United Nations

A/56/164

General Assembly

Distr.: General
3 July 2001
English
Original: English/Spanish

Fifty-sixth session
Item 81 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/56/50.

** On behalf of the States members of the European Union that are Members of the United Nations.

I. Introduction

1. In its resolution 55/28 of 20 November 2000 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 content of relevant international concepts aimed at strengthening the security of global information and telecommunication systems; and requested the Secretary-General to submit a report based on replies received from Member States to it at its fifty-sixth session.

2. On 19 March 2001, the Secretary-General addressed a note verbale to Member States requesting them to provide their views pursuant to the invitation of the General Assembly. The replies received from Governments as at 3 July 2001 are reproduced in section II of the present report; any other replies received will be issued as addenda to it.

II. Replies received from Governments

Bolivia

[Original: Spanish]
[14 June 2001]

Information has been received from the Ministry of Foreign Affairs of Bolivia indicating that at present the Bolivian armed forces do not possess adequate electronic means and do not expect to acquire or manufacture such means in the future.

Mexico

[Original: Spanish]
[16 May 2001]

1. Mexico considers that greater efforts should be directed at encouraging civilian application of scientific and technological advances and information technology. Mexico supported General Assembly resolutions 53/70, of 4 December 1998, and 54/49, of 1 December 1999, entitled “Developments in the field of information and telecommunications in the context of international security”.

2. Concerns about security currently focus mostly on the possible vulnerability of the information systems under which some countries’ defence programmes operate and the danger that information technology and telecommunications will be used by terrorists or to back a threat.

3. In that context, international cooperation and international law are the only means for ensuring that measures adopted to deal with information security problems do not in any way restrict freedom of information and communication.

4. This is undoubtedly a very important topic. The developments and discussions in other General Assembly committees should, however, also be borne in mind, since they could make a valuable contribution to defining and specifying concepts that could be used in considering information security problems.

5. As for the question of the definition of basic international criteria or notions related to information security, Mexico considers that the notion of unauthorized interference could give rise to undesirable confusion, since it implies some similarity with actions taken by certain States which invoke questionable humanitarian or other motives in order to intervene, individually or jointly, in the affairs of other States.

6. It would therefore be preferable to replace that notion with the phrase “impermissible access” or simply “illegal access” in relation to activities by any individual or body involved with information systems.

7. With regard to the need to develop international principles to increase the security of world information and telecommunication systems, it should be emphasized that such principles should be geared not only to increasing system security but also to protecting it more effectively with legal guarantees.

8. There should also be a more rigorous examination of the relevant provisions in international instruments adopted over the years both by the General Assembly and by other international organizations — the United Nations Educational, Scientific and Cultural Organization (UNESCO), for example — dealing with international security, international terrorism and

information, with the aim of identifying and assessing the relevant existing principles in this field.

9. In that context, Mexico is in agreement with General Assembly resolution 51/210, of 17 December 1996, on measures to eliminate international terrorism, particularly part I, paragraph 3(c), which refers to the risk of terrorists using electronic or wire communications systems and networks to carry out criminal acts and to the need to find means, consistent with international law, to prevent such criminality and to promote cooperation.

10. During the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Vienna from 10 to 17 April 2000, the Secretariat prepared a document entitled “Crimes related to computer networks” (A/CONF.187/10), which stated that effectively preventing and combating cyber crime requires a coordinated international approach at different levels.

11. At the domestic level, the investigation of such crimes requires experts, specialized knowledge and adequate procedures. States should be urged to consider the possibility of establishing mechanisms enabling them to obtain timely, accurate information from computer systems and networks, when such information is required as evidence in judicial proceedings.

12. At the international level, the efficient investigation of cyber crime requires timely action, supported by coordination between national law enforcement bodies and the relevant legal authority.

Philippines

[Original: English]
[22 May 2001]

1. General appreciation of the issues of information security

1. The complexity and extent of the problems and issues in the realm of information security is immense and limitless, making information security a serious global issue. The threats posed by problems arising in today’s information age are spawning rapidly. Every technological advance and innovation also creates new opportunities that can be exploited against the good vision of humanity.

2. The problem of information security is something equally threatening to that of weapons of mass destruction. It threatens all aspects of human existence. It is a problem that no single nation or group of nations can address alone. It is thus a global concern that urgently needs a concerted response from all nations, whether they are technologically advanced or not.

2. Definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunication systems and information resources

3. The basic notions listed below may be defined as follows:

(a) *Unauthorized interference or unsanctioned penetration*. (i) A non-governmental act of interference; or (ii) government-sanctioned interference that is not within the established international regime or protocols of information security;

(b) *Authorized interference*. Government-initiated “interference” as sanctioned by international treaties or within the boundaries of an established international regime or protocols of information security;

(c) *Unsanctioned use of information*. (i) Use of public and private information illegally and legally obtained without prior permission from the sources; (ii) use of vital public and private information illegally and legally obtained by government entities for personal, non-governmental interests; (iii) use of vital public and private information illegally and legally obtained by the Government, outside the framework of any established international regime or protocols of information security or other related treaties and international laws;

(d) *Misuse of information and telecommunication systems*. (i) The use of information and telecommunication resources, including related infrastructures for malicious intent; and (ii) all unsanctioned use of information;

(e) *Information resources*. Unprocessed and processed data (i.e. statistics, facts, figures, records, etc.), software programs, techno-cyber hardware and equipment (i.e. personal computers, laptops, scanners and other new and advance forms of technology), information technology and other related facilities (i.e.

