

دليل الامم المتحدة الارشادي بشأن الجرائم المرتبطة بالكمبيوتر لعام 1994  
منقحا ومعدلا كما في عام 2001 .

## United Nations Manual on the prevention and control of computer-related crime

The burgeoning of the world of information technologies has, however, a negative side: it has opened the door to antisocial and criminal behavior in ways that would never have previously been possible. Computer systems offer some new and highly sophisticated opportunities for law-breaking, and they create the potential to commit traditional types of crimes in non-traditional ways. In addition to suffering the economic consequences of [computer crime](#), society relies on computerized systems for almost everything in life, from air, train and bus traffic control to medical service coordination and national security. Even a small glitch in the operation of these systems can put human lives in danger. Society's dependence on computer systems, therefore, has a profound human dimension. The rapid transnational expansion of large-scale computer networks and the ability to access many systems through regular telephone lines increases the vulnerability of these systems and the opportunity for misuse or criminal activity. The consequences of computer crime may have serious economic costs as well as serious costs in terms of human security.

---

### CONTENTS

---

#### [Introduction](#)

#### [The international problem](#)

#### [Regional action](#)

#### [The need for global action](#)

#### [Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders](#)

### [THE PHENOMENON OF COMPUTER CRIME](#)

#### [Definition of computer crime](#)

#### [The extent of crime and losses](#)

#### [Perpetrators of computer crime](#)

#### [The vulnerability of computer systems to crime](#)

#### [Common types of computer crime](#)

### [SUBSTANTIVE CRIMINAL LAW PROTECTING THE HOLDER OF DATA AND INFORMATION](#)

#### [Background](#)

#### [The development of national law](#)

#### [The international harmonization of criminal law](#)

### [SUBSTANTIVE CRIMINAL LAW PROTECTING PRIVACY](#)

#### [Background](#)

#### [The development of national law](#)

#### [International harmonization](#)

### [PROCEDURAL LAW](#)

#### [Background](#)

#### [The coercive powers of prosecuting authorities](#)

#### [Specific problems with personal data](#)

#### [Admissibility of computer generated evidence](#)

#### [International harmonization](#)

### [CRIME PREVENTION IN THE COMPUTER ENVIRONMENT](#)

#### [Security in the electronic data processing environment](#)

[Assets](#)  
[Security measures](#)  
[Law enforcement and legal training](#)  
[Victim cooperation in reporting computer crime](#)  
[Developing a computer ethic](#)  
[International security of information systems](#)  
[INTERNATIONAL COOPERATION](#)  
[General aspects](#)  
[The jurisdiction issue](#)  
[Transborder search of computer data banks](#)  
[Mutual assistance in transborder computer related crime](#)  
[Extradition](#)  
[Transfer of proceedings in criminal matters](#)  
[Concluding remarks and suggestions](#)  
[CONCLUSION](#)

---

## Introduction

---

1. When future historians scrutinize the second half of the twentieth century, they will be reviewing what is sure to be known as the Information Revolution. Humankind has progressed further in the last 50 years than in any other period of history. One of the reasons for this rapid advance in technology is the computer. Technological capabilities have increased at an accelerating pace, permitting ever larger and more sophisticated systems to be conceived and allowing ever more sensitive and critical functions to be assigned to them.<sup>1</sup>

2. Indeed, the world is undergoing a second Industrial Revolution. Information technology today touches every aspect of life, irrespective of location on the globe. Everyone's daily activities are affected in form, content and time by the computer. Businesses, Governments and individuals all receive the benefits of this Information Revolution. While providing tangible benefits in time and money, the computer has also had an impact on everyday life, as computerized routines replace mundane human tasks.<sup>2</sup> More and more of our businesses, industries, economies, hospitals and Governments are becoming dependent on computers. Computers are not only used extensively to perform the industrial and economic functions of society but are also used to perform many functions upon which human life itself depends. medical treatment and air traffic control are but two examples. Computers are also used to store confidential data of a political, social, economic or personal nature. They assist in the improvement of economies and of living conditions in all countries. Communications, organizational functioning and scientific and industrial progress have developed so rapidly with computer technology that our form of living has changed irreversibly.

3. With the computer, the heretofore impossible has now become possible. The computer has allowed large volumes of data to be reduced to high-density, compact storage, nearly imperceptible to the human senses. It has allowed an exponential increase in speed, and even the most complex calculations can be completed in milliseconds. The miniaturization of processors has permitted worldwide connectivity and communication. Computer literacy continues to grow.

4. The burgeoning of the world of information technologies has, however, a negative side: it has opened the door to antisocial and criminal behavior in ways that would never have previously been possible. Computer systems offer some new and highly sophisticated opportunities for law-breaking, and they create the potential to commit traditional types of crimes in non-traditional ways. In addition to suffering the economic consequences of computer crime, society relies on computerized systems for almost everything in life, from air, train and bus traffic control to medical service coordination and national security. Even a small glitch in the operation of these systems can put human lives in danger. Society's dependence on computer systems, therefore, has a profound human dimension. The rapid transnational expansion of large-scale computer networks and the ability to access many systems through regular telephone lines increases the vulnerability of these systems and the

opportunity for misuse or criminal activity. The consequences of computer crime may have serious economic costs as well as serious costs in terms of human security.

---

#### A. The international problem

5. Laws, criminal justice systems and international cooperation have not kept pace with technological change. Only a few countries have adequate laws to address the problem, and of these, not one has resolved all of the legal, enforcement and prevention problems.

6. When the issue is elevated to the international scene, the problems and inadequacies are magnified. Computer crime is a new form of transnational crime and effectively addressing it requires concerted international cooperation. This can only happen, however, if there is a common framework for understanding what the problem is and what solutions there may be.

7. Some of the problems surrounding international cooperation in the area of computer crime and criminal law can be summarized as follows:

The lack of global consensus on what types of conduct should constitute a computer-related crime;

The lack of global consensus on the legal definition of criminal conduct;

The lack of expertise on the part of police, prosecutors and the courts in this field;

The inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers to intangibles such as computerized data;

The lack of harmonization between the different national procedural laws concerning the investigation of computer-related crimes;

The transnational character of many computer crimes;

The lack of extradition and mutual assistance treaties and of synchronized law enforcement mechanisms that would permit international cooperation, or the inability of existing treaties to take into account the dynamics and special requirements of computer-crime investigation.

---

#### B. Regional action

8. Examination of these questions has already occurred to some degree at the international and regional levels. In particular, the Organisation for Economic Co-operation and Development (OECD) and the Council of Europe have produced guidelines for policy makers and legislators.

9. In 1983, OECD undertook a study of the possibility of an international application and harmonization of criminal laws to address the problem of computer crime or abuse. In 1986, it published *Computer-Related Crime: Analysis of Legal Policy*, a report that surveyed the existing laws and proposals for reform in a number of Member States and recommended a minimum list of abuses that countries should consider prohibiting and penalizing by criminal laws, for example, computer fraud and forgery, the alteration of computer programs and data and the copyright and interception of the communications or other functions of a computer or telecommunication system. A majority of members of the Committee on Information, Computer and Communications Policy also recommended that criminal protections should be developed for other types of abuse, including the theft of trade secrets and unauthorized access to, or use of, computer systems.

10. Following the completion of the OECD report, the Council of Europe initiated its own study of this issue with a view to developing guidelines to assist legislators in determining what conduct should be prohibited by the criminal law and how this should be achieved, having regard for the conflict of interest between civil liberties and the need for protection. The minimum list of OECD was expanded considerably by adding other types of abuses that were recommended as deserving of the application of the criminal law. The Select Committee of Experts on Computer-Related Crime of the Committee on Crime Problems examining these questions also addresses other areas, such as privacy protection, victims, prevention, procedural issues such as the international search and seizure of data banks, and international cooperation in the investigation and prosecution of computer crime. Recommendation R(89)9 of the Council of Europe on computer-related crime, which contains guidelines for national legislatures, was adopted by the Committee of Ministers of the Council of Europe on 13 September 1989.

11. In 1992, OECD developed a set of guidelines for the security of information systems, which is intended to provide a foundation on which States and the private sector may construct a framework for the security of information systems. In that same year, the Council of Europe began a study that will concentrate on procedural and international cooperation issues related to computer crime and information technology.

---

#### C. The need for global action

12. Despite these international efforts, much remains to be accomplished in order to achieve international cooperation. While much of the international work has so far been centered in western European and OECD countries, the potential extent of computer crime is as broad as the extent of the international telecommunication systems. All regions of the world must become involved in order to prevent this new form of criminality.

13. Ensuring the integrity of computer systems is a challenge facing both developed and developing countries. It is predicted that within the next decade, it will be necessary for developing nations to experience significant technological growth in order to become economically self-sufficient and more competitive in world markets. As dependence on computer technology grows in all nations, it will be crucial to ensure that the rate of technological dependence does not outstrip the rate at which the corresponding social, legal and political frameworks are developing. It is important to plan for security and crime prevention at the same time that computer technology is being implemented.

14. The participation of both developed and developing nations in international computer-crime initiatives is an encouraging trend. For example, the three associated conferences on computer crime at Würzburg in October 1992 were attended by delegates from Africa, Asia, eastern and western Europe, Latin America, the Middle East and North America. An adequate response to computer crime requires that both developed and developing nations should encourage regional and international organizations to examine the issue and promote crime prevention programs on a national level.

15. This strategy is necessary, both immediately and in the long term, to ensure international cooperation and to foster the political will to create a secure information community and the universal criminalization of computer crime.

---

#### D. Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders

16. Following the Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders, which took place in 1985, the Secretary-General prepared a report entitled "Proposals for concerted international action against forms of crime identified in the Milan Plan of Action" (E/AC.57/1988/16). Computer crime was discussed in paragraphs 42-44 of that report.

17. In preparation for the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, the Asia and Pacific Regional Preparatory Meeting indicated concern with the effects of technological progress, as reflected in computer crimes (A/CONF.144/RPM.2).

