United Nations A/59/116

General Assembly

Distr.: General
23 June 2004
English
Original: Arabic/Chinese/English/
Spanish

Fifty-ninth session
Item 62 of the preliminary list*
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/59/50 and Corr.1.

04-40704 (E) 210704
0440704

I. Introduction

1. In paragraph 3 of its resolution 58/32 of 8 December 2003 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 telecommunications systems and information resources; and (c) the context of relevant international concepts aimed at strengthening the security of global information and telecommunications systems. In paragraph 4 of the resolution, the 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 assistance of a group of governmental experts, to be established in 2004, appointed by him on the basis of equitable geographical distribution and 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. The Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security will commence its work in July 2004.

2. By a note verbale dated 18 February 2004, 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 these replies are reproduced in section II below. Additional replies received will be issued as addenda to the present report.

II. Replies received from Member States

Argentina

[Original: Spanish]
[14 May 2004]

Current situation

1. The Argentine Republic has made important advances with respect to data security and privacy. At the normative level, law No. 25326 on the protection of personal data is one of the most modern of its type in the world; its supervisory authority is the head of a directorate especially created for that purpose as part of the Ministry of Justice. In addition, a number of draft bills on computer crime are at an advanced stage of consideration by the National Congress.

2. Progress has also been made in legislation concerning digital signatures which seeks to provide electronic documentation with legal validity and technical security in order to guarantee its authorship and integrity. Argentina has been a pioneer in this area and final steps are currently being taken to implement the national public key infrastructure.

3. In particular, the Argentine State has made important advances with respect to information security. In that connection, the National Office of Information

Technology has primary responsibility for handling, assisting in and supervising matters relating to the security and privacy of digitalized and electronic information in the national public sector.

4. As part of the Office, ArCERT (Coordination of Emergencies in Teleinformatic Networks of the National Public Administration) is a response team that deals with incidents in networks of public bodies. Its principal objective is to raise the security threshold in the public sector. In that context, reported security incidents are handled, alerts are issued for preventive and corrective purposes, specific security tools have been developed, courses are being held on the subject for public sector workers and officials and progress is being made in the development of model State security policies.

General appreciation of issues

5. Information security has several aspects the solution of which represents a real challenge given the growing complexity of the problems to be resolved as a result of technological progress.

6. The main problems may be divided into three classes:

attacks against information per se;

improper use of information resources;

cybernetic crime.

7. With respect to information, the new technologies make it increasingly difficult to ensure the three principal characteristics of information: confidentiality, integrity and availability. At the same time, within the problems of information itself there are two main classes that require special treatment: personal information, which must be administered with the greatest care in order to preserve the privacy of individuals, and information relating to organizations — whether it is commercial, industrial or relates to public bodies or agencies — the dissemination, modification or loss of which might be prejudicial to economic, social, political or other objectives.

8. Another normally underestimated problem is the improper use of information resources. Improper use is the use of the resources made available for purposes other than those authorized or their use in an unreasonable manner that involves abuse, extravagance or waste. For example, the current dissemination of viruses and other kinds of interference through the Internet, and the necessary countermeasures, give rise to additional expense far greater than was necessary for the original purpose. A preventive approach to this matter will provide major savings in resources and efforts.

9. Lastly, the new technologies are providing new opportunities for the perpetration of crimes, both what are regarded as traditional crimes, which are now supported by the new technologies, and new variations inspired by technological progress.

China

[Original: Chinese]
[24 May 2004]

China's view on the issues of information society

1. Rapid development in the field of information and telecommunications is an important feature of scientific and technological advancement. Under new circumstances with security threats multiplied, non-traditional security factors rising and international terrorist activities increasingly rampant, information security has become a grave challenge in the field of international security. China supports international efforts aimed at maintaining and promoting information security of all countries and the establishment of the United Nations Governmental Expert Group to discuss and address the issue of information security.

