United Nations

A/58/373

General Assembly

Distr.: General
17 September 2003
English
Original: English/French/Russian/
Spanish

Fifty-eighth session
Item 69 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Contents

[*] A/58/150.

I. Introduction

1. In paragraph 3 of its resolution 57/53 on developments in the field of information and telecommunications in the context of international security, the General Assembly invited all Member States to continue to inform the Secretary-General of their views and assessments on the following questions: (a) general appreciation of the issues of information security; (b) definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunication systems and information resources; and (c) the context of relevant international concepts aimed at strengthening the security of global information and telecommunication systems. In paragraph 4 of the resolution, the General Assembly requested the Secretary-General to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, and to conduct a study, with the help of a group of governmental experts to be established in 2004 and whose members would be appointed by him on the basis of equitable geographical distribution, as well as with the help of Member States in a position to render such assistance, and to submit a report on the outcome of the study to the General Assembly at its sixtieth session.

2. By a note verbale dated 18 February 2003, all Member States were invited to inform the Secretary-General of their views and assessments on the subject. To date, seven replies have been received, the texts of which are reproduced in section II below. Additional replies received will be issued as addenda to the present report.

II. Replies received from Member States

Bolivia

[Original: Spanish]
[17 June 2003]

Developments in the field of information and telecommunications in the context of international security

1. Bolivia is concerned that technological developments could be used for purposes that are incompatible with international stability and security and that have a negative effect on the integrity of the State, in particular its military and civil security.

2. It is essential to make sure that information technology resources are not used for criminal or terrorist purposes.

3. Accordingly, Bolivia wishes to set out the following basic criteria concerning information security and unauthorized interference in related systems:

The importance of information

4. When we speak of information we are referring, directly or indirectly, to information technology and telecommunication systems (new technologies, new software, new hardware, new ways of elaborating ever more consistent, reliable and speedy information) and, in particular, the risk and security of such systems.

5. We should bear in mind that the place where information is centralized can often be very secure and, at the same time, very vulnerable.

6. Given the vulnerability of telecommunications, particular attention should be given to the Internet and telephone services. The Internet is directly related to information technology systems. Telephone services are divided into cellular and land line services. Cellular services share a common transmitting space, where radio waves travel, and where users are immersed in telephone traffic and interception.

Overview of offences relating to information system

7. Incidental and accidental offences committed using computers and receivers have increased in gravity, form and diversity. Nowadays, most offences are discovered accidentally (fraud, counterfeiting and the sale of information).

8. Regarding the management of information systems, we have to consider computer viruses, programmes elaborated accidentally or intentionally that require particular attention and that must be countered with strict operating procedures.

9. It should be emphasized that, when a problem is encountered, it is important to consider the motive for the offence and to propose solutions immediately. The motives that pose the greatest risks include: personal gain, the Robin Hood syndrome, hatred of an organization, mental illness and dishonesty; the motives that pose the least risks include organizational benefit and games.

Organizational paradigms concerning security

10. Paradigms play an important role in the current philosophy of science, and the rules governing investigations derive from them.

11. The following are among the principal paradigms: responsibility for auditing the system rests with the user and the internal audit department; security systems do not contemplate the possibility of internal fraud; accidents are unlikely to occur in an institution; there will always be errors because no system is perfect; there are many others.

Identifying the risk

12. It is important to create awareness among the users in an organization about the risks facing information so they understand that security is part of their work. To this end, it is necessary to establish the cost and quality of the security system, assess its installation in terms of risk, identify high-risk applications, quantify the impact of the suspension of services, and formulate the required security measures.

13. When the degree of risk has been determined, the next step should be to draw up a list of preventive measures and of measures to be taken in case of a disaster, indicating the priority of each.

14. The risk should be considered and quantified at the institutional, regional and State level and an indication given of the availability and retrieval possibilities of support programmes.

Considerations of an integrated security system

15. Developing a security system means "planning, organizing, coordinating, directing and controlling activities related to maintaining and ensuring the integrity of the resources involved in the information system, as well as safeguarding the assets of the institution, the region and the State".

16. To do this, we must define administrative elements and security policies, organize and distribute responsibilities, establish emergency procedures, define security goals, make a diagnosis of the risk and security status of the information and, finally, draw up a security plan.

