crime units to meet and exchange practical information and experience. Other permanent facilities, such as data banks, web sites and discussion groups will contribute to a better exchange of information.[9]

54. A third element of the action plan of the Group of Eight is the coordination of cooperation between industry and the State. It involves:

(a) Encouraging standard-setting bodies to develop standards for reliable and secure telecommunications and data-processing technologies;

(b) Developing information and telecommunications systems capable of detecting network abuse, tracing the perpetrator and collecting relevant evidence.

Since criminal investigations in computer environments may burden industry, cooperation and coordination with industry is important and necessary. This involves many issues, from information security and product development to factual cooperation in the execution of judicial orders. The negotiations between Government industrial organizations may take the form of sectoral arrangements or other non-binding or enforceable agreements.

B. Mutual legal assistance and other international treaties

55. International cooperation in the form of mutual legal assistance requires an international agreement or other similar arrangement such as reciprocal legislation. Such provisions, whether multilateral or bilateral, oblige the authorities of a contracting party to respond to a request for mutual legal assistance in the agreed cases. The execution of such a request can take place only if it is consistent with the domestic law of the requested State or, lacking specific rules, insofar as it is not a violation of that law.

56. States cooperate in criminal matters more effectively if they share a common interest, as reflected in the mutual criminal statutes or codes and in the way the criminal law is enforced in the States concerned. In many international conventions on criminal matters, the common interest is embodied in the rule of dual criminality. A State cannot cooperate with another State concerning the investigation and prosecution of certain acts that are not criminalized in the requested State. In older conventions, the lack of dual criminality, therefore, is a valid basis for refusing

assistance. More recent conventions do not raise such a formal condition, but contain a criterion of reasonability. It may be considered unreasonable to comply with a request for legal assistance if, for example, the crime involved is a minor offence or concerns certain conduct that is not criminal in the requested State.

57. One way to improve international cooperation in criminal matters, therefore, is the harmonization of certain substantive criminal law provisions. Cultural, social and economic divergences among States may lead to different criminal policies. In that respect, international deliberations directed at harmonizing "confidentiality, integrity, availability" offences (see para. 15), such as technology-oriented provisions, may be less complicated than the intended harmonization of content-related offences, because of their impact on human rights (such as freedom of expression). Child pornography, concerning which there exists a broad consensus for control, seems to be the exception that proves the rule.

58. Mutual legal assistance refers here to any form of legal assistance. Such assistance generally relates to specific coercive powers concerning the investigation of cyber crime. Apart from requests for traditional help, such as interviewing witnesses, its purpose is to obtain certain data stored in a computer system that is located in the territory of another State or being transferred electronically through a network and capable of being monitored or intercepted in the territory of that State.

59. States determine in their domestic law which of their powers can be applied in the assistance of other signatory States. They may not necessarily offer all their domestic powers on behalf of the investigation of criminal cases by other signatories. In some cases assistance may be made available in a specific case, given the mutual interests of the States involved, that would not be made available on a regular or routine basis. Mutual legal assistance, as a part of international law, is also ultimately governed by the principle of reciprocity. For this and other reasons, States negotiating the scope of mutual legal assistance with other States may be hesitant to go as far as domestic law would allow. Dual criminality—the requirement that an offence in respect of which assistance is sought must be a crime in both States involved—may also be invoked directly or indirectly as a ground for refusal of mutual legal assistance. In addition, international agreements to provide mutual assistance may contain exceptions where it will not be given. Common exclusions are certain types of offences, such as fiscal, political or military crimes, and crimes that are not seen as sufficiently serious (as assessed by the potential punishments involved) to warrant the effort.

60. Additional problems may arise with respect to legal assistance in the investigation of international cyber crime. If a party has not provided specific powers to search for evidence in electronic environments under domestic law, it may not be able to respond (or to respond adequately) to a request for assistance. For this reason, the harmonization of coercive powers is an important condition for international cooperation.