18. At the 12th plenary meeting of the Eighth Congress, which took place in 1990, the representative of Canada introduced a draft resolution on computer-related crimes on behalf of the 21 sponsors. At its 13th plenary meeting, the Congress adopted the resolution, in which it, inter alia, called upon Member States to intensify their efforts to combat computer crime by considering, if necessary, the following measures:

"Modernization of national criminal laws and procedures, including measures to:

Ensure that existing offences and laws concerning investigative powers and admissibility of evidence in judicial proceedings adequately apply and, if necessary, make appropriate changes;

In the absence of laws that adequately apply, create offences and investigative and evidentiary procedures, where necessary, to deal with this novel and sophisticated form of criminal activity;

Provide for the forfeiture or restitution of illegally acquired assets resulting from the commission of computer-related crimes;

Improvement of computer security and prevention measures, taking into account the problems related to the protection of privacy, the respect for human rights and fundamental freedoms and any regulatory mechanisms pertaining to computer usage;

Adoption of measures to sensitize the public, the judiciary and law enforcement agencies to the problem and the importance of preventing computer-related crimes;

Adoption of adequate training measures for judges, officials and agencies responsible for the prevention, investigation, prosecution and adjudication of economic and computer-related crimes;

Elaboration, in collaboration with interested organizations, of rules of ethics in the use of computers and the teaching of these rules as part of the curriculum and training in informatics;

Adoption of policies for the victims of computer-related crimes which are consistent with the United Nations Declaration of Basic Principles of Justice for Victims of Crime and Abuse of Power, including the restitution of illegally obtained assets, and measures to encourage victims to report such crimes to the appropriate authorities." 5

19. In its resolution, the Eighth Congress also recommended that the Committee on Crime Prevention and Control should promote international efforts in the development and dissemination of a comprehensive framework of guidelines and standards that would assist Member States in dealing with computer-related crime and that it should initiate and develop further research and analysis in order to find new ways in which Member States may deal with the problem of computer-related crime in the future. It also recommended that these issues should be considered by an ad hoc meeting of experts and requested the Secretary-General to consider the publication of a technical publication on the prevention and prosecution of computer-related crime.

---

## I. The Phenomenon of Computer Crime

---

### A. Definition of computer crime

20. It is difficult to determine when the first crime involving a computer actually occurred. The computer has been around in some form since the abacus, which is known to have existed in 3500 B.C. in Japan, China and India. In 1801 profit motives encouraged Joseph Jacquard, a textile manufacturer in France, to design the forerunner of the computer card. This device allowed the repetition of a series of steps in the weaving of special fabrics. So concerned were Jacquard's employees with the threat to their traditional employment and livelihood that acts of sabotage were committed to discourage Mr. Jacquard from further use of the new technology. A computer crime had been committed.

21. There has been a great deal of debate among experts on just what constitutes a computer crime or a computer-related crime. Even after several years, there is no internationally recognized definition of those terms. Indeed, throughout this Manual the terms computer crime and computer-related crime will be used interchangeably. There is no doubt among the authors and experts who have attempted to arrive at definitions of computer crime that the phenomenon exists. However, the definitions that have been produced tend to relate to the study for which they were written. The intent of authors to be precise about the scope and use of particular definitions means, however, that using these definitions out of their intended context often creates inaccuracies. A global definition of computer crime has not been achieved; rather, functional definitions have been the norm.

22. Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are generally subject everywhere to criminal sanctions. The computer has also created a host of potentially new misuses or abuses that may, or should, be criminal as well.

23. In 1989, expanding on work that had been undertaken by OECD, the European Committee on Crime Problems of the Council of Europe produced a set of guidelines for national legislators that enumerated activities that should be subject to criminal sanction. By

discussing the functional characteristics of target activities, the Committee did not attempt a formal definition of computer crime but left individual countries to adapt the functional classification to their particular legal systems and historical traditions.

24. The terms "computer misuse" and "computer abuse" are also used frequently, but they have significantly different implications. Criminal law recognizes the concepts of unlawful or fraudulent intent and of claim of right; thus, any criminal laws that relate to computer crime would need to distinguish between accidental misuse of a computer system, negligent misuse of a computer system and intended, unauthorized access to or misuse of a computer system, amounting to computer abuse. Annoying behavior must be distinguished from criminal behavior in law.

25. In relation to the issue of intent, the principle of claim of right also informs the determination of criminal behavior. For example, an employee who has received a password from an employer, without direction as to whether a particular database can be accessed, is unlikely to be considered guilty of a crime if he or she accesses that database. However, the principle of claim of right would not apply to the same employee who steals a password from a colleague to access that same database, knowing his or her access is unauthorized; this employee would be behaving in a criminal manner.

26. A distinction must be made between what is unethical and what is illegal; the legal response to the problem must be proportional to the activity that is alleged. It is only when the behavior is determined to be truly criminal that criminal prohibition and prosecution should be sought. The criminal law, therefore, should be employed and implemented with restraint.

---

#### B. The extent of crime and losses

27. Only a small portion of crimes come to the attention of the law enforcement authorities. In his book *Computer Security*, J. Carroll states that "computer crime may be the subject of the biggest cover-up since Watergate". While it is possible to give an accurate description of the various types of computer offences committed, it has proved difficult to give an accurate, reliable overview of the extent of losses and the actual number of criminal offences. At its Colloquium on Computer Crimes and Other Crimes against Information Technology, held at Würzburg, Germany, from 5 to 8 October 1992, AIDP released a report on computer crime based on reports of its member countries that estimated that only 5 per cent of computer crime was reported to law enforcement authorities.

28. The number of verifiable computer crimes is not, therefore, very high. This fact notwithstanding, authorities point out that the evidence of computer crime discernible from official statistical sources, studies and surveys indicates the phenomenon should be taken seriously.

29. The American Bar Association conducted a survey in 1987: of 300 corporations and government agencies, 72 claimed to have been the victim of computer-related crime in the 12-month period prior to the survey, sustaining losses estimated to range from \$ 145 million to \$ 730 million. In 1991, a survey of security incidents involving computer-related crime was conducted at 3,000 Virtual Address Extension (VAX) sites in Canada, Europe and the United States of America. Seventy-two per cent of the respondents said that a security incident had occurred within the previous 12-month period; 43 per cent indicated that the security incident they had sustained had been a criminal offence. A further 8 per cent were uncertain whether they had sustained a security incident. Similar surveys conducted around the world report significant and widespread abuse and loss.

30. Law enforcement officials indicate from their experience that recorded computer crime statistics do not represent the actual number of offences; the term "dark figure", used by criminologists to refer to unreported crime, has been applied to undiscovered computer crimes. The invisibility of computer crimes is based on several factors. First, sophisticated technology, that is, the immense, compact storage capacity of the computer and the speed with which computers function, ensures that computer crime is very difficult to detect. In contrast to most traditional areas of crime, unknowing victims are often informed after the fact by law enforcement officials that they have sustained a computer crime. Secondly, investigating officials often do not have sufficient training to deal with problems in the

complex environment of data processing. Thirdly, many victims do not have a contingency plan for responding to incidents of computer crime, and they may even fail to acknowledge that a security problem exists.

31. An additional cause of the dark figure is the reluctance of victims to report computer offences once they have been discovered. In the business sector, this reluctance is related to two concerns. Some victims may be unwilling to divulge information about their operations for fear of adverse publicity, public embarrassment or loss of goodwill. Other victims fear the loss of investor or public confidence and the resulting economic consequences. Some experts have suggested that these factors have a significant impact on the detection of computer crime.

---

### C. Perpetrators of computer crime

32. History has shown that computer crime is committed by a broad range of persons: students, amateurs, terrorists and members of organized crime groups. What distinguishes them is the nature of the crime committed. The individual who accesses a computer system without further criminal intent is much different from the employee of a financial institution who skims funds from customer accounts.

33. The typical skill level of the computer criminal is a topic of controversy. Some claim that skill level is not an indicator of a computer criminal, while others claim that potential computer criminals are bright, eager, highly motivated subjects willing to accept a technological challenge, characteristics that are also highly desirable in an employee in the data-processing field.

34. It is true that computer criminal behavior cuts across a wide spectrum of society, with the age of offenders ranging from 10 to 60 years and their skill level ranging from novice to professional. Computer criminals, therefore, are often otherwise average persons rather than supercriminals possessing unique abilities and talents. 8 Any person of any age with a modicum of skill, motivated by the technical challenge, by the potential for gain, notoriety or revenge, or by the promotion of ideological beliefs, is a potential computer criminal.

35. According to a number of studies, however, employees represent the largest threat, and indeed computer crime has often been referred to as an insider crime. One study estimated that 90 per cent of economic computer crimes were committed by employees of the victimized companies. A recent survey in North America and Europe indicated that 73 per cent of the risk to computer security was attributable to internal sources and only 23 per cent to external criminal activity.

36. As advances continue to be made in remote data processing, the threat from external sources will probably increase. With the increasing connectedness of systems and the adoption of more user-friendly software, the sociological profile of the computer offender may change.

37. Owing to the greater complexity of certain computer routines and augmented security measures, it is becoming increasingly unlikely that any one person will possess all the information needed to use a computer system for criminal purposes. Organized computer criminal groups, composed of members from all over the world, are beginning to emerge. Corresponding with this increasing cooperation in criminal activity, the escalating underground use of electronic bulletin boards for clandestine criminal communication has been detected around the world. Rapidly improving telecommunication technology has added to the threat from external sources. Computer-based voice mailbox systems, for example, are being used by the computer criminal community to exchange stolen access numbers, passwords and software.

38. The advent of viruses and similar mechanisms whereby computer software can be made to act almost on its own initiative poses a new and significant threat. Sophisticated viruses and devices such as "logic bombs" and "trojan horses", discussed below, can be targeted for specific objectives at specific industries to commit a variety of traditional criminal offences, from mere mischief of extortion. These crimes, furthermore, can be committed immediately or can be planted to spring at a future date.

39. Computer criminals have gained notoriety in the media and appear to have gained more social acceptability than traditional criminals. The suggestion that the computer criminal is a less harmful individual, however, ignores the obvious. The current threat is real. The future threat will be directly proportional to the advances made in computer technology.

---

D. The vulnerability of computer systems to crime

40. Historically, economic value has been placed on visible and tangible assets. With the increasing appreciation that intangible data can possess economic value, they have become an economic asset that can be targeted for crime. Tangible assets in the computer environment, therefore, often have a double value. The replacement cost of a piece of computer equipment may represent only a small portion of the economic loss caused by the theft of, or damage to, that equipment. Of much greater significance is the value of the information lost or made inaccessible by the misappropriation or damage.

41. Computer systems are particularly vulnerable to threats because of a number of interacting factors. The more significant of these are analysed briefly below.

1. Density of information and processes

42. Storage technology has allowed the development of filing systems that can accommodate billions of characters of data on-line. Providing different access privileges for different users of such systems is often difficult. A further problem lies in the fact that, owing to the methods for accessing stored information, a single error can have widespread impact. This fact can be used to great advantage by a party who wants to corrupt data or disrupt service.

43. At the same time, memory management techniques allow many independent processes to be supported concurrently within a single operating system. Independent data files can be combined to produce new and unforeseen relationships. Data items may be linked to produce a new item with a higher level of sensitivity than the original discrete data components. The centralization of information and processing functions provides an attractive target for the infiltrator or saboteur intent on attacking the functions or information assets of an organization.

44. The density of data stored on such media as tapes, diskettes, cassettes and microfilms means that the loss or theft of such items can be very significant.