2. China holds that use of information technology should abide by the United Nations Charter and other internationally accepted principles, and maintain and promote international and regional peace, stability and development. With non-traditional security threats increasingly salient, States should attach great importance to information criminality and terrorism. In view of the imbalanced development of countries in the field of telecommunications, the international community should also strengthen cooperation in the research and application of information technology.

3. China holds the view that within the framework of the United Nations Governmental Expert Group on information security, all parties should examine the existing and potential threats in the field of information security, and explore concrete ways and means to address them. China will take a positive and constructive part in the work of the United Nations Governmental Expert Group, and hopes its work will achieve positive results.

Costa Rica

[Original: Spanish]
[15 March 2004]

1. The Government of Costa Rica states that, on 24 October 2001, the Legislative Assembly of Costa Rica adopted an amendment to the Penal Code entitled "Addition of articles 196 bis, 217 bis and 229 bis to the Penal Code, law No. 4573, for the suppression and punishment of computer crime". That amendment has been the most significant development in recent years with respect to computer security in Costa Rica.

2. The amendment identified three types of computer crime (violation of electronic communication, computer fraud and alteration of data and computer sabotage). This was an important development for Costa Rica in this area and was tailored to the current requirements for ensuring computer security.

3. The entire document on the amendment is attached for your consideration (see appendix).

Appendix

Addition of articles 196 bis, 217 bis and 229 bis to the Penal Code, law No. 4573, for the suppression and punishment of computer crime

8148

The Legislative Assembly of the Republic of Costa Rica

Decrees:

Addition of articles 196 bis, 217 bis and 229 bis to the Penal Code, law No. 4573, for the suppression and punishment of computer crime

Single article: Articles 196 bis, 217 bis and 229 bis are added to the Penal Code, law No. 4573, of 4 May 1970, the texts of which shall be as follows:

Article 196 bis: Violation of electronic communications

(a) A term of imprisonment of between six months and two years shall be imposed upon any person who, in order to discover secrets or threaten the privacy of another person without that person's consent, gains possession of, accesses, amends, alters, deletes, intercepts, interferes with, uses, disseminates or defeats the purpose of messages, data or images contained in electronic, informatic, magnetic and telematic media. The penalty shall be between one and three years' imprisonment if the actions described above are carried out by persons responsible for such electronic, informatic, magnetic and telematic media.

Article 217 bis: Computer fraud

A term of imprisonment of between one and ten years shall be imposed on any person who, with the intention of procuring or obtaining an inheritance benefit for himself or for a third person, influences the processing or output of the data of a computer system by means of programming, the utilization of incorrect or incomplete data, the improper use of data or any other action affecting the processing of data in the system.

Article 229 bis: Alteration of data and computer sabotage

A term of imprisonment of between one and four years shall be imposed on any person who, by whatever means and without authorization, erases, deletes, modifies or disables the data recorded in a computer.

If, as a result of the said conduct, the operation of a computer programme, database or information system is interfered with or disabled, the penalty shall be between three and six years' imprisonment. If the computer programme, the database or information contains data of a public nature, a term of imprisonment of up to eight years shall be imposed.

Cuba

[Original: Spanish]
[1 June 2004]

Opinions of the Republic of Cuba to the request contained in paragraph 3 of resolution 58/32 entitled "Developments in the field of information and telecommunications in the context of international security"

1. In paragraph 3 (a) and (b) of resolution 58/32 of 8 December 2003 concerning 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 telecommunications systems and information resources; and

(c) The content of the international concepts aimed at strengthening the security of global information and telecommunications systems.

2. Cuba considers that the hostile use of telecommunications, with the declared or covert intent of undermining the legal and political order of States, is a violation of recognized international norms and a negative and irresponsible 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.

3. In its eighth preambular paragraph, resolution 58/32 reiterates once again the concern of the General Assembly "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 and infrastructure of States to the detriment of their security in both civil and military fields". Cuba fully shares that concern.