Cuba

[Original: Spanish]
[28 May 2003]

1. Cuba has supported the resolutions on "Developments in the field of information and telecommunications in the context of international security", ever since the item began to be considered by the First Committee of the United Nations General Assembly in 1998.

2. The fact that the item has been placed on the agenda of the General Assembly shows that the international community is becoming aware of the potential danger for peace and security, when information technologies are not used for peaceful means.

3. The preparatory process and the organization of the two-stage World Summit on the Information Society, Geneva 2003 and Tunis 2005, has brought the item covered by the said resolution and others that are closely related to it, to the forefront of the international community's attention.

4. The hostile use of telecommunications, with the declared or hidden intent of undermining the legal and political order of States, is a negative manifestation of the use of these means, which can give rise to tensions and situations that are not conducive to international peace and security, in open contradiction to the principles and purposes embodied in the Charter of the United Nations.

5. Resolution 57/53 explicitly states that the dissemination and use of information technologies and means affect the interests of the entire international community and that optimum effectiveness is enhanced by broad international cooperation.

6. In its eighth preambular paragraph, the resolution expresses "concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields".

7. Furthermore, operative paragraph 3(b) requests all Member States to provide their views and assessments on the definition of basic notions related to information security, "including unauthorized interference with or misuse of information and telecommunications systems and information resources".

8. Cuba understands "unauthorized interference" to mean the use of these systems outside procedures and norms agreed upon internationally, particularly

within the framework of the International Telecommunication Union (ITU), and in violation of the relevant national regulations.

9. Those States which have not yet done so, should take all necessary measures to strengthen such national regulations.

10. Moreover, international regulations in this field must be reviewed periodically, given the speed at which the corresponding technologies are developing, in order to ensure that their effectiveness and efficiency keep pace with such development.

11. Information and telecommunication systems can become weapons when they are designed or used to cause harm to a State's infrastructure. For example, attacking national networks with foreign software or from sources within the State, but promoted or conceived from abroad; radio and television broadcasts intended to disrupt the social order and the institutional framework deriving from the Constitution of another State to which these signals are sent; activities intended to interfere with, damage or paralyse the broadcasting services of other States, etc.

12. Cuba reiterates that all States must respect existing international norms in this field. Access to the information or telecommunication systems of another State should accord with the international cooperation agreements that have been concluded, based on the principle of the consent of the State concerned. The type and scope of exchanges must respect the legislation of the State whose system will be accessed.

13. An attack by one State on the information or telecommunication systems of other States can undermine international peace and security. Unfortunately, such tactics are already used as tools to carry out hostile policies.

14. Cuba suffers from attacks of this nature, which have been instigated, tolerated and executed by the United States Government for almost 20 years. Since 1985, when the latter illegally established a radio station, and 1990, when it set up a television station, Cuban radio and television broadcasts have been affected and interfered with. Every week, these government radio stations and others, transmit towards our country more than 2,220 hours of subversive programming against the constitutional order. Twenty-four frequencies are devoted to programming specifically to this end.

15. Since 1990, the United States Government has invested more than $20 million a year in these radio and television attacks.

16. As indicated in the statement from the Ministry of Foreign Affairs of the Republic of Cuba on 22 May 2003, the United States Government has initiated new activities that represent an escalation in the radio and television attacks it has been waging against Cuba for decades.

17. On 20 May 2003, the radio station created and operated by the United States Government to promote subversion in Cuba transmitted on four new frequencies, affecting and interfering with Cuban radio transmissions.

18. These acts constitute a blatant and flagrant violation of international law and of the norms and regulations established by the International Telecommunication Union, the international organization established to promote efficient telecommunication services throughout the world, and, in particular of its Radio Regulations.

19. During the afternoon of 20 May, between 6 p.m. and 10 p.m., the official United States propaganda services, using an EC-130 airplane of the United States Armed Forces, transmitted towards Cuba television signals with a similar objective on channels legally assigned to Cuban television stations and duly registered with the above-mentioned international organization.

20. This action also violates international law and the norms agreed upon by all States within the framework of the International Telecommunication Union, particularly number 23.3 of its Radio Regulations, which prohibits television transmissions beyond national borders.