2. System accessibility

45. Before security became a significant design criterion, the goal was often to provide the maximum computing capability to the largest possible user community. Access concerns once confined to the restricted computer room area must now be extended to remote terminal locations and interconnecting communications links. However, remote terminal stations and transmission circuits are often not subject to the same controls as those in the main centre. Two forms of attack that exploit remote access are the use of fraudulent identification and access codes to obtain the use of system resources and the unauthorized use of an unattended terminal, logged on by an authorized person.

46. Because of the desire to give system users maximum capability, unrestricted access privileges are often granted rather than allowing only the privileges necessary to perform an intended function. A transaction-oriented system permitting read-only or inquiry-only access offers a greater degree of protection than a system offering full programming capability.

47. Many systems in current use offer very limited ability to control user capabilities related to passive data and programs on a read-only, read-write or execute basis. This situation frequently necessitates operating on the assumption that every user has the capability to use the full computing potential of the operating system. A known penetration technique that utilizes this weakness involves disguising user instructions intended for clandestine purposes as a common utility, such as a file-copying routine, or inserting them into an existing routine. When the illicit code is activated, it performs functions more privileged than were intended for that user.

48. Finally, computer control functions are normally made accessible to numerous support and maintenance personnel. Tampering with software or hardware logic to obtain extended privilege or to disable protection features has been known to occur. The exposure provided

through increasingly easy access to electronic data processing (EDP) resources is an important contributor to the vulnerability of modern computer systems.

### 3. Complexity

49. The typical operating environment of medium- and large-scale systems is characterized by support for local batch, remote batch, interactive and, occasionally, real-time user modes. Typical operating systems contain from 200,000 to 25 million individual instructions. The number of logic states that are possible during execution in a multiprogramming or multiprocessing environment approaches infinity. It is not surprising that such systems are not fully understood by anyone, including the designers, or that they are often unreliable. It is only possible to prove the presence of errors, not their absence, and any system error can result in down time or a potential security fault. Even when systems have been carefully designed, errors in implementation, maintenance and operation can still occur. The prospective infiltrator can be expected to take full advantage of the uncertainties created by system complexity. Incidents have been noted where deliberate attempts to confuse operators, or to interrupt systems by attacking little-known weaknesses, have been instrumental in producing security violations.

### 4. Electronic vulnerability

50. The reliance of computer systems on electronic technology means that they are subject to problems of reliability, fragility, environmental dependency and vulnerability to interference and interception. On systems using telecommunications, these vulnerabilities extend to the whole communications network in use.

51. Traditional forms of electronic eavesdropping can be readily adapted to exploit data-processing systems. They include wire-tapping and bugging, the analysis of electromagnetic radiations from equipment and monitoring of the cross-talk induced in adjacent electrical circuits. Interconnecting data communications circuits also suffer the same vulnerabilities, and communications on them can be subject to misrouting. A variation on wire-tapping involves the illegal use of a minicomputer to intercept data communications and to generate false commands or responses to other system components.

52. In the commission of a fraud, electronic technology has an advantage over manual data manipulation, which generally leaves behind an audit trail. Computer data, however, can be instantly changed or erased with minimal chance of detection, by, for example, a virus or logic bomb. The computer criminal can easily modify systems to perpetrate the fraud and then cover the evidence of the offence. It is suggested, moreover, that data processing is protected by only one tenth of the controls afforded to the same process in the manual environment, an insufficiency that facilitates the opportunity to commit crime without detection.

53. The performance of EDP systems may also be adversely affected by electromagnetic interference. Conducted or radiated electrical disturbances can interfere with the operation of electronic equipment. The system may suffer only very temporary and intermittent impairment, measurable in microseconds and from which recovery is possible, or it may suffer complete equipment failure, resulting in an inability to process.

54. All hardware is susceptible to failure through ageing, physical damage and environmental change. To ensure that error propagation is confined to non-sensitive functions, i.e., that the system fails safely, malfunctions must be detected immediately. Progress is being made towards this goal, but few designs in current use offer the desired level of reliability.

### 5. Vulnerability of electronic data-processing media

55. It is sometimes inferred that a degree of security is provided by the inability of humans to translate machine-readable data in the form of punched holes in cards or tape, magnetic states on tapes, drums and disks, and electrical states in processing or transmission circuits. In practice, not only can such computerized information codes be readily interpreted by most technical personnel, but the data obscurity created has the additional negative effect of creating identification and accounting problems.

56. Because the contents of most EDP media are not visually evident, data-processing personnel are often required to handle sensitive files without being aware they are doing so. As a result, the control of data items becomes a problem. Scratched tapes, discarded core memories can all contain residual data that may demand special attention. Because identity

and accountability have been lost, safeguards are frequently relaxed for these items even though the same information is protected elsewhere in the system. The ease with which such sources of information can be utilized has resulted in several well-publicized system penetrations.

#### 6. Human factors

57. As discussed above, employees represent the greatest threat in terms of computer crime. It is not uncommon, operators, media librarians, hardware technicians and other staff members to find themselves in positions of extraordinary privilege in relation to the key functions and assets of their organization. A consequence of this situation is the probability that such individuals are frequently exposed to temptation.

58. A further complication is the tendency on the part of management to tolerate less stringent supervisory controls over EDP personnel. The premise is that the work is not only highly technical and specialized but difficult to understand and control. As an example systems software support is often entrusted to a single programmer who generates the version of the operating system in use, establishes password or other control lists and determines the logging and accounting features to be used. In addition, such personnel are often permitted, and sometimes encouraged, to perform these duties during non-prime shift periods, when demands on computer time are light. As a result, many of the most critical software development and maintenance functions are performed in an unsupervised environment. It is also clear that operators, librarians and technicians often enjoy a degree of freedom quite different from that which would be considered normal in a more traditional employment area.

59. There is another factor at play in the commission of computer crime. Criminological research has identified a variation of the Robin Hood syndrome: criminals tend to differentiate between doing harm to individual people, which they regard as highly immoral, and doing harm to a corporation, which they can more easily rationalize. Computer systems facilitate these kinds of crimes, as a computer does not show emotion when it is attacked. 12

60. Situations in which personnel at junior levels are trusted implicitly and given a great deal of responsibility, without commensurate management control and accountability, occur frequently in the EDP environment. Whether the threat is from malicious or subversive activities or from honest errors on the part of staff members, the human aspect is perhaps the most vulnerable aspect of EDP systems.

---

#### E. Common types of computer crime

61. All stages of computer operations are susceptible to criminal activity, either as the target of the crime or the instrument of the crime or both. Input operations, data processing, output operations and communications have all been utilized for illicit purposes. The more common types of computer-related crime are categorized next.

##### 1. Fraud by computer manipulation

62. Intangible assets represented in data format, such as money on deposit or hours of work, are the most common targets of computer-related fraud. Modern business is quickly replacing cash with deposits transacted on computer systems, creating an enormous potential for computer abuse. Credit card information, as well as personal and financial information on credit-card clients, have been frequently targeted by the organized criminal community. The sale of this information to counterfeiters of credit cards and travel documents has proven to be extremely lucrative. Assets represented in data format often have a considerably higher value than traditionally targeted economic assets, resulting in potentially greater economic loss. In addition, improved remote access to databases allows the criminal the opportunity to commit various types of fraud without ever physically entering the premises of the victim.

63. Computer fraud by input manipulation is the most common computer crime, as it is easily perpetrated and difficult to detect. Often referred to as "data diddling", it does not require any sophisticated computer knowledge and can be committed by anyone having access to normal data-processing functions at the input stage.

64. Program manipulation, which is very difficult to discover and is frequently not recognized, requires the perpetrator to have computer-specific knowledge. It involves changing existing programs in the computer system or inserting new programs or routines. A

common method used by persons with specialized knowledge of computer programming is the trojan horse, whereby computer instructions are covertly placed in a computer program so that it will perform an unauthorized function concurrent with its normal function. A trojan horse can be programmed to self-destruct, leaving no evidence of its existence except the damage that it caused. 13 Remote access capabilities today also allow the criminal to easily run modified routines concurrently with legitimate programs.

65. Output manipulation is effected by targeting the output of the computer system. The obvious example is cash dispenser fraud, achieved by falsifying instructions to the computer in the input stage. Traditionally, such fraud involved the use of stolen bank cards. However, specialized computer hardware and software is now being widely used to encode falsified electronic information on the magnetic strips of bank cards and credit cards.

66. There is a particular species of fraud conducted by computer manipulation that takes advantage of the automatic repetitions of computer processes. Such manipulation is characteristic of the specialized "salami technique", whereby nearly unnoticeable, "thin slices" of financial transactions are repeatedly removed and transferred to another account. 10

### 2. Computer forgery

67. Where data are altered in respect of documents stored in computerized form, the crime is forgery. In this and the above examples, computer systems are the target of criminal activity. Computers, however, can also be used as instruments with which to commit forgery. The created a new library of tools with which to forge the documents used in commerce. A new generation of fraudulent alteration or counterfeiting emerged when computerized colour laser copiers became available. 14 These copiers are capable of high-resolution copying, the modification of documents and even the creation of false documents without benefit of an original, and they produce documents whose quality is indistinguishable from that of authentic documents except by an expert.

### 3. Damage to or modifications of computer data or programs

68. This category of criminal activity involves either direct or covert unauthorized access to a computer system by the introduction of new programs known as viruses, "worms" or logic bombs. The unauthorized modification, suppression or erasure of computer data or functions with the internet to hinder normal functioning of the system is clearly criminal activity and is commonly referred to as computer sabotage. Computer sabotage can be the vehicle for gaining economic advantage over a competitor, for promoting the illegal activities of ideologically motivated terrorists or for stealing data or programs (also referred to as "bitnapping") for extortion purposes. In one reported incident at London, Ontario, in 1987, a former employee of a company sought unsuccessfully to sabotage the computer system of the company by inserting a program into the system that would have wiped it out completely.

69. A virus is a series of program codes that has the ability to attach itself to legitimate programs and propagate itself to other computer programs. A virus can be introduced to a system by a legitimate piece of software that has been infected, as well as by the trojan horse method discussed above.

70. The potential purposes of viruses are many, ranging from the display of harmless messages on several computer terminals to the irreversible destruction of all data on a computer system. In 1990, Europe first experienced a computer virus, used to commit extortion in the medical research community. The virus threatened to destroy increasing amounts of data if no ransom was paid for the "cure". A significant amount of valuable medical research data was lost as a result.

71. A worm is similarly constructed to infiltrate legitimate data-processing programs and to alter or destroy the data, but it differs from a virus in that it does not have the ability to replicate itself. In a medical analogy, the worm can be compared to a benign tumor, the virus to a malignant one. However, the consequences of a worm attack can be just as serious as those of a virus attack: for example, a bank computer can be instructed, by a worm program that subsequently destroys itself, to continually transfer money to an illicit account.