4. Information and telecommunications systems may be transformed into weapons when they are designed and/or used to cause damage to the infrastructure of a State.

5. Cuba reiterates that all States must respect existing international norms in this field. Access to information or telecommunications 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.

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

7. 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.

8. Every week, 2,227.5 hours of subversive radio and television programming against the constitutional order are transmitted towards Cuba by the United States. Twenty-nine different frequencies are devoted to programming specifically to this end from 18 medium-wave, short-wave, FM and television transmitters.

9. In all, between 312 and 315 hours a day of politically slanted programming are produced on the frequencies indicated. This has nothing to do with the promotion of the free flow of information and ideas since what is transmitted are false allegations fabricated by means of fraud, lies and misrepresentations, and messages are broadcast intended to promote the breakdown of the constitutional order of the country.

10. Of the 18 transmitters taking part in the radio and television attacks against Cuba, 15 belong to organizations linked with or belonging to known terrorist elements that reside, operate and work in United States territory with the full knowledge and consent of the authorities of the United States Federal administration.

11. Of these transmitters, 12 are directed specifically against Cuba, including the misnamed TV and Radio Martí. They are the property of the United States which invests $35 million a year in this radio electronic war against Cuba.

12. In a new and dangerous provocation, the Government of the United States announced in May 2004 that it would deploy the airborne EC-130 Comando Solo platform and allocate additional funds to purchase and recondition an airborne platform intended for broadcasts towards Cuba by the so-called TV and Radio Martí.

13. In the illegal broadcasts against Cuba, the true situation of our country is distorted, encouragement is given to illegal emigration under dangerous conditions, there is incitement to civil disrespect and disobedience as well as to violence, the perpetration of terrorist acts and the destruction of the institutional and legal order established by the Constitutions of the Republic of Cuba approved by the affirmative vote of over 96 per cent of Cubans.

14. The use of information in the clear interest of subverting the internal order of States, violating their sovereignty and meddling and interfering in their internal affairs is an illegal action under international law and impairs the enjoyment of the right of peoples to self-determination.

15. These broadcasts not only violate Cuban sovereignty but are flagrant violations of the regulations of the International Frequency Registration Board of the International Telecommunication Union, particularly No. 23.3 of the ITU Radio Regulations which prohibits television transmissions beyond national borders. Such actions are thus violations of international law.

16. 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.

17. Cuba considers that attention should be drawn once again to the following aspects that are closely associated with making full use of telecommunications as an instrument to facilitate international peace and security:

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

(b) 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 and based on standards adopted by the international community.

(c) 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.

(d) Legislative and other measures should be adopted as a matter of urgency, 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 their potential use as a tool for propaganda against peace and incitement to war.

(e) A multilateral, intergovernmental 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 should be intergovernmental in nature.

(f) 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 sovereignty and security of many States, as well as individual privacy, that occur with the global spying systems developed by industrialized countries, in particular the United States.

(g) The development of firm guarantees of respect for cultural diversity and the elimination of all forms of discrimination or incitement to hate in the content of the information disseminated by international telecommunications systems should be promoted.

Georgia

[Original: English]
[18 May 2004]

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

1. The current status of information safety in Georgian telecommunications

1.1 The system of information safety of Georgia is at a developmental stage.

1.2 The concept of the national information safety system has been conceived by the Ministry of Infrastructure and Development of Georgia and the Georgian National Communications Commission.

1.3 The initiating group carries on its work without target financing.

2. The status of a task

The working group on the initiative consists of the following members:

- Ministry of Infrastructure and Development of Georgia: Department of Telecommunications and Information Technologies Politics
- Georgian National Communications Commission: Technical Department

3. The basic principles of policy of the national information safety system of Georgia is as follows:

3.1 The common directions of the concept of information safety are defined by the Georgian Information Programme. The Programme is at a developmental stage.

3.2 The strategy of information safety for corporate, government and public information systems and appropriate telecommunications infrastructure should be based on the national system of information security standards.