21. These television transmissions also violate the preamble to the Constitution of the International Telecommunication Union in that these activities do not facilitate peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunication services.

22. Therefore, Cuba rejects and denounces the tolerance which the United States authorities have shown for the activities of the terrorist, José Basulto, and his attempts to transmit television signals towards Cuban territory. Even though it was duly announced through the diplomatic channel that Mr. Basulto had been warned that any transmission towards Cuba would be considered a violation of United States law and result in action being taken against him, on 20 May, this known terrorist was able to fly unhindered; while he did not transmit, this was due to problems with the transmitter he was going to use rather than to the actions of the United States authorities, which acted in blatant complicity.

23. In accordance with number 15.34 of the ITU Radio Regulations, the television attacks by the United States constitute harmful interference, caused by a television station operating on Channel 13 VHF (210 to 216 MHz), which seriously affected Cuban television services duly registered on this channel.

24. Cuban radiocommunication authorities have reported this to the Federal Communications Commission (FCC) of the United States Government, describing all the technical and legal parameters that have been flagrantly violated.

25. Cuba is also taking steps to report these facts to the Secretary General of the International Telecommunication Union and to request that appropriate measures be taken.

26. Cuba considers that it is necessary to reinforce the international legal framework for information and telecommunications. It is also essential that the international order that has been established in this area should be respected, in accordance with full respect for international law and the Charter of the United Nations, which should have primacy in relations between States. Indeed, relevant international principles, regulations and procedures already exist and they should be respected.

27. It is imperative to work towards the formulation of non-binding guidelines and also towards the adoption of norms which can take the form of multilateral and legally binding international agreements or protocols.

28. Both methods should take into consideration basic criteria such as unauthorized interference or the misuse of information and telecommunication systems and information resources; aspects of sovereignty associated with these topics; the peaceful use of the means of information and telecommunications in all

its aspects; the promotion of international cooperation so as to encourage the development of information and telecommunication systems in developing countries, based on the crucial impact of information and communication technologies on socio-economic development; the prevention, tackling and eradication of hostile practices in the use of these systems and the application of national measures to establish greater State control over information and telecommunication systems and deal with the corresponding criminal acts.

29. In addition to the elements described above, Cuba considers that attention should be drawn to the following aspects that are closely associated with making full use of telecommunications as an instrument to facilitate international peace and security:

- All States must refrain from applying unilateral coercive measures — which are contrary to international law — to restrict the affected State's access to technologies and to international networks for the exchange of information and communication.

- The systems relating to certification of and possible sanctions on any State as regards access to telecommunication or other closely related technologies by reason of posing a threat to international peace and security, should be multilateral in nature and based on standards adopted by the international community.

- International cooperation in this area should be strengthened and the necessary resources should be mobilized in order to help developing countries enhance and expand their telecommunication systems.

- Legislative and other measures should be adopted, at both the national and the international level to prohibit undue concentration in private hands of ownership and control of the telecommunication media — as well as other means of information and communication — because of the negative impact this would have on the necessary diversity of information sources and could be used as a tool for propaganda against peace and incitement to war.

- A multilateral, intergovernmental, democratic and transparent system should be established for the administration and control of the Internet and other international information and communication networks. It is vital that the monitoring system be intergovernmental in nature.

- The systems for controlling and monitoring telecommunications and other forms of international communication should be multilateral and transparent, with clear responsibilities and public scrutiny procedures, so as to put an end to the violations of the privacy, sovereignty and security of many States, that occur with the global spying systems developed by some industrialized powers, in particular the United States.

- Firm guarantees of respect for cultural diversity should be developed so as to eliminate all forms of discrimination or incitement to hate in the content of the information disseminated by international telecommunication systems.

El Salvador

[Original: Spanish]
[30 June 2003]

1. Article 24 of the Constitution prohibits interference with and intervention in telephonic communications; this is the constitutional framework in force in El Salvador with regard to the security of information and telecommunications.

2. Under Articles 184, 185, 186 and 302 of the Penal Code seizure of written communications, computer hardware and any other personal effects or documents not addressed to oneself, or of confidential information of a personal or family nature constitutes a punishable offence, as does any act involving the receiving of communications, such as intercepting or interrupting telegraphic or telephonic communications and interfering with and intervening in them, by means of technical devices to listen in on or to record such communications.