72. A logic bomb, also known as a "time bomb", is another technique by which computer sabotage can be perpetrated. The creation of logic bombs requires some specialized knowledge, as it involves programming the destruction or modification of data at a specific

time in the future. Unlike viruses or worms, however, logic bombs are very difficult to detect before they blow up; thus, of all these computer crime schemes, they have the greatest potential for damage. Detonation can be timed to cause maximum damage and to take place long after the departure of the perpetrator. The logic bomb may also be used as a tool of extortion, with a ransom being demanded in exchange for disclosure of the location of the bomb.

73. Irrespective of motive, the fact remains that the use of viruses, worms and logic bombs constitutes unauthorized modification of legitimate computer data or programs and thus fall under the rubric computer sabotage, although the motive of the sabotage may be circumstantial to the alteration of the data.

#### 4. Unauthorized access to computer systems and service

74. The desire to gain unauthorized access to computer systems can be prompted by several motives, from simple curiosity, as exemplified by many hackers, to computer sabotage or espionage. Intentional and unjustified access by a person not authorized by the owners or operators of a system may often constitute criminal behavior. Unauthorized access creates the opportunity to cause additional unintended damage to data, system crashes or impediments to legitimate system users by negligence.

75. Access is often accomplished from a remote location along a telecommunication network, by one of several means. The perpetrator may be able to take advantage of lax security measures to gain access or may find loopholes in existing security measures or system procedures. Frequently, hackers impersonate legitimate system users; this is especially common in systems where users can employ common passwords or maintenance passwords found in the system itself.

76. Password protection is often mischaracterized as a protective device against unauthorized access. However, the modern hacker can easily circumvent this protection using one of three common methods. If a hacker is able to discover a password allowing access, then a trojan horse program can be placed to capture the other passwords of legitimate users. This type of program can operate concurrently with the normal security function and is difficult to detect. The hacker can later retrieve the program containing the stolen passwords by remote access.

77. Password protection can also be bypassed successfully by utilizing password cracking routines. Most modern software effects password security by a process that converts a user's selected password into a mathematical series, a process known as encryption. Encryption disguises the actual password, which is then almost impossible to decrypt. Furthermore, legitimate security software has been developed that allows access to data only after it checks encrypted passwords against a dictionary of common passwords so as to alert system administrators of potential weakness in security. However, this same security process can be imitated for illegitimate purposes. Known as a "cracker" program when used for illegitimate purposes, these tools encrypt some or all of the data of the system. This creates a dictionary of data to compare with cracker software, for the purpose of identifying common passwords and gaining access to the system. A variety of these system-specific encryption routines can be obtained from hacker bulletin boards around the world and are regularly updated by the criminal community as security technology develops.

78. The third method commonly used to access a system is the "trapdoor" method, whereby unauthorized access is achieved through access points, or trapdoors, created for legitimate purposes, such as maintenance of the system.

79. The international criminal hacker community uses electronic bulletin boards to communicate system infiltration incidents and methods. In one case, details of a Canadian attempt to access a system were found on suspects in an unrelated matter in England; they had removed the material from a bulletin board in Germany. This sharing of information can facilitate multiple unauthorized infiltrations of a system from around the globe, resulting in staggering telecommunication charges to the victim.

80. With the development of modern telecommunications system, a new field for unauthorized infiltration was created. Personal telecommunications have been expanded with the advent of portable, cellular telecommunication devices. The criminal community has responded to these advances by duplicating the microchip technology.

81. Modern telecommunications systems are equally vulnerable to criminal activity. Office automation systems such as voice mail boxes and private business exchanges are, in effect, computer systems, designed for the convenience of users. However, convenience features such as remote access and maintenance capabilities, call-forwarding and voice-messaging are easily infiltrated by computer criminals.

82. Modern telecommunications systems, like other computer systems, are also susceptible to abuse by remote access. The integration of telecommunications systems means that once one system is accessed, a computer operator with sufficient skill could infiltrate the entire telecommunications network of a city. The usual motive for telecommunications crime is to obtain free telecommunications services. However, more innovative telecommunications fraud has also been uncovered, and telecommunications systems have been used to disguise other forms of criminal activity.

5. Unauthorized reproduction of legally protected computer programs

83. The unauthorized reproduction of computer programs can mean a substantial economic loss to the legitimate owners. Several jurisdictions have dictated that this type of activity should be the subject of criminal sanction. The problem has reached transnational dimensions with the trafficking of these unauthorized reproductions over modern telecommunication networks.

---

#### IV. PROCEDURAL LAW

---

##### A. Background

146. Computer-specific procedural law problems arise not only in the prosecution of computer-crime cases but also in many other fields of criminal investigation. This is especially illustrated by the prosecution of economic crimes, predominantly in the field of banking, where most of the relevant evidence is stored in automated data-processing systems. In the field of traditional crime, computer-stored evidence is already a significant issue, as is illustrated by cases of drug traffickers conducting their business using personal computers and international telecommunication systems. In future, new optical storage devices based on compact disc technology will further encourage the destruction of originals (if paper originals still exist) after the information has been recorded in automated data-processing systems. Owing to these new technical developments and to the growing use of computers in all areas of economic and social life, courts and prosecution authorities will depend to an increasing extent on evidence stored or processed by modern information technology.

147. The resulting replacement of visible and corporeal objects of proof by invisible and intangible evidence in the field of information technology not only creates practical problems but also opens up new legal issues: the coercive powers of prosecuting authorities, discussed in paragraphs 148-165; specific problems with personal data, discussed in paragraphs 166-170; and the admissibility of computer-generated evidence, discussed in paragraphs 171-175. The relevant problems are dealt with not only at the national level but also by various international organizations, as discussed in paragraphs 176-185.

---

##### B. The coercive powers of prosecuting authorities

148. In accordance with the practical requirements of investigations in the field of information technology and based on the various coercive powers existing in most legal systems, an analysis of the coercive powers of prosecuting authorities has to differentiate among search and seizure in automated information systems; duties of active cooperation; and wire-tapping of telecommunication systems and "eavesdropping" of computers.

###### 1. Search and seizure in automated information systems

Problems of traditional law

149. Collecting data stored or processed in computer systems generally first requires entry to and search of the premises in which the computer system is installed (powers of search and entry of premises); it is then necessary that the data can be seized or captured (powers of seizure and retention).

150. With respect to the investigation of computer data permanently stored on a corporeal data carrier, the general limitation of the powers of search and seizure to the search and seizure of (corporeal) objects relevant to the proceedings or to finding the truth does not, in most countries, pose serious problems, since the right to seize and to inspect the corporeal data carrier or, in case of internal memories, the central processing unit also includes the right to inspect the data. In other words, there is no difference whether the data are fixed with ink on paper or by magnetic impulses in electronic data carriers. This conclusion is even more evident for provisions in which the powers of search and/or the powers of seizure are directed towards "anything" that would be admissible as evidence at a trial. The same evaluation also applies *mutatis mutandis* for powers of confiscation.

151. Application of the traditional powers of search and seizure might, however, cause problems in cases where data are not permanently stored in a corporeal data carrier. In these instances, it is questionable whether pure data or information can be regarded as an object in the sense of criminal procedural law. The same holds true if the legal principle of minimum coercion or of proportionality makes it unlawful to seize comprehensive data carriers, or complete computer installations, in order to gather only a small amount of data. Similarly, search and seizure of comprehensive data carriers could cause serious prejudice to business activities or infringe the privacy rights of third parties. Uncertainties may also arise in cases in which data carriers (such as core-storage, fixed-disk devices or chips) cannot be taken away to be evaluated on a police computer but must be analysed using the computer system in question. In all these cases one might consider applying the powers of search not only to detect a computer installation and data but also to fix (especially to print) the relevant data on a separate data carrier and then seize this new object, which might be a diskette or a printout.

152. However, such a construction depends on the question of whether and to what degree the powers of search and seizure include the power to use technical equipment and (copyrightable) programs belonging to a witness or to an accused, in order to search and/or fix computer data. Only a few laws state that in the execution of search and seizure all necessary measures may be taken. Consequently, in many legal systems an effective search for pure data or information is not provided for by the law.

153. Special problems also arise with respect to search and seizure in computer networks. Here, it is questionable whether and to what extent the right to search and seize a specific computer installation includes the right to search databases that are accessible by this installation but that are situated in other premises. This question is of great practical importance since perpetrators increasingly store their data in computer systems located elsewhere in order to hinder prosecution. Specific problems of public international law arise with respect to search and seizure of foreign databases via international telecommunication systems. In these international systems, the direct penetration by prosecuting authorities of foreign data banks generally constitutes an infringement of the sovereignty of the State of storage (and often in a punishable offence); however, there might be some specific exceptions that could be developed internationally in which direct access to foreign data banks via telecommunication networks could be permissible and the lengthy procedure of mutual assistance avoided.

154. Problems of interpretation also arise with respect to extra safeguards for specific information. This is not only an issue with respect to the materials of professional legal advisers, doctors, journalists and other people who may, in some legal systems, be exempt from giving evidence. One of the latest disputes in this area is the question of how far the privileges of the press should also be applicable to electronic bulletin boards. Even more intricate questions arise with the application of safeguards and specific provisions to papers, documents and letters, especially in the fields of electronic mail and telecommunication systems. Owing to the rationale of these privileges, they should generally apply equally to paper-based and computer-stored material, especially as between traditional mail and electronic mail.

Law reform

155. In some countries attempts have been made to resolve these uncertainties and loopholes in the field of search and seizure of data and information by legislative amendments. In the

United Kingdom, the general power of seizure provided by section 19 of the Police and Criminal Evidence Act of 1984 is directed to "anything which is on the premises" and, under certain conditions, provides the power "to require any information which is contained in a computer" (for the latter duty of active cooperation, see paragraphs 157-162). In Canada, section 14 of the Competition Act and similar provisions in the Environmental Protection Act and the Fisheries Act permit searching for "any data contained in or available to the computer system". Furthermore, section 3(1) of the legislation proposed by the Law Reform Commission of Canada with respect to search and seizure defines objects of seizure as "things, funds, and information" which are reasonably believed to be takings of an offence, evidence of an offence or contraband.

156. Such *sui generis* provisions for gathering data not only provide legal certainty and a basis for efficient investigations in an EDP environment but, with respect to legal policy, can also be based on the argument that copying data is often a less severe inhibition than the seizure of data carriers. Moreover, *sui generis* provisions have the advantage of being able to solve specific questions of search and seizure of data, such as compensation of costs for the use of EDP systems, subsequent erasure of copied data that are no longer required for the prosecution, or search and seizure in telecommunication networks.