3.3 The system of information security standards of Georgia is based on a harmonization of international standards of the International Organization for Standardization (ISO), the International Telecommunication Union (ITU) and the European Telecommunications Standards Institute (ETSI).

3.4 At the corporate level, the policy of information safety is realized on the methodical recommendations and rules with voluntary certification according to ISO standard 17799.

4. Georgian participation in global information society should offer the following opportunities:

4.1 The establishment of a united information space and infrastructure, with the participation of Georgia in international processes, including the development of an international security information system.

4.2 Integrated globalization, based on international information standards, compatible with the participation of Georgia in the World Trade Organization, the United Nations and other international communities.

4.3 Entry into global post-industrial economy, based on principles of cooperation and information access, overcoming the information divide between Georgia and the international information community.

4.4 Increase of security in Georgia.

5. Main tasks of the Ministry of Infrastructure and Development of Georgia in the region of information security

5.1 Definition of the telecommunications standards deficiency, monitoring and study of activity results of the international standardization organizations, quality certification systems, ecological and information security.

5.2 Coordination of international and local programmes and the strategy of communications development with the requirements of the international organizations; cooperation with the international initiatives and regional projects of safety.

6. Enhancement of the national information safety in Georgia

6.1 For the successful realization of the information programme and the system of information safety, target financing and international support is needed.

6.2 The help of international organizations is important in the following areas:

- Researching the telecommunications infrastructure and migration to new generation networks;
- Analysis of conditions and comparability of national information security system of standards;
- Development of the programmes and techniques of information security at various levels of economic and social activity.

7. Cooperation with international organizations

- ITU and the Regional Communications Community (RCC)
- The United Nations
- The Economic and Social Commission for Asia and the Pacific, the United Nations Conference on Trade and Development and the World Trade Organization

8. Projects, seminars and other activities

8.1 ITU: A project for a system of protection from non-authorized access for the Ministry of Infrastructure and Development of Georgia.

The organizers: BDT, ITU, “Utimaco”, Government of Bulgaria, Department of Telecommunications and Information Technologies.

8.2 Training workshops about development of the trade finance infrastructure of Georgia.

- The problems of construction of a corporate system with the support of new ICT technologies.
- Electronic commerce, ICT development and trade finance, development of e-trade financial systems, e-banking systems and e-payment systems.
- Discussion of the problems, including the development of the national trade finance infrastructure.

Lebanon

[Original: Arabic]
[27 May 2004]

In view of the development and application of the utilization of information technologies and means of communication, Lebanon is concerned that such technologies and means of communication should not be used for purposes that are inconsistent with the concepts of international stability and security, and considers that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes. It will respond to and cooperate with resolutions of the United Nations that are conducive to protecting the security and confidentiality of information and to preventing their misuse by any means.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[14 May 2004]

1. The United Kingdom welcomes the engagement of the United Nations community in addressing the implications of our increasing dependence on communication networks and information systems, including our vulnerability to threats. Information security is crucial to the growth of the global economy, and its importance was recognized in the principles and action plan adopted by the World Summit on the Information Society at the conclusion of its first phase.

2. The principles adopted call for "a global culture of cybersecurity ... to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies" and for these efforts to be "supported by increased international cooperation". The United Kingdom strongly believes that the security objectives of nations can best be met by promoting a global culture of cybersecurity as described in the principles of the World Summit and the Principles for Protecting Critical Information Infrastructures of the Group of Eight and as referred to in General Assembly resolution 58/199.

3. The United Kingdom does not, however, believe that there is a need for a multilateral instrument that would restrict the development or use of certain civil and/or military technologies. With respect to military applications of information technologies, such an instrument is unnecessary. The law of armed conflict, in particular the principles of necessity and proportionality, governs the use of such technologies. Moreover, such an approach might impinge on the free flow of information, which was also recognized by the World Summit on the Information Society as a key principle of the information society.