3. None of the foregoing constitutes an offence if a person is receiving threats, demanding payment of ransom for a person who has been kidnapped or abducted or if organized crime is involved and the victim or his representative, whichever is applicable, requests or gives permission in writing for the Office of the Attorney General to listen in on or to record the conversations or acts through which such threats or demands are made.

4. The application of the telecommunications regulatory framework and the imposing of administrative sanctions is the responsibility of the General Superintendency of Electricity and Telecommunications, pursuant to article 4 of the act that created this office and article 29 (b) of the Telecommunications Act, which establishes protection for the secrecy of communications.

5. During 2001 and 2002, a proposed amendment to the Constitution was submitted to the Legislative Assembly, so as to allow telephone interference and/or intervention as a mechanism to assist in the fight against organized crime and drug-trafficking. To date, this proposal has not been adopted.

Georgia

[Original: English]
[24 June 2003]

1. The Government of Georgia is in the process of creating national information strategy aimed at development of the telecommunications field and promoting new technologies, underlining at the same time importance of State policy for securing use of information technologies.

2. Furthermore, the Government of Georgia adopts policies towards integration of Georgia into the global information society, again being aware of all the risks and challenges existing in terms of security of information.

3. The Government of Georgia deems it extremely important to take part in international programmes and cooperative projects intended for establishing a more secure international information society with the understanding that given the current realities of information technologies and systems, as well as the

particularities of the region Georgia is in, it is impossible to deal with the issues of information security unilaterally.

Russian Federation

[Original: Russian]
[28 April 2003]

Issues connected with the work of the group of governmental experts on information security

1. In accordance with General Assembly resolutions 56/19 of 29 November 2001 and 57/53 of 22 November 2002 on developments in the field of information and telecommunications in the context of international security, which were adopted by consensus, a group of governmental experts is to be established in 2004. Under those resolutions, the group of governmental experts will be asked to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them, conduct a study of relevant international concepts aimed at strengthening the security of global information and telecommunication systems and submit a report on the outcome of the study to the General Assembly at its sixtieth session.

2. The Russian Federation believes that international information security continues to be important and is increasingly topical and has now become a central issue in the national security of States and part of the overall system of international security and strategic stability. The use of information and telecommunication technologies and methods is directly related to the establishment of military and political security in countries throughout the world, and it should therefore be considered in a global, comprehensive and non-discriminatory manner with the participation of as many countries as possible on the basis of the principle of equitable geographical distribution.

3. Consideration of the issue under the auspices of the United Nations would provide just such an approach. As an important international organization which most fully represents the interests of all countries and plays a coordinating role in the area of disarmament, the United Nations provides a foundation for a balanced and effective system of global security.

4. We believe that General Assembly resolutions 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001 and 57/53 of 22 November 2002 have played an important part in exploring the whole range of issues connected with international information security and developing suitable recommendations. By tradition, they were adopted by consensus and therefore reflect the views of the whole international community, as well as the assessments of States on issues of information security contained in reports of the Secretary-General of the United Nations (A/54/213, A/55/140 and Corr.1 and Add.1, A/56/164 and Add.1 and A/57/166 and Add.1).

5. The seminar on international information security matters organized by the United Nations Institute for Disarmament Research and the Department for Disarmament Affairs of the United Nations Secretariat in Geneva in August 1999, in accordance with the recommendations set out in resolution 53/70, in which

representatives of more than 50 countries participated, played an important role in determining the approach to current issues relating to international information security.

6. The seminar confirmed that information security was an urgent matter and that it was time to include it in the international agenda. It also provided an opportunity to determine a variety of ways of addressing the essential nature of the issue. There are currently no generally accepted appropriate international standards or instruments dealing with questions of information security from the standpoint of measures to reduce existing and potential global threats to information security.

7. There is therefore a need for a joint effort, involving as many countries as possible, to study existing concepts and approaches in this area and analyse current international legal provisions relating to various aspects of international information security.

8. We believe that the establishment of the group of governmental experts on information security will move international, multilateral discussion of this matter to a qualitatively new phase. The group will give the international community a unique opportunity to examine the entire range of issues involved.

9. The Russian Federation would like to play a constructive part in the work of the group of governmental experts and would therefore like to raise a number of issues which it believes might be included in the group's agenda.