## 2. Duties of active cooperation

### The practical problems

157. The aforementioned powers of entry, search and seizure, and even a *sui generis* power of gathering data, do not, in many cases, guarantee a successful investigation, since the traditional authorities often lack the knowledge of computer hardware, operating systems and standard software necessary to access modern data-processing systems. The very complexity of modern information technology creates many problems regarding access to computer systems, which can be solved, but only partially, by better police training. This is mainly the case with respect to specific security software and encryption designed to prevent unauthorized access to information. Serious problems are also caused by the multitude of data stored in computer systems and by the limited time and financial resources available to prosecuting authorities for checking these data. Consequently, the duties of citizens to cooperate with prosecuting agencies become of much greater importance in computerized environments than in non-technical, "visible" areas.

158. The traditional legal systems of most countries include two instruments that might be used to achieve the cooperation necessary for gathering evidence in a computerized environment: the duty to surrender seizable objects of evidence and the duty to testify. In some countries, additional and more extensive provisions or reform proposals have been enacted or suggested.

### Duties to surrender seizable objects

159. The duty to surrender seizable objects is often coupled with the powers of search and seizure. In many countries the holder of a seizable object is obliged to deliver it on request to the (judicial) authorities; however, some legal systems do not provide such an obligation, and in some countries the respective court orders are not enforceable. The duty to surrender seizable objects can help the investigating authorities, especially in selecting specific data carriers from among the many tapes and diskettes that are usually stored in a computer centre. However, the obligation to surrender seizable objects does not generally include the duty to print or deliver specific information stored on a data carrier. Consequently, in many countries the powers of seizure and the duties to surrender seizable objects can only support voluntary printing of specific information. Practice with respect to search and seizure in the field of banking shows that banks often voluntarily print out specific data in order to prevent the seizure of large volumes of data carriers. However, the threat of a comprehensive seizure and serious prejudice to business activities cannot be regarded as a satisfactory legal solution for the relevant problems.

### Duties to testify

160. In many cases an important duty of active cooperation can be based on the duties to testify, i.e. the duty of (unsuspected) witnesses to "testify", to "tell the truth", to "answer questions" etc. This is especially the case in countries in which the traditional duties to testify

contain the more extensive obligation that the witness refresh his or her knowledge of the case, e.g. by examining account books, letters, documents and objects that are available to the said witness without special inconvenience, and to make notes and bring them along to the court. However, in most legal systems the traditional duties to testify cannot be extended to efficient duties of cooperation, especially not to the printing out of specific information. The main reason for this conclusion is the fact that the duty to testify, and consequently the duty of witnesses to refresh their knowledge, refers only to knowledge they already had in mind and not to new information. A different conclusion would also confuse the roles of witnesses and experts. Furthermore, in many countries the witness must testify before a judge, and in some countries before the public prosecutor, but not before police conducting the investigation; in some legal systems, the duties to testify exist only at a later stage of the proceedings and not during the police investigation. Moreover, the requirement that a (written or oral) court summons be given to the witness in due time prior to the proceedings could make such proceedings ineffective.

#### Law reform

161. To make investigations in computerized environments more efficient, some countries have recently enacted or suggested new compulsory duties to produce specific information. According to the police and Criminal Evidence Act 1984 of the United Kingdom, the constable "may require any information which is contained in a computer and is accessible from the premises to be produced in a form in which it can be taken away and in which it is visible and legible". In Canada, the Mutual Legal Assistance Act provides for an evidence gathering order addressed to a person "to make a copy of a record or to make a record from data and to bring the copy or record with him". However, with respect to data accessible via international telecommunication networks, these provisions leave open the question whether and to what degree a State, in accordance with international public law, has the right to oblige its citizens to gather evidence in foreign countries. Furthermore, other than in respect of recognized privileges, it is unclear under which conditions citizens have the right to deny cooperation.

162. The question whether or not such duties to produce and hand over computer printouts should be recommended *de lege ferenda* is difficult to judge and requires a differentiation between the duties of witnesses and the duties of defendants or suspected persons. With respect to (innocent) witnesses, there are good arguments for the introduction of such a duty. However, with respect to the defendant or suspect, there are equally good arguments that a duty of active cooperation should be rejected since this duty could impede the accused's right to remain silent and could infringe upon the privilege against self-incrimination. It is true that the wording of article 14(3)g of the International Covenant on Civil and Political Rights only guarantees that, in the determination of any criminal charge against a person, everyone shall be entitled to the minimum guarantee of "not to be compelled to testify against himself or to confess guilt". However, the reasons underlying this guarantee could justify a general privilege against any active self-incrimination.

#### 3. Wire-tapping and "eavesdropping"

##### Problems of traditional law

163. Tapping telecommunication lines and eavesdropping on computer systems can assist criminal investigations, especially in cases where data are only transmitted and not permanently stored, where data merely cross a country or where permanent observation of telecommunications or computer activities is necessary. These investigative acts, however, constitute not only a highly efficient means of prosecution but also a very severe intrusion into the civil liberties of the person whose communications have been surveyed. This is primarily based on the fact that tapping telecommunication systems and eavesdropping on computers is, generally, a permanent and clandestine intrusion, whereas the above-mentioned powers of entry, search and seizure usually constitute a single, "visible" interference with civil liberties. Consequently, in most countries the statutory requirements for telephone tapping and the recording of telecommunications are much more stringent than for other coercive measures.

164. The question whether the traditional powers of wire-tapping can be applied to tapping other telecommunication services and computer systems is answered differently in various countries. No computer-specific issues arise in legal systems in which the statutory law permits, for example, "surveillance of the telecommunication traffic including the recording of its content". On the other hand, computer-specific problems of interpretation exist, especially in countries that permit only "monitoring of conversations" or "surveillance and tapping of the telecommunication traffic on sound carriers". Such clauses are particularly problematic if an analogous application of coercive powers in criminal procedural law is not jurisprudentially permissible.

#### Law reform

165. To avoid problems of interpretation, some countries have already enacted or proposed new legislation that would make it possible to tap all kind of telecommunications under the same conditions as must be met for tapping telephone conversations. In Denmark, a new provision of the Administration of Justice Act was passed in 1985, according to which the police, under certain conditions, may "interfere in private communication by ... tapping telephone conversations or other similar telecommunication". In 1986, in the United States, the Electronic Communication Privacy Act extended legal protection and powers of wire-tapping from aural communication (covered by the Omnibus Crime Control and Safe Street Act of 1968) to electronic communication. Similarly, in the Federal Republic of Germany, an amendment to the Criminal Procedural Code in 1989<sup>11</sup> extended the possible use of wire-tapping to public telecommunication networks. With respect to future policy-making, such clarifications are helpful since telecommunication between computers probably does not merit more protection than telecommunication between persons.

---

#### C. Specific problems with personal data

166. Potentially coercive powers for collecting evidence in the field of information technology, as analysed above, cover both personal and non-personal data. With respect to personal data, however, there are additional legal problems that mainly concern gathering, storing and linking personal data in the course of criminal proceedings. In this field of "privacy protection in criminal matters", legal requirements vary considerably among countries. Differences between various legal systems are found not only in substantive law requirements but also in the constitutional background, legal context and legislative technique of the relevant provisions.

167. An extensive discussion of the underlying constitutional implications regarding the gathering, storing and linking of personal data exists in only a few countries. For example, in the Federal Republic of Germany, the Federal Constitutional Court, in its famous "census decision", recognized that the State's storage of personal data, especially in computer systems, could influence citizen's behaviour and endanger their general liberty of action and must therefore be considered as a violation of civil liberties ("right of informational self-determination"), which requires an express and precise legal basis. This legal balance must balance the interests of the individual and the right to privacy, on the one hand, and the interests of society in the suppression of criminal offences and the maintenance of public order, on the other hand. The new Constitution of Spain of 1978, the new revised Constitution of Portugal of 1982, the Constitution of the Netherlands of 1983 and the new Constitution of Brazil of 1988 even contain specific safeguards protecting their citizens' privacy against the incursions of modern computer technology. However, in many other countries the gathering and storing of personal data are not (yet) considered to be of constitutional relevance and are dealt with by the legislature in ordinary statutory (non-constitutional) law on a voluntary basis.

168. In regulating the legality of gathering, storing and linking personal data (either on a constitutional, compulsory basis or on an ordinary, voluntary legal basis), various legal systems place the relevant provisions in different contexts and laws. A few countries, such as Germany, intend to place most of the respective provisions within the purview of their criminal procedural law. This legislative technique has the advantage that the criminal procedural code retains its monopoly over the application of criminal law and thus retains the

exclusive enumeration of powers regulating the infringement of civil liberties in the course of criminal prosecution. However, most countries (uniquely or in part) regulate the legality of police files within their general data protection acts; in most cases the relevant provisions are applicable both to the enforcement activity of the police (prosecution of crimes) and to its preventive action (maintenance of public order). Some countries exclude police files, completely or partly, from their general data protection laws and/or create specific acts or decrees for all types of (law enforcement or preventive) police data. In a number of countries, additional specific laws concerning criminal records exist. However, there are also legal systems without any statutory legal provisions regulating the general use of personal data in the police sector.

169. Apart from these questions of placement and context of the relevant statutes, the legislative technique, content and control mechanisms of the relevant laws also vary. With respect to legislative technique, some countries, such as Germany, consider a more detailed and precise regulation necessary; other countries resort to more or less general clauses.

170. As far as the contents of the various laws are concerned, serious limitations rarely seem to be applicable to police files. In many countries, far-reaching and precise regulations concerning the deletion of entries exist only with respect to registers of criminal convictions.

---

#### D. Admissibility of computer-generated evidence

171. The admissibility of computer-generated evidence is not only important for the use of computer records in the criminal trial process but is also essential to define the extent of the above-described coercive investigatory powers, including those of mutual assistance. In most countries coercive powers are applicable only to material that would be admissible in evidence at a trial, if specific computer data or printouts could not be used as evidence; consequently, they could also not be searched and seized. In practice, the various legal problems are particularly crucial since computer printouts and computer data can easily be manipulated, a phenomenon that is illustratively described as the "second-hand nature" of computer printouts.

172. The admissibility in courts of evidence from computer records depends to a great extent on the underlying fundamental principles of evidence in the particular country. It is necessary to differentiate among varying legal systems, including but not limited to (a) civil law countries and (b) common law countries. Other legal systems, such as Islamic law, incorporate elements from one of these two primary types of systems.

##### 1. Civil law countries

173. Civil law countries and many other countries operate according to the principle of free introduction and free evaluation of evidence (*système de l'intime-conviction*). In these countries the judge can, in principle, consider all kinds of evidence and then weigh the extent to which the court can rely on the evidence. Legal systems based on these principles do not, in general, hesitate to introduce computer records as evidence. Problems occur only when procedural provisions contain specific regulations for the proof of judicial acts or proof with legal documents.