transmission towers, satellite disks, control towers/ buildings), information technology experts and professionals (i.e. computer programmers, system analysts, etc.), including information-cybernetic networks and systems (Internet);

(f) *Information weapons*. Information resources strategically developed or created for information warfare or to cause damage, confusion or disadvantage and with any other forms of malicious intent;

(g) *Information warfare*. (i) Actions aimed at achieving information superiority by executing measures to exploit, corrupt, destroy, destabilize or damage the enemy's information and its functions; (ii) actions taken to protect one's information resources and telecommunication systems; (iii) acts of exploiting one's information resources and telecommunications systems to achieve goals and interests, for example, cyber warfare (information warfare in the defence and military context) or "Internet war" (information warfare in the larger societal context);

(h) *Information terrorism*. Terroristic acts in the context of information security;

(i) *Cyber crimes or information crimes*. (i) Criminal acts involving elements of information security; (ii) acts of malicious intent directed at information resources (e.g. techno-vandalism, techno-trespass and superzapping); (iii) all unauthorized interference or unsanctioned penetration;

(j) *Cyber/techno-criminals*. (i) Persons committing acts violating established international regimes or protocols on information security; (ii) persons whose criminal acts involved or depend greatly on the use of information security; (iii) persons found to be repeatedly committing acts directed against information resources (suspects who are minors should be exempted from being convicted as techno-criminals);

(k) *Information colonization*. (i) Acts committed by a State or States against another State in order to dominate and control the information arena and prevent access to the latest information technologies and create a situation in which other States become technologically dependent in the information sphere; (ii) acts of information expansion and acquisition of a monopoly over another State's national information and telecommunication infrastructures creating conditions of dependency and control;

(l) *Technologically advanced nations*. (i) Countries whose economy is more than 50 per cent wired; (ii) may generally refer to developed countries.

3. The content of the concepts aimed at strengthening the security of global information and telecommunication systems mentioned in paragraph 2 of resolution 55/28

4. The proposal for the establishment of an international regime on information security is very crucial at the present point. Such proposals should ensure accountability on the part of States that violate the said protocols on information security. It should also create a balance between the technologically advanced nations against those which are not. The regime should consider technologically advanced nations that are already conducting their own form of "interference" against nations that are at a disadvantage. Lastly, the regime should strongly consider that "law enforcement" is a vital factor in enhancing international information security. This can be operationalized by creating an international centre to coordinate law enforcement units of different nations in tracking down suspects as well as to help those nations in their domestic operations.

Sweden*

[Original: English]
[26 June 2001]

1. At the fifty-fifth session of the United Nations General Assembly, the member States of the European Union (EU) supported the consensus on Assembly resolution 55/28, entitled "Developments in the field of information and telecommunications in the context of international security". The EU member States wish to provide the following common reply to paragraph 3 of the resolution, which invites Member States of the United Nations to communicate to the Secretary-General their views and assessments.

* On behalf of the States members of the European Union that are Members of the United Nations.

1. General appreciation of the issues of information security

2. Information and telecommunication technology facilitates substantially the free flow of information and brings enormous benefits to individuals, businesses and Governments worldwide. It enhances the development of democracy and freedom of speech as well as the advancement of a civil society. EU believes that it is important to promote and ensure further development in the field of information and telecommunication technology, along with the reinforcement of the principle of freedom of information. EU recognizes that there exists a potential threat of unauthorized interference with or misuse of information and telecommunication systems, the integrity of information-based infrastructures and the information resources of individuals, enterprises, educational or medical institutions and private sector organizations, as well as of Governments.

3. Information and network security is concerned with securing senders' and receivers' identities, protecting information from unauthorized changes, protecting against unauthorized access to information and providing a reliable supply of equipment, services and information.

4. Information security extends to the protection of information related to military capabilities and other aspects of national security. Insufficient protection of vital information resources and information and telecommunication systems may pose a threat to international security.

2. Possible content of relevant international concepts aimed at strengthening the security of global information and telecommunication systems

5. As a starting point, EU would like to emphasize that while international cooperation is essential in order to combat effectively the novel and complex issues related to information security, it is first and foremost both the right and the responsibility of every country to protect its own information and information-based systems.

6. EU believes that existing risks are transboundary in character and that the technologies enabling attacks on information and telecommunication systems are widely available. All economies depend on the free flow of information and the peaceful use of information technologies. Any preventive action aimed at containing potential criminal or terrorist attacks, including a danger to international security, should take into account the protection of information resources and information-based systems.

7. Several ongoing multilateral efforts are already addressing international cooperation in the field of information security, for example, by the Council of Europe; the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 10-17 April 2000 (see A/CONF.187/15); the United Nations Commission on Crime Prevention and Criminal Justice; the Working Group on Informatics of the Economic and Social Council; the Information and Communication Technology (ICT) Task Force of the United Nations; the Organisation for Economic Cooperation and Development; the International Telecommunication Union; the high-tech crime groups of the G8; and the Organization of American States.

8. EU thus considers that the Member States of the United Nations should monitor work in those and other forums with a view to evaluating in due course the type of substantive actions that might make a useful contribution in this field. EU is not of the view that, within the context of the General Assembly, the First Committee should be the main forum for discussing the issue of information security. Since the question mainly encompasses subjects other than disarmament and international security, EU believes there are other committees better suited for discussion of at least some of the aspects of the issue.