61. Mutual legal assistance is also more likely to be urgent in cases of cyber crime than in conventional investigations because of the potential loss of electronic evidence if it is not secured quickly. Immediate action may not always be possible for formal and practical reasons, however. The necessary action may require a judicial order in the requested State, for example. In order to avoid the loss of evidence in such cases, a system of fast preliminary action could be developed, requiring as little formality as possible, followed by more conventional proceedings once the evidence had been secured in order to determine whether it should be turned over to the requesting State. Under such a system, domestic law would permit both securing data in response to an informal request and preserving it while awaiting a formal request for its disclosure under the mutual legal assistance arrangement. If no such request was received in due time or if such a request was rejected as inadequate, the secured data would be deleted. A similar system is possible with regard to the preservation of traffic data held by telecommunications operators and Internet service providers.

62. International computer networks make it possible for activities to be undertaken in a particular territory that may (deliberately or inadvertently) have extraterritorial effects. For example, law enforcement authorities in one State might obtain data from a computer network as part of a lawful computer search in that State, only to find that some of the data obtained had been stored in a part of the network in another State and protected by the laws of that State. Similarly, a State might legally intercept electronic communications that are passing through its territory, even though the communications are between persons located in other jurisdictions where they enjoy the legal protection of that State against arbitrary interference with private communications. Law enforcement officers operating on a network could also be acting as undercover agents in compliance with the laws of their own jurisdiction in circumstances where their actions or the methods they

employed were not permitted by the laws of other jurisdictions in which they were operating. All of these scenarios are new and without parallel, and international law does not at present provide much assistance or guidance in resolving the issues involved.

63. There is also, at present, no broad consensus about possible solutions to the transborder effects of lawfully applied domestic investigative measures. It is generally recognized that a State is legally authorized to apply investigative measures or coercive powers against any of its citizens, within its own territory, over which it has exclusive jurisdiction. The application of those powers may result in cases where data located elsewhere are searched and copied, or possibly deleted. From the perspective of the searched State, this may constitute a criminal act according to domestic criminal law and a violation of national sovereignty. Another view, however, is that international law does not forbid such an intervention, because the data are technically accessible and available from the searching State without any assistance or intervention by the searched State. Data present anywhere in a network could be considered ubiquitous and, for that reason, access to them from any State in which they are present would be a question of purely domestic, not international, law. From this point of view, it would not be necessary to involve the searched State at any stage. The extent to which data are or are not ubiquitous (searchers must actively download them from one jurisdiction to another, for example) continues to raise questions in international law.

64. With regard to the view that any interference in a computer network located in the territory of a State represents a violation of the territorial sovereignty of that State, it is useful to consider two different opinions about the state of international law. One view is based on the principle that States should not be allowed to search, copy or otherwise interfere with data or computer systems located in another State unilaterally, on the same basis that doing the same things by a unilateral physical presence there would not be allowed. To obtain evidential data from another State, standing mutual legal assistance procedures should be followed. This follows traditional principles, but may not recognize the practical problems of investigating computer crime.

65. A more pragmatic view advanced by some is that international law does not at present provide clear answers to questions of violation of national laws or infringement of sovereignty. Those who take this position argue that international law can be shaped by the emergence of international consensus that such activities should be permitted and by clearly defining the conditions under which they would be permitted. Notification of the searched State is suggested as an important element of such a solution.

66. The international community could come up with new concepts to establish a legal rule on how to define the rights of States concerning the shared use of terrestrial, mobile or satellite computer networks. In the meantime, a pragmatic approach could be agreed to in the form of a treaty or other international instrument on certain procedures by which the interests of the searching State can be properly balanced against the interests of the searched State and its residents.