##### 2. Common law countries

174. Contrary to the legal situation in civil law countries, common law countries are characterized by an oral and adversarial procedure. In these countries a witness can only testify concerning his or her personal knowledge, thereby permitting the statements to be verified by cross-examination. Knowledge from secondary sources, such as other persons, books or records, is regarded as hearsay evidence and is, in principle, inadmissible. Additionally, the "best-evidence" rule generally requires that originals, rather than copies, be introduced as evidence before the court in order to lessen the chance of fraud and error. There are, however, several exceptions to the hearsay and best-evidence rules, such as the "business records exception" or the "photographic copies exception". The business records exception, for example, permits a business record created in the course of everyday commercial activity to be introduced as evidence even if there is no individual who can testify from personal knowledge. If certain prerequisites are met, copies of certain types of records may also be permitted. The questions whether computer files are "real evidence" and whether computer

printouts fall under one of the exceptions of the hearsay rule have been the subject of extensive debate. The courts in some common law countries have accepted computer printouts as falling within the business records exception. Other common law countries have elaborated new laws allowing computer records to be admitted as evidence if certain conditions are met.

### 3. Islamic law countries

175. Under Islamic law, computer crime falls within the area of taazir offences, which operates according to the same principles of evidence law as civilian systems: the free introduction and evaluation of evidence (*système de l'intime-conviction*). In adjudicating taazir offences the judge weighs the reliability of evidence, and thus computer records are generally admissible in the prosecution of computer crime.

### E. International harmonization

176. In procedural law, international action has already commenced in all of the areas described above and has been concerned with (a) the field of coercive powers; (b) the legality of processing personal data in the course of criminal proceedings; and (c) the admissibility of computer-generated evidence in court proceedings.

#### 1. Coercive powers in the field of information technology

177. One example of international harmonization of the above-mentioned coercive powers in information technology derives primarily from the guarantees of article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The European Court of Human Rights applied these guarantees especially in the area of wire-tapping. In the *Klass* case, the Court confirmed the legality of the German law on limitations of the secrecy of letters, post and telecommunication, which, under specific conditions, provides the authorities with the competence to supervise

---

## VI. INTERNATIONAL COOPERATION

---

### A. General aspects

239. As modern society is heavily information-dependent, computer-related crimes are easily committed on an international scale. International access to information and the mobility of data are fundamental to the working of our economic systems. Distance, time and space have ceased to be obstacles in commercial transactions. There is no longer any need for the physical presence of human agents. As the manipulation and storage of data take place within the dimension of international telecommunication networks, the usual border controls are bypassed. International instruments containing principles of the transborder flow of data, such as those by the United Nations or OECD, focus clearly on the principle of free flow of information, tempered by concerns to protect the confidentiality and integrity of the transmitted information, particularly in the case of sensitive data. Given the utility of paperless commercial transactions in international commerce and the rapidly improving sophistication of electronic communications, the volume of cross-boarder computer has increased significantly.

240. Currently, whole sectors of economy, such as banking and international aviation, rely heavily or even exclusively on international telecommunication networks. With the continuing development of standards and norms for electronic data interchange (EDI), such as that under the auspices of the United Nation Electronic Data Interchange for Administration, Commerce and Transportation (UN/EDIFACT), the use of EDI will increase substantially in the decade to come.

241. The international element in the commission of computer crime create new problems and challenges for the law. Systems may be accessed in one country, the date manipulate in another and the consequences felt in a third country. Hackers can operate physically operate in one country, move electronically across the world from one network to another and easily access databases on a different continent. The result of this ability is that different sovereignties, jurisdictions, laws and rules will come into play. More than in any other

transnational crime, the speed, mobility, flexibility, significance and value of electronic transactions profoundly challenge the existing rules of international crime law.

242. There are a number of complex issues to confront, given the multiplicity of countries potentially involved in a crime. How can it be determined which country the crime was actually committed? Who should have jurisdiction to prescribe rules of conduct or of adjudication? In crimes involving multinational contacts, there will be frequently be conflicts of jurisdiction. Countering computer crimes committed from a distance and having an increasing range of international targets (such as country of commission of the crime, the number of actors and victims involved, and the range of potential consequences) will require a well-developed network of inter-State cooperation to attain effective investigation and prosecution. In the light of the technicalities of international interaction, cooperation between nations in criminal matters is crucial.

243. These issues have to be addressed by all countries, whether they be producers, users or consumers of the new information technologies, since these technologies are becoming an integral part of economic, social and culture development.

244. In seeking solutions to the above problems, the international community should strive for the following:

Maximizing cooperation between nations in order to address, firstly, the potential for enormous economic losses and, secondly, the general threat to privacy and other fundamental values that near-instantaneous cross-border electronic transactions may create;

Worldwide protection so as to avoid "data paradises" or computer crimes havens where computer criminals can find refuge or launch their attacks;

A lawfully structured cooperation scheme, taking into account and balancing the necessities of international trade and relations on the one hand and the rights and freedoms of the individual on the other hand.

---

## B. The jurisdiction issue

### 1. The territoriality principle

245. There are a number of problems related to the issue of jurisdiction. In every computer crime, the determination of the locus delicti (the location of the offence) will affect the ability of a particular country to sanction the crime. Will the sanction arise by virtue of territorial jurisdiction and domestic law, or must extraterritorial principles apply?

246. Today, it is technologically possible for an operator to punch a keyboard in country A so as to modify data stored in country B, even the operator does not know that the data are stored there, to have the modified data transferred over a telecommunications network through several other countries, and to cause an outcome in country C. On the basis of the physical act, the technical modification, the transmission of the falsified data and the consequences, three or perhaps more countries will have been involved and may have a claim to jurisdictional competency.

247. Depending on which elements or stages of the crime are given priority, several countries in the above scenario could, within their full sovereignty, declare the incident as having occurred on their territory, thus invoking the principle of territorial jurisdiction in order to prosecute and sanction. This raises a potential jurisdictional conflict, as well as the question of the appropriate arbitration of these equal claims for jurisdiction, the applicability of the non bis in idem rule, and the impact of the lex mitior rule.

248. The recurring threat of computer viruses worms is another striking example of transnationality. If a virus infects the system in one location, the infection can spread with destructive rapidity and affect programs throughout the international network. What criteria should apply in determining which country may act? Once again, several choices are available: the country in which the virus was introduced, all countries in which software or databases were affected and all countries in which results were felt. It is possible that it may not manifest itself far away from the country of origin. It is also possible that it may not manifest itself until considerable time has passed, when retracing the technological path of the original offender has become difficult, as, for example, in cases of the so-called time-bomb virus. What, then, determines the competency to prosecute and sanction? Can it be the

best evidence rule or the first-come, first-served principle, or do the traditional solutions discussed below still stand firm?

249. The primacy of the principle of territoriality is generally accepted in sphere of criminal jurisdiction. The principle is based on mutual respect of sovereign equality between States and is linked with the principle of non-intervention in the affairs and exclusive domain of other States. Even in the exceptional event that a country might apply extraterritorial jurisdiction for a sake of protecting its own vital interests, the primacy of the extraterritorial principle is not altered.

250. The ubiquity doctrine is often referred to in determining the place of commission. The offence will be considered to have been committed in its entirety within a country's jurisdiction if one of the constitutive elements of the offence, or the ultimate result, occurred within that country's borders. Jurisdiction is equally applicable to co-perpetrators and accomplices.

251. Common law countries also use the effects doctrine in addition to focusing on the physical act. This doctrine locates crimes in the territory in which the crime is intended to produce, or actually does produce, its effects. Thus, where various elements or effects of a crime may occur in more than one country, the two doctrines of territorial jurisdiction may lead to concurrent, legitimate jurisdictional claims.

252. These positive conflicts of jurisdiction, while at first glance not very problematic in determining the appropriate judicial response, do contain some inherent risks. The most fundamental problem is the general refusal, particularly in civil law systems, to apply the double jeopardy rule. Thus, the accused is submitted to a multitude of prosecutions for the same act.

253. Equally important is the manner of classification of the multiple acts potentially involved in a pattern of computer crimes. In particular, in cases of repeated data manipulation, data espionage or unauthorized access, it is unclear whether the acts should be considered as separate crimes or as a single act by application of the principle of international connexity, by which a single prosecution for the whole transaction would be justified.

254. States should, therefore, endeavour to negotiate agreements on the positive conflicts issue. These agreements should address the following issues:

An explicit priority of jurisdictional criteria: for example, of location of act over location of effect, of the place of physical detention of the suspect over in absentia proceedings or extradition;

A mechanism for consultation between the States concerned in order to agree upon either the priority of jurisdiction over the offence or the division of the offence into separate acts;

Cooperation in the investigation, prosecution and punishment of international computer offences, including the admissibility of evidence lawfully gathered in the other countries, and the recognition of punishment effectively served in other jurisdictions. This would prevent unreasonable hardship to the accused, otherwise possible by an inflexible interpretation of the territoriality principle.

## 2. Other base of jurisdiction

255. The issue of international computer crime also requires an analysis of the principles of extraterritorial jurisdiction. State practice discerns the following theoretical grounds:

The active nationality principle, which is based on the nationality of the accused. The principle, when applied in conjunction with the territoriality principle, may result in parallel concurrent jurisdictions, creating a situation of double jeopardy. The use of the active nationality principle is therefore generally confined to serious offences;

The passive personality principle, which is based on the nationality of the victims. This principle has been highly criticized, since it could subject a national of State A, although acting lawfully in State A, to punishment in State B for acts done in State A to a national of State B, if the acts were unlawful in State B and State B were to apply the principle. On practice, therefore, this principle is seldom used;

The protective principle, which is based on the protection of the vital interests of a State. By this principle, a State may exercise jurisdiction over foreigners who commit acts that are considered to be a threat to national security. Given the potential for abuse of this principle if

security is interpreted too broadly, the protective principle is not highly favoured; in practice, therefore, it is often linked to other doctrines, such as the personality principle or the effects doctrine;

The universality principle, based on the protection of universal values. It is usually effected on the basis of express treaty provisions but is otherwise rarely used. It is generally held that this principle should apply only in cases where the crime is serious, where the State that would have jurisdiction over the offence, based on the usual jurisdictional principles, is unable or unwilling to prosecute.

256. Other than the basic policy considerations as to whether a State should apply one or more of these bases of jurisdiction, it is unlikely that application of these principles of extraterritorial jurisdiction to information technology offences will create specific problems. Nevertheless, the characteristics of transnational computer crime do have the potential to involve an increasing number of States, thereby creating a jurisdiction network in which the ordering of the subsequent priorities is required.

257. There are no rules of international law, other than the principles of comity and non-intervention, that impose express limitations on the freedom of sovereign States in establishing extraterritorial criminal jurisdiction. Where there is strong international solidarity by way of customary or conventional international law, jurisdiction over important offences may be decided by the principle of universality, in addition to the applicability of other grounds of jurisdiction. No such conventions exist yet in relation to computer crime. Eventually, however, as has been the case in other major international crimes, international conventions will regulate this area.