10. In considering issues of international information security, it is important, above all, to adhere to such human values as guaranteed universal, free, equitable and secure international exchanges of information on the basis of generally accepted standards and principles of international law.

11. The group should take into account the assessments received from States, in accordance with the General Assembly resolutions on international information security and other material which may be referred to it for consideration.

12. In our view, the group could focus on the following issues, which we consider of central importance:

13. First, it should agree on an appropriate conceptual system of international information security. The main goals at that stage of the activities of the group of governmental experts could be to develop basic definitions relating to information networks, resources and systems, information infrastructure and information weapons, and to determine characteristics, hallmarks, descriptions and classification of threats to information security.

14. Second, it should examine the factors influencing international information security. This is a complicated and complex field and the international community must take a comprehensive approach, taking into account terrorist, criminal or military threats, in both the civil and military fields.

15. In the emerging global information society, information and communications technologies are interlinked and transcend borders. For that reason, within the global information community, international information security is inextricably and naturally connected with questions relating to the identification of the source of threats of an internal or external nature and issues of State sovereignty and respect for human rights and freedoms, in particular the right to non-interference in one's

personal life. These and related matters could provide a basis for discussion within the group of governmental experts.

16. The next stage could be to determine mutually acceptable measures to prevent the use of information technologies and methods for terrorist and other criminal purposes, as well as measures to restrict the use of information weapons, particularly when such weapons are targeted at the critical infrastructure of States. It would seem that the goals at that stage would be to examine the potential for developing procedures for mutual notification and the prevention of unsanctioned cross-border influence of information technology, the establishment of a system of international monitoring to track threats which may appear in the information area, a mechanism to monitor implementation of the arrangements for international information security, and a mechanism to resolve conflict situations relating to information security, and the establishment of conditions to govern an international system of certification of information and telecommunication technologies and methods (including those connected with software) in order to guarantee information security.

17. Thought should be given to the possible avenues of international cooperation between law enforcement agencies to prevent and halt offences in information space and, in particular, to identify sources of cyber attack. The issue of harmonizing the national legislation of individual countries governing information security should be considered in order to achieve a uniform classification of information security offences and liability for actions classified as criminal.

18. It is also proposed that consideration should be given to the possibility of providing international assistance to countries which have suffered cyber attacks, in order to mitigate the effects of disruption to their normal operations, especially attacks to their critical State infrastructures.

19. In the longer term, efforts should perhaps be made to develop a multilateral, mutually acceptable international legal document aimed at strengthening international legal security arrangements. This would provide that States and other subjects of international law must bear international liability for activities in information space which they carry out or which are carried out from territory under their jurisdiction.

20. The Russian Federation believes that the basis of a universal international information security regime might be the obligation on participants to refrain from activities in information space aimed at causing harm to the information networks, systems, resources and processes of another State or to its infrastructure, or aimed at disrupting its political, economic and social system or psychologically manipulating the population in order to destabilize society and the State.

Senegal

[Original: French]
[9 June 2003]

1. Measures relating to telecommunications and information security come into play in connection with the exchange of information particularly information concerning arms trafficking. Such information must remain confidential.

2. Consequently, it must be safeguarded by a certain number of measures, to ensure, inter alia:

- the security of materials, software and data processing, by the installation of specific technical devices;
- the security of procedures for the exchange of information, by specific and exclusive regulations.

Ukraine

[Original: Russian]
[27 May 2003]

1. General assessment of the issues of information security

1. The international process of globalization, the introduction of new information technologies and the emergence of the information society all underline the significance of information security as an element of national security.

2. The development of a State's information infrastructure and the creation and introduction of new information technologies give rise to certain specific risks to information security. Among the most important are deliberate threats, which may arise as a result of objective or subjective differences in the spiritual, intellectual or material interests of the individuals concerned and the ways and means in which their aspirations may be met. This may, in some cases, give rise to conflict situations.

3. The main threats to information security include:

- Manipulation of information (disinformation, concealment or distortion of information);
- Contravention of established methods of information exchange, unsanctioned access or unjustified restriction on access to information resources, or the unlawful collection or use of information;
- Destruction of a State's information space or its use for anti-State purposes;
- Information terrorism, for example through the dissemination of computer viruses, the bugging of programs or apparatus, the installation of radio frequency devices for the interception of information in technical facilities or premises, the unlawful use of information and telecommunication systems and information resources, the peddling of false information, etc.