VI. Conclusion

67. The increasing occurrence of computer-related crime, facilitated by the establishment of global international and public electronic networks, has made international coordination and cooperation in this area essential. The major elements of such international action could be based on the following principles:

(a) *Raising awareness with the public.* Public education and awareness may reduce the number of crimes in the electronic environment. Industry—hardware and software manufacturers, service providers and others—consumer organizations and Governments may perform a common task of informing the public about security and other risks of open electronic environments and provide them with suggestions about how to protect their interests;

(b) *Moving toward a common policy on cyber crime.* The transnational nature of network crime suggests that the development of common policies on key issues should be part of any control strategy. Such common policies are important to prevent the occurrence of "data havens" in jurisdictions where certain activities have not been criminalized, for example. The development of common policies could be an aspect of the United Nations Crime Prevention and Criminal Justice Programme, in support of the work already undertaken by international organizations;

(c) *Improving investigative measures.* Effective measures could be pursued for improving criminal investigative capabilities in network environments,

particularly in cases involving multiple jurisdictions. This includes responding to the need for operations that could be conducted quickly enough to prevent the loss or inaccessibility of evidence. Searching computer systems and surveillance of computer networks may require additional powers not found at present in traditional criminal procedural law. The amounts of data found on computer systems and the ease with which they can be accessed by searchers also raise significant privacy and related issues. The human rights of the individuals concerned must be carefully considered and balanced, both in developing new legal powers and in the execution of those powers;

(d) The investigation of cyber crime requires the availability of staff with particular forensic and technical expertise and for specific procedures to be in place. This implies the formulation of training programmes and the development of investigative software tools. International training programmes should be developed and expertise should be shared between States. The United Nations, within the framework of the United Nations Crime Prevention and Criminal Justice Programme, could study the desirability of reviewing its manual on computer crime and further support the work already undertaken by other international organizations;

(e) *Improving cross-border coordination and assistance.* Cyber crimes will be committed in global electronic environments and will not necessarily be restricted to the territory of a particular State. In order to investigate effectively, States may therefore be dependent on assistance from other States. This includes both informal cooperation by law enforcement personnel and formal mutual legal assistance conducted through central authorities. The fact that data in computer networks may be volatile makes the ability to provide such assistance quickly and effectively more important than for many other offences. Effective assistance in cases involving cyber crime would be supported by the following actions:

(i) The establishment of contact points similar to those set up by the Group of Eight in order to advise requesting States about the assistance that can be given and in order to initiate the measures necessary to fulfil requests as permitted under domestic law;

(ii) The review of legal assistance systems in the context of cyber crime. There is a need to examine conventional legal assistance requirements and practices to determine whether they meet the needs of modern cyber crime investigation and to identify possible improvements. Areas that might be examined include the general adequacy of powers to execute criminal investigations in computer networks and the possibility of taking expeditious measures in order to secure data on behalf of the criminal investigations of other States.

Notes

[1] Examples of associations or societies include the United States Internet Providers Association (USIPA), the Canadian Association of Internet Providers (CAIP) and the pan-European association of the Internet service providers associations of the countries of the European Union (EuroISPA). National associations exist in some European countries including Belgium, France, Germany, Italy, the Netherlands, Spain and the United Kingdom of Great Britain and Northern Ireland.

[2] http://www.nua.ie/surveys/how-many-online, 18 October 1999.

[3] See the technical International Organization for Standardization definitions of data.

[4] *Computer-Related Crime: Analysis of Legal Policy*, ICCP Series No. 10, 1986.

[5] Council of Europe (1989), Recommendation No. R (89) 9.

[6] "Global Information Networks: Realising the Potential", Ministerial Conference, Bonn, July 1997.

[7] See the Communiqué of the Meeting of the Justice and Interior Ministers of The Eight, Washington, 9-10 December 1997, http://www.usdoj.gov/criminal/cybercrime/communique.htm. The action plan was endorsed by the heads of State or Government in 1998. The action plan has been recommended to other international organizations such as the Organisation of American States and the European Union.

[8] *International Review of Criminal Policy*, Nos. 43 and 44, 1994 (United Nations publication, Sales No. E.94.IV.5).

[9] Such as the World Justice Information Network <http://www.justinfo.net> or the Police Officer Internet Directory <http://www.officer.com/c_crimes.htm>.