258. A spirit of moderation might be expected from States in exercising these jurisdictional principles, in order to encourage international cooperation and to avoid significant conflicts of jurisdiction with other States. In that spirit, the passive personality principle, although sometimes used to protect the economic interests of nationals (natural or legal persons), is highly disputed, while universality is best limited to express treaty provisions. The protective principle may be relevant for certain types of computer offences, because it grants jurisdiction to a State over offences committed outside its territory, in the defence of fundamental (vital) interests.

259. There exists very little consensus on what constitutes vital interests. No doubt a sovereign State might consider attacks on data or telecommunication infrastructures, when related to basic government activities (police data, military data, State security systems etc.), to fall within its purview. However, a tendency may arise to consider certain economic interests, naturally involving a significant amount of transborder data flow, as a vital concern of the State. Nevertheless, caution is needed in regard to such extensions, since they can affect adversely the legitimate flow of information and data, as well as other economic and social interests. Therefore, the State concerned should be expected to take due account of the principles of cooperation, comity and reasonableness, which should govern State action in exercising extraterritorial jurisdiction.

260. Even if very few specific computer-related concerns seem apparent, the general issues in extraterritorial jurisdiction remain valid: the need for harmonized legislation (see paragraphs 268-273), the settlement of concurrent jurisdictional claims, the international validity of the non bis idem principle and the development of agreements on mutual cooperation and the transfer of criminal proceedings (see paragraphs 279-280).

#### C. Transborder search of computer data banks

261. One very specific transborder situation in relation to computer-related offences deserves particular attention. Within the international economic environment, in particular within multinational corporate structures, data are often stored centrally in one country (e.g. where headquarters are located), with on-line access available to company partners (e.g. subsidiary corporations) operating in the territory of other countries.

262. Criminal investigations in such situations are presented with the problem of how to retrieve the data, as potential evidence, that are stored abroad, when investigating by means of on-line access to that data. The question arises whether the investigating authorities may penetrate the database by direct access, without the intervention, knowledge or agreement of

the State in which the data are located. Urgent situations compelling the preservation of evidence may require that data be made readily available or, at least, that they be seized and blocked, thereby securing their evidential value. A suspect with sufficient speed and expertise in the access to and the functioning of the system could otherwise interfere with the data and make them unavailable by, for example, erasing them or transmitting them to another data bank.

263. Traditional means for cooperation between States in criminal cases do exist, in the form of conventional mutual assistance agreements, particularly the procedure of the letters rogatory. This procedure, however, by which a State is requested to undertake an investigation on its own territory on behalf of the investigating State, is highly time-consuming. The investigation of crime in the computer environment requires quicker, more efficient action. Another problem arises when a person, natural or legal, is compelled by the investigating State to produce data located in another State, whether or not they are available by on-line access, even though under the law of the State of storage that person is obliged to secrecy.

264. There is no unanimity today on the solution to these problems. However, the view that the deliberate investigation of on-line data constitutes a violation of the sovereignty of the other State is probably correct, whether it is done by the investigating authorities from the premises of the suspect or from their own terminals. In fact, such access might even be considered in the other State as a form of computer crime, such as unauthorized access.

265. The only explicit rule in international public law relevant to this situation seems to be the non-intervention principle, which historically has been applied only when foreign agents have operated physically on a State's territory. Nevertheless, the direct penetration of data banks appears very similar to acts of physical intervention by official foreign agents. The analogy is strengthened if the acts of penetration also constitute an offence in the other State. However, some people will probably resist the analogy and accept the legality of this penetration.

266. There is a definite need to address these questions, which are indeed not hypothetical ones, and to find solutions that balance the requirement of quick action with the appropriate respect for the sovereign rights of the other State in matters of police or investigatory action within its territory. States could, therefore, strive to conclude agreements that make direct penetration acceptable only as an exception. Any exception should, in addition, be subject to a number of stringent conditions, such as the following:

The freezing of data, by which any further operation on the data is rendered impossible, would be permissible only for preserving the data for evidentiary purposes;

The use of this evidence in the investigating State would be subject to the explicit consent of the State where the evidence was stored;

The right to penetrate data banks directly would be limited to serious offences only;

Sufficient indication must exist that the usual method of mutual assistance would, for lack of rapidity, compromise the search for evidence;

Upon commencement of the investigation, a duty would be imposed to immediately inform the authorities of the State being investigated.

267. The problem of on-line transborder searches of computerized data has not been adequately addressed so far. By virtue of not being cooperative acts, such actions do not fall within the traditional category of mutual assistance in criminal matters. However, the appropriate solution is not to view States as having a complete unilateral freedom to act, provided there is no violation of the non-intervention principle by physical interference. This potential area of conflict between States could be solved by a solution based on the principles mentioned above.

---

#### D. Mutual assistance in transborder computer-related crime

268. As discussed above, transnational computer crime can be efficiently addressed only if the countries involved agree to provide maximum cooperation in countering it. This cooperation is usually organized by multi- or bilateral conventions may give rise to a number of problems of which States should be aware.

269. First, as for other forms of international cooperation, the requirement of dual criminality may be an issue. Refusal of assistance could be based on the ground that the act in relation to which the request is made is not an offence in the territory of the requested State. Thus there is a clear need to make the substantive criminal law of computer crime correspond from State to State.

270. Even if the dual criminality rule is not an aspect of all incidents of mutual assistance, it is often a requirement in cases of search and seizure, which is a particularly important means of assistance where data are concerned. Double criminality, furthermore, is basic to other common cooperation modes, such as extradition, or other schemes for solving jurisdictional conflicts as discussed above. Unless domestic criminal legislation, as it develops, moves beyond expressions of sovereignty to espousing common principles as agreed among nations, conflicts will not be avoided. Efforts by States to harmonize their domestic laws will prevent conflicts of jurisdiction and, at minimum, will lay the basic groundwork for cooperation.

271. It is, therefore, imperative that States undertake action to achieve this aim. Such action may range from the undertaking of consultations among States prior to enacting domestic legislation; solutions for harmonization, such as recommended guidelines for national legislation; and the elaboration of a convention of substantive law that defines computer crime under international law, including the governing principles in jurisdiction and cooperation.

272. Secondly, a form of mutual assistance rendered to requesting States is the search and seizure of data banks or carriers that store or transmit information. The target of request is not the carrier itself but the intangible specific data. If seizure remains applicable only to physical objects, the carrier is still at issue. The technical storage capacity of such data banks and carriers often far exceeds the volume of content requested by the investigating State. Explicit rules should be elaborated in relation to the surplus of information a data bank or carrier might contain, which would allow the execution of letters rogatorys upon only the targeted data. Notions such as relevance, proportionality and defined purpose should necessarily be included.

273. A final concern relates to potential grounds of refusal, which almost uniformly include the protection of the essential interests of the requested party. Data that relate to the privacy of nationals, including, for example, financial or medical information, could be considered sufficiently sensitive by a State, in its role of protecting its citizens, to be an essential interest. Many computer-related investigations may concern tax fraud or violations of customs, import and export rules, equally subject to the essential public interest qualification. Again, it is to be expected that States interpret their treaty obligations in a practical manner, in a spirit of cooperation and international comity.

---

#### E. Extradition

274. Given the potential for multiple territorial and extraterritorial jurisdictions, resolving the resulting jurisdictional conflicts will often require an agreement between States. It is therefore possible that the effective exercise of an agreed jurisdiction will involve extradition, since the State of physical location of the suspect may not necessarily be the appropriate forum for prosecuting the crime.

275. The terms of traditional extradition treaties will remain applicable. Computer crimes do not appear to raise any specific difficulties, provided the requirements of the extradition law and/or treaty are met. The most important issues are the requirement, again, of double criminality, i.e. the impugned conduct would be an offence punishable under the law of both the requesting and the requested State, and the fulfilling of any other conditions that would include computer crime within the category of extraditable offences. This could be accomplished either by setting sanctions for the open formula, e.g. a maximum punishment of a certain number of months, or by including computer crime in the enumerated list of extradition crimes appended to the extradition treaty in question.

276. Both conditions require careful attention in the computer crime area. The first condition highlights once again the absolute need to legislate the substantive law in each State as consistently as possible, thus avoiding loopholes or conflicting interpretations of the

requirements of criminality. Currently, there is insufficient international discussion in the definition of computer crime, or at least on the constitutive elements of the most significant criminal behaviour. The efforts of OECD, the Council of Europe and the United Nations have not yet produced conclusive results. Nevertheless, the reports of these bodies contain sufficient indicators to allow States to formulate criminal laws that are consistent with the criminal laws of partner States.

277. The second condition, the extraditable character of the offence, requires an attentive legislative drafting policy. In particular, offences such as unauthorized access to computers or telecommunications facilities are often characterized as minor offences, and penalty scales may not meet the minimum threshold standards of extraditable crimes. Unfortunately, experience shows that transborder hacking cases are common, significantly affecting important transnational economic networks. It might be advisable to consider serious penalties, at least in cases where the hacking affects the international relations of the victim, whether the victim is a legal or physical person or a State. Disregarding the use of extradition or other cooperation methods could seriously hinder the efficiency of the cooperative response to this important and disturbing phenomenon.

278. Other important concerns, not specific to networking but potentially magnified by it, relate to grounds of refusal where the offence for which extradition is requested is, under the law of the requested State, viewed as having been committed in whole or in part within the territory of that State. A second problematic scenario is possible if the invoked ground for jurisdiction is an extraterritorial one but the law of the requested State does not provide such jurisdiction in similar cases. These situations might also create positive or negative conflicts of jurisdiction. The creation of channels of consultation or negotiation in order to solve such conflicts is highly recommended.

---

#### F. Transfer of proceedings in criminal matters

279. As mentioned above, the exercise of jurisdiction in transborder cases involves the possibility of competing claims, which may eventually lead to multiple prosecutions and bring about friction between States. The technique of transfer of proceedings offers a rather effective mechanism to solve this problem in a harmonious way. By creating agreements by which one State can waive its jurisdiction rights in favour of another State, conflicting claims can be resolved. The reason for such an initiative, beyond avoidance of jurisdictional conflicts, are the effective administration of penal justice, the interests of the victim and the reintegration of the offender into society. In case where multiple proceedings are pending in two or more States, a provision can be made for compulsory consultation to reach a settlement.

280. Few conventions of this type are in force today. The European Convention for the Transfer of Proceedings in Criminal Matters (1972), for example received a limited number of ratifications. However, the United Nations Model Treaty on the Transfer of Proceedings in Criminal Matters (General Assembly resolution 45/118, annex) represents an excellent basis for more effective international cooperation and deserves greater attention. The basic issues, e.g. the issues of double criminality and non bis in idem, remain similar to those in the other cooperation techniques, but again, any problems can be overcome. In the interests of the administration of criminal justice, which includes effective truth-finding and locating the most important or best items of evidence, agreements in this field may very well solve recurring, conflicting claims of jurisdiction while serving the interests of efficiency.