Basic notions and relevant concepts

4. We need to see the risk to networks and information systems as a function of threat and vulnerability. The threat is constantly shifting, but it is clear that it has become more complex in recent years. State actors represent only a small part of the threat to information systems. Of greater concern in recent years have been the activities of terrorists, organized criminals and hackers, who have sought to access systems inappropriately or attack the proper functioning of networks. To enhance

global cybersecurity we need to ensure that attacks against information systems and networks are addressed by criminal law. The Council of Europe Convention on Cybercrime is the best model for instituting the criminalization of cybercrime.

5. Threat analysis is however only one aspect of cybersecurity. The United Kingdom believes that the defence of networks and information systems is to a very large extent independent of the source of threat. International cooperation should therefore be directed towards addressing vulnerabilities. These can be technological, software or protocol vulnerabilities, but can also arise from user error when users are duped into releasing security information by social engineering or "phishing". Changing the cyberculture, the way in which networks and information systems are developed, deployed and used, is our greatest challenge. The "Guidelines for the Security of Information Systems and Networks — *towards a culture of security*" of the Organization for Economic Cooperation and Development (OECD) provide a firm basis of initiating this cultural change.

Implementing relevant concepts: the United Kingdom approach

6. In 2003, the United Kingdom adopted a national strategy on information security, which addresses critical information systems protection and network resilience. It focuses on protection of Government information assets and systems while recognizing the importance of working with the private sector, and includes a clear outreach element, both to business and the individual citizen. It also acknowledges the importance of working in partnership with other countries in achieving a more secure cyberspace.

7. New structures have been put in place within Government to implement the strategy, involving active participation by the interior, industry and defence Ministries plus the appointment of a nominated risk owner in every Department of State. To support the strategy, the technical capability of Government experts to anticipate and respond to information security challenges is also being developed. The strategy also recognizes the importance of research and innovation and is due to publish a major study on long-term approaches to cybersecurity in June 2004.

8. The United Kingdom strategy comprises three key initiatives. In 1999, the United Kingdom established the National Infrastructure Security Coordination Centre, a multi-agency initiative, which now enjoys an international reputation for excellence in the protection of critical infrastructures. It encourages information sharing between communities of interest, acts as a focal point for the real-time dissemination of alerts based on international contacts and has a leading role in the identification and correction of protocol vulnerabilities.

9. The United Kingdom has also been instrumental in the development of standards on information security management, including the Guidelines on Information Security Management (ISO/IEC 17799), originally a British Standard, which is rapidly becoming accepted at the pre-eminent standard in this field. Such standards adopt a vulnerability- or risk-based approach to information security, enabling organizations to mainstream information security management.

10. To tackle cybercrime, the United Kingdom is developing an e-crime strategy, which draws on the Council of Europe Convention and European Union legislation. In addition, the law enforcement community in the United Kingdom has adapted to reflect the changing nature of cybercrime with the creation of a national resource,

the National High-Tech Crime Unit, together with specialist units in local police forces.

Implementing relevant concepts: the potential for international cooperation

11. The World Summit on the Information Society emphasized the importance of international cooperation in maximizing the potential of the information society. General Assembly resolution 58/32 provides us with an opportunity to build a culture of cybersecurity that will protect the interests of Governments, businesses and citizens by minimizing the risk of systems disruption and protecting the free flow of information. The Organization for Economic Cooperation and Development guidelines provide a powerful model of the principles, which could help to foster such a culture and should inform our approach to cybersecurity.

12. The United Kingdom welcomes the engagement of the United Nations community with regard to the issue of information security and believes that the United Nations can contribute to the development of a culture of cybersecurity by focusing on the following issues:

- Developing and exchanging best practices
- Establishing a baseline approach to the criminalization of cybercrime activities based on the Council of Europe Convention
- Enhancing real-time collaboration between national authorities on the identification of threats, vulnerabilities and the conduct of investigations and prosecution of offenders
- Developing a more coherent approach to the removal of vulnerabilities from information systems.