4. One direct result of negative information effects is misinformation, which leads to the distortion and/or destruction of a State's information environment and its information resources, as well as the inability of important State, industrial, financial, academic or general cultural systems to function, with the result that national sovereignty over information is lost.

5. Consideration of issues of information security thus shows that, in addition to more general problems, there are also problems in maintaining the essential range and quality of information resources, elaborating strategies for their use in conjunction with appropriate information technologies, establishing an adequate

information infrastructure, maintaining information security in information and telecommunication systems and combating negative activities that affect individuals, society and the State as a whole.

6. An inadequate level of protection for a State's information resources may involve it in significant economic damage owing to depreciation and loss in its industrial and information technology trade sector and also a substantial loss of national security as a whole as a result of possible breakdowns in the normal functioning of the systems of communication, monitoring and administration, the leaking of information concerning State secrets, and the like.

7. Information security depends on the adoption of measures to protect information at every stage. The aim of information security is to ensure the integrity of the system and protect and guarantee the accuracy and integrity of the information and also to minimize any consequences that may arise if such information is altered or destroyed.

8. One feature of the modern world is the use, in various spheres of social and State activity, of local and global information systems intended to speed up the exchange of information and access to a variety of information resources.

9. The widespread introduction of such systems, particularly in spheres of activity connected with State administration, has created real possibilities for unsanctioned access to State information resources and control systems, for the dissemination of unlawful information, for the destruction of the integrity and accessibility of information, etc.

10. The stable functioning of the political, economic, military, financial and other aspects of State activity depends on the reliability, as well as the efficiency of telecommunication and information systems. Where an information space is being established, the reliability and protection of information and telecommunication systems that serve the interests of State administration take on particular importance and relevance. Not only does access to information systems make valuable information available but, through the disruption or blocking of the work of information systems, it is possible to paralyse, wholly or partially, the activities of important aspects or even whole areas of the economy, to exert a detrimental effect on information resources, to disseminate information that is prohibited by law and so on.

11. Ensuring the security of information contained in information and telecommunication systems is one of the main factors in, and a precondition of, the guaranteeing of information security, national and State sovereignty and stable social development.

12. At the present stage of the development of information and telecommunication systems, the main threats to the information that they contain include:

- Disruption of the ordered functioning of important information and telecommunication systems;
- Accidental or deliberate acts resulting in the breakdown of the confidentiality, integrity and accessibility of information;

– Interference with information systems (dissemination of computer viruses, installation of bugging programs and apparatus, use of interception devices in technical facilities and premises, information interception and decipherment, peddling of false information, radio frequency interference with key password systems, the jamming of lines of communication and control systems, etc.).

13. Information and telecommunication systems, especially those relating to State administration, can be reliably protected from criminal encroachment only by the establishment of a complex information protection system, which would include the use of cryptographic and technical protection measures, together with a range of organizational and technical approaches.

14. Particular attention should be paid to the question of linking computer networks to international information networks.

15. Ukraine's entry into the international community cannot be fully realized unless cooperation with global information exchange networks such as the Internet is expanded. Such systems provide a wide choice of modern information and telecommunication services, many of which are advertised as providing protection for information.

16. At the same time, the wide variety of devices used in such systems, the special features of which are hard, if not impossible, to assess without access to previous programming codes, pose a threat to the security of information, financial transactions and electronic payments. Countless cases are known of the incautious use by banks of imported information technology that an expert can use to penetrate the system in a single 10-minute session.

17. Attention must be paid to the danger arising when servers and local networks are connected to global networks without due preparation. Practically any local computer network connected to the Internet can easily be accessed by hackers if it is not provided with appropriate protection measures.

18. The new ways and means of passing information between countries and, in particular, the increasing popularity of new forms of entrepreneurial activity using the Internet (electronic commerce), together with the gradual introduction of electronic control systems, have been accompanied by a widespread use of computer technologies and a wider range of information in electronic form. As a result, objects of information links become increasingly dependent on the degree of protection provided for that information, which, in turn, is targeted by negatively disposed elements of society and their associates. The incompatibility between existing protection systems and mechanisms creates a real potential for the unsanctioned access, use, blocking or obliteration of information created, processed, transferred or stored in electronic form.