---

#### G. Concluding remarks and suggestions

281. In coping with the increase in transborder computer-related transactions, it is clear that a set of solutions elaborated by the international community represents an effective response. The problems predictable in confrontations among different States, whether common to all transborder crime situations or specific to computer crimes, require well-regulated solutions. Whether the problems are related to multiple jurisdiction conflicts, of a positive or negative nature, or to the requirements of mutual cooperation agreements, it is suggested that States should elaborate explicit rules to solve them.

282. Problems of concurrent jurisdiction based on the principle of territoriality are likely to be the most difficult to solve. Criminal law and jurisdictional questions are still integrated in national policy, and the implementation of that policy remains exclusively in the hands of the sovereign State.

283. Rather than seeking a solution through a conventional classification of priorities, a more effective action might be to develop a mechanism for mutual consultation and for allocating responsibilities on a case-by-case basis. A procedure for settling jurisdictional disputes by a body of experts knowledgeable in both jurisdictional issues and computer crime could also be developed. This could provide a speedy and flexible alternative to existing dispute-resolution mechanism, such as the Council of Europe Convention on Peaceful Settlements of Disputes.

284. It appears to be generally accepted that claims of extraterritorial jurisdiction are subsidiary to primary territoriality claims. Conflicts of extraterritorial jurisdiction should preferably also be settled by cooperative mutual consultation.

285. In the administration of criminal justice in a multi-sovereign environment, different cooperation techniques can be of relevance. Traditional techniques such as extradition or mutual assistance are generally applicable, provided that the basic requirements of double criminality and conditions for extradition are met. States must, therefore, operate with criminal laws that are as consistent as possible. Laws will be consistent only if there has been cooperation with international institutions such as the United Nations, the Council of Europe, the Organization of American States, the British Commonwealth of Nations, OECD and similar groups. The imposition of penalties sufficient to classify international computer crimes as serious offences is also required.

286. In the search and seizure of data, the mass storage of information in data banks and its transmission through carriers may necessitate additional safeguards, with regard to the criteria for limiting acceptable purpose of search and seizure and for determining relevance in the selection of the data.

287. Many key issues could be properly addressed by the more extensive use of, and consequent greater confidence in, a mechanism for transferring criminal proceedings. It would be advisable to develop conventional agreements that offer cooperative avoidance of conflict, mutual assistance and effective administration of justice.

288. Finally, and more specifically, the legality of direct access to computerized data stored abroad, for evidentiary purposes, should be examined to determine the appropriate balance between, on the one hand, preservation of evidence and efficient prosecution, and on the other hand, respect of exclusive sovereign territorial rights. The basis for a valid solution could be found by combining the notion of a right to immediate access to information for the purpose of freezing and conservation, with the requirement that clearance be given by the other State before the frozen data could be used as evidence. Few if any transborder problems in computer crimes will resist solution by appropriate, balanced legal rules. What is fundamental is the political willingness, in a spirit of international cooperation, to tackle a crime that has no frontiers.

---

## VII. CONCLUSION

---

289. This Manual has attempted to provide a broad overview of the newest forms of computer and computer-related crime. It has exposed the history, extent and complexities of this phenomenon. The complexities, intrinsic to the technology itself and to the vagaries of human nature, are exacerbated by the inadequacies of current law. The Manual has canvassed the various solutions that have been suggested and proposed some reform initiatives in the legal area. Pertinent issues for security in the electronic environment have been explored. In addition, the use of non-penal methods to combat this problem has been noted.

290. Many groups of experts in the computer and crime-enforcement fields have discussed, and continue to discuss, these issues. The discussions suggest that the phenomenon of computer crime has existed for some time and will not go away. Computer technology today is where automotive technology was in 1905. Significant developments lie ahead. Equally, we have not yet seen the full extent of computer-related crime.

291. Countries must be cognizant of the problem and realize its implications for their own social and economic development. Action must be taken at the national level to address the problem. This first step is not enough, however: computer-related crime is not merely a national problem, but an international one.

292. Given the international scope of telecommunications and computer communications, the transborder nature of many computer crimes and the acknowledged barriers within current forms of international cooperation, a concerted international effort is required to address the problem effectively. Attempts to define computer crime, or at least achieve common conceptions of what it comprises, and to harmonize the procedural processes for sanctioning it have a number of benefits:

A growing commonality of technology permits the transnational expansion of large-scale computer networks. This in turn increases the vulnerability of these networks and creates opportunities for their misuse on a transnational basis. Yet, concerted international cooperation can occur only if there is a common understanding of what a computer crime is or should be;

The expansion of international trade and commerce raises a concomitant need for laws that will adequately safeguard economic interests and facilitate, stabilize and secure economic activities. Likewise, the increasing computerization of data on the personal characteristics, attributes and socio-economic status of individuals, combined with a growing concern for privacy, engenders a corresponding need for legal protection, not only nationally but internationally;

International legal harmonization increases the ability of transnational business and other computer users to predict the legal consequences of criminal misuse of computer systems. Predictability leads to confidence and stability on the international investment market;

To the extent that criminal law establishes positive norms of conduct and serves to educate and deter, harmonization of the criminal law facilitates the creation of international norms of conduct for computer usage;

Harmonization can help to avert market restrictions and national barriers to the free flow of information and the transfer of technology. Business and Governments may otherwise refrain from exporting computer programs, data or technology to, or from establishing complex computer interconnections with, countries that do not have an effective system of legal protection;

The harmonization of laws, including criminal laws, could promote equal conditions for competition. The inadequate legal protection of computer programs, technology or trade secrets in some countries could cause some companies to operate there in a manner that would be considered by other countries to be unfair competition;

Better harmonization can prevent some countries from becoming havens from which international computer crime could be committed with impunity;

Harmonization facilitates law enforcement by the agencies of different countries because it provides a common understanding of what types of conduct constitute crime and, in particular, computer-related crime.

The harmonization of substantive law facilitates the extradition of alleged or fugitive offenders. Extradition treaties generally require dual criminality, that is, the conduct must be considered to be a crime under the laws of both countries and, sometimes, must be the same type of crime. Accordingly, harmonization of the concept and even the definition of crime can be crucial to the ability to extradite;

Harmonization facilitates mutual legal assistance, that is, the use of legally controlled investigatory powers, such as search and seizure, examination of witnesses, electronic surveillance etc., by one country for the benefit of another country. In some mutual assistance treaties, dual criminality is also required before one country will use its judicial or law-enforcement mechanisms to aid another country. Even where dual criminality is not a prerequisite, a common conceptualization of what constitutes a crime assists the law-enforcement and judicial authorities of the country in undertaking investigations within its own territory on behalf of a foreign country;

The harmonization of offences facilitates the harmonization of procedural law with respect to investigatory powers.

293. Much remains to be accomplished to achieve international cooperation. Most of the international work so far has been done in just a few regions of the world. The challenge for the future is to expand that cooperation to other portions of the international community. The potential for computer crime is as vast and extensive as the interconnections of worldwide telecommunications networks. All regions of the world, both developed and developing countries, must become involved in order to stifle this new form of criminality. Computer technologies will be increasingly important for developing countries attempting to achieve economic sufficiency. The implementation of security and crime-prevention procedures should be an integral aspect of technological progress in these countries, as should their cooperation in international computer-crime matters.

294. Cooperation in addressing computer-related crime must be developed and improved at both the national and international levels. At the national level, working groups could be established to address the relevant issues. These groups could draw their members from various disciplines and fields, including government, industry and learned societies. They could commence by examining the experience acquired in the field, including the material set forth in this Manual, and by conducting a similar analysis of their own national situations and laws. They could also consider adopting the following measures:

Reviewing the present state of legislation in light of the issues raised in this Manual, assessing the substantive and procedural adequacy of their legal and administrative infrastructures and recommending appropriate solutions;

Cooperating in the exchange of experience and information about legislation and judicial and law-enforcement procedures applicable to computer crime. This would foster international cooperation and the understanding of common problems;

Undertaking a review of sentencing legislation, policies and practices with a view to developing more effective penal sentencing provisions. International cooperation in sentencing reform would ensure the uniform treatment of computer-crime offenders and could prevent computer offenders from relocating to jurisdictions where computer misuse might be treated more leniently;

Ensuring periodic reviews and reform of laws, policies and practices in order to incorporate changes arising from technological developments and trends in computer crime;

Inviting educational institutions, associations of hardware and software manufactures and the data processing industry to add courses on the legal and ethical aspects of computers to their educational and training curricula, with a view to preventing the misuse of computers and creating ethical standards for the respective sectors;

Developing a mechanism to educate potential victims of computer crime and to expose the real extent of computer crime. The active involvement of victims should be encouraged in developing prevention programs and victim assistance programs that are commensurate with the scope of the problem;

In view of international character of data-processing and information technology, sharing security standards and procedural techniques among all sectors of the industry, both nationally and internationally;

In consultation with groups in other countries, and in order to keep abreast of advances in modern computer crime, consolidating and facilitating law enforcement efforts, including the development of and training in innovative techniques for investigative and prosecutorial personnel;

Implementing voluntary security measures by computer users in the private sector;

Imposing obligatory security measures in certain sensitive sectors;

Encouraging the creation and implementation of national computer security legislation, policies and guidelines;

Encouraging management and senior executives to commit their organizations to security and crime prevention;

Incorporating and promoting the use of security measures in the information technology industry;

Developing and promoting computer ethics in all sectors of society, but especially in educational institutions and professional societies;

Developing professional standards in the data-processing industry, including the option of disciplinary measures;

Educating the public about the prevalence of computer crime and the need to promote computer ethics, standards and security measures;

Promoting victim cooperation in reporting computer crime;

Training and educating personnel in the investigative, prosecutorial and judicial systems.

295. At the international level, further activities could be undertaken, including the following:

Within regional groups or associations, conducting comparative analyses of substantive and procedural law relating to computer crime;

Attempting to harmonize substantive and procedural law among the States of a region by developing guidelines, model law or agreements;

When negotiating or reviewing treaties on extradition, mutual assistance or transfer of proceedings, whether bilateral or multilateral, addressing the following issues, taking into account human rights, including privacy rights, and the sovereignty of States:

Ensuring a jurisdictional base for the prosecution of transborder, computer-related crime and enacting mechanisms for resolving jurisdictional conflicts;

Imposing obligations to extradite or prosecute offenders;

Facilitating mutual assistance, particularly regarding synchronized law enforcement, transborder search and seizure and the interception of communications.

296. To ensure that human rights principles, privacy rights and international legal principles are effectively balanced, model treaties on criminal matters, such as those developed by the United Nations, can provide valuable guidelines. The implementation of security and crime prevention measures should be concomitant with technological development. The time to act is now.