19. The problem of interference with a State's information resources is a topical one throughout the world. Whereas before the beginning of the 1990s the crucial issue was to protect the State from foreign espionage, in recent years, the problem of combating so-called computer crime has become the more urgent, owing to the widespread introduction of information technologies into all aspects of national life. This is evidenced by the fact that computer crime is internationally recognized as a new form of intellectual crime. Moreover, such crime is committed not only by organized criminal groups but also by terrorist organizations and individual criminals.

20. Criminals are particularly attracted by the information systems used by State organs, law enforcement, customs and tax agencies, finance and credit institutions, the military and so on. In Ukraine, the law enforcement agencies have, on more than one occasion, detected illegal operations involving the use of the plastic cards used in international payment systems and the execution of fictitious electronic payments with a view to illegally obtaining money or interfering with the activities of computer networks through the Internet, etc.

2. Definition of the fundamental concepts of information security, including unauthorized interference in or unlawful use of information or telecommunication systems or information resources

21. The intensive development of information and telecommunication technologies is exacerbating the problem of ensuring information security, including the question of unauthorized interference in or unlawful use of information and telecommunication systems and the question of the protection of information resources.

22. In this context the term “information security” must be understood as the kind of protection of a State’s information space that allows the attainment of its national interests and observance of the rights of the individual, society and the State.

23. In view of the considerable social risks associated with the unlawful activities mentioned above and of the importance of the efficient functioning of information and telecommunication systems, the Criminal Code of Ukraine defines offences connected with the use of computers and computer systems or networks and sets out the corresponding penalties for commission of such offences, specifically:

- Unlawful interference in the working of computers or computer systems or networks: acts resulting in the distortion or destruction of computerized information or carriers of such information or in the dissemination of computer viruses by means of software or other technical devices with the intention of unlawfully penetrating computers or computer systems or networks;

- Theft, appropriation or extortion of computerized information or the acquisition thereof by deception or abuse of an official position;

- Violation of the operating rules of automated computers or computer systems or networks by a person responsible for their operation: acts resulting in the theft, distortion or destruction of computerized information or the means of its protection, in the unlawful copying of computerized information or in substantial disruption of the working of computers or computer systems or networks.

24. In short, the term “computer offence” may be defined as an unlawful act which encroaches on the established procedure for the operation of information technology systems or the procedure for access to them or which damages the integrity, confidentiality or accessibility of the information and the rights and freedoms of citizens in the course of information technology operations.

3. The content of international concepts designed to strengthen the security of global information and telecommunication systems

25. The twenty-first century will go down in history as the period of the birth and development of the global information society, which will consolidate or extend material processes with processes of information technology and help to bring about a substantial improvement in the productivity of labour and in social well-being. Many countries are already creating the organizational and technical basis of national and global infrastructures. The United Nations addresses the question of the delivery of the right of access to the basic means of communication and information in the Universal Declaration of Human Rights.

26. The experience of the developed countries in finding effective solutions to the problems of disseminating information technology in the second half of the 1990s, which has been formally compiled by international organizations (International Telecommunication Union, International Organization for Standardization/International Electrotechnical Commission, European Telecommunications Standards Institute) and many national standardization organizations, argues for the need to create multilevel (national and regional) information technology infrastructures and subsequently to combine them in the Global Information Infrastructure (GII).

27. Europe’s participation in GII signifies not only the creation of national information infrastructures within the European region but also assistance with the building of such infrastructures in individual countries for the common benefit of every country in Europe as a whole. Instead of talking about a “European Information Infrastructure” the Europeans prefer to use the term “European Information Society (EIS)”. The building blocks of EIS are its networks, basic services and additional services. The existing European networks may be strengthened by the introduction of a European broadband superhighway, which will combine in a single whole all the European telecommunication, cable and satellite services. The European countries support the use of trans-European basic services, including electronic mail services and the transmission of files and videos.

28. The European countries are also devoting much attention to the social aspect of the next stage of the world technological revolution. The Council of Europe has produced resolutions and documents on the formation of national policy relating to the building of the information society. This is perceived not as a tribute paid to fashion but as a necessary condition of development, the rejection of which will result in a loss of impetus and a retreat from the foremost economic and technological positions.

29. World trends in the legal regulation of activities connected with the latest data-transmission technologies testify to the need to formulate unified approaches to the creation of legislative and standardization instruments for all the participants in the international exchange of information. In the view of the American Association of Jurists, there already exists today a real demand for the creation of a multinational commission on cyberspace legislation. The establishment of a “cybercourt” is one of the most important items on the list of issues recommended for consideration by the future commission. At the present stage the main problem of legislation relating to information security is the need to adapt the existing legal rules to advances in information technology.

30. It is impossible today to imagine an information space without computer networks. It was precisely this technology which prompted the emergence and development of many types of business: electronic accounting cards, operational inter-bank settlement, stock-exchange services, brokerage services, etc.

31. It is expected that by 2005 one half of the population of the European Union will have access to the Internet. The countries of the European Union are therefore directing their efforts towards building up confidence in commercial and financial operations through the Internet and speeding up the transition to electronic commerce.

32. On 7 May 1999 the European Parliament reached agreement on a draft version of INFOPOL 98, which authorizes the competent agencies lawfully to engage in network monitoring. This was in fact a draft Council resolution on the lawful interception of telecommunications in relation to new technologies. This document calls for access by the agencies carrying out the monitoring in real time to all telecommunications networks, including the Internet and telephone satellite systems. The United Kingdom Government has begun to implement a project on the establishment of a centre for the interception of all electronic traffic within the country.

33. The Government of China is controlling access to the Net by licensing the use of modems, and all Internet information flows pass through a limited number of national operators.

34. Attention may be drawn to the following problems of information security:

– Infringement of intellectual property rights;

– Dissemination of information having a harmful influence on people’s social health, including problems connected with children’s access to the Internet;

– Conduct of unlawful commercial operations;

– Unauthorized access to confidential information;

– Infringement of the rights and lawful interests of individuals in the course of the exchange of information;

– Dissemination of low-grade advertising.

35. There is a further danger connected with the Internet — the possibility of using a person’s confidential information without his or her permission. It is possible to acquire such information by analysing the use which the person makes of the Internet.

36. The Internet is a very specific means of communication which, because of its transboundary nature, is difficult to subject to legal regulation. All Internet users are subject to the laws of their own country. But unlawful content may be displayed in the territory of a country other than the one where it is held in a server. International agreements are essential for the regulation of legal relations involving the Internet, but their adoption is complicated in turn by the variety of approaches taken by national legislation to one offence or another; for example, the concept of “pornography” is subject to different interpretations. Today the general trend of legislative initiatives connected with the Internet is towards the establishment of the liability of the providers of host services for the content of the information

contained in their computers. Since this is a very complicated matter from the technical standpoint, the legislation of some countries subjects the establishment of the liability of providers to the condition that they were aware of the content of the unlawful information.

37. Interpol, whose membership includes the law enforcement agencies of 178 countries, has reported that it will publish information on Net offences on the site of the United States company Atomic Tangerine. Interpol provides information about hackers and about the types of offence that threaten companies engaging in electronic business. Atomic Tangerine, for its part, must pass to Interpol information obtained through the NetRadar early warning system, which belongs to Atomic Tangerine and is designed for Internet monitoring.

38. The anonymity of communications is one of the most important problems, for it complicates, and sometimes renders impossible, the establishment of the identity of the owner of unlawful information and his or her prosecution. Experts from many countries are therefore proposing to impose a legal ban on anonymous communications, but one which would allow communications under pseudonyms since, where necessary, it would be possible to determine the authors of such communications.

39. On 21 December 1998 the Council of the European Union adopted a safer Internet action plan proposed by the European Parliament. This plan operated for four years (from 1 January 1999 to 31 December 2002). It had a budget of 25 million euros. The plan proposed the creation of various Internet quality standards to be established in accordance with Internet benchmarks on products. These provisions were to be incorporated both in national legislations and in the self-regulation codes of Internet providers. In March 1999 the European Commission, following discussion of the provisions of the report on the convergence of the telecommunication, media and information technology sectors, adopted a report containing the following fundamental conclusion: the legal regulation of the Internet must be transparent, clear and proportional.