United Nations A/57/166/Add.1

General Assembly

Distr.: General
29 August 2002
English
Original: Arabic/English/Spanish

Fifty-seventh session
Item 62 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**

Addendum

Contents

* A/57/150.
** The information contained herein was received after the submission of the main report.

02-56149 (E) 200902 200902
0256149

Replies received from Governments

Cuba

[Original: Spanish]
[15 July 2002]

General appreciation of the issues of information security

1. The world has witnessed immense scientific and technological development in recent decades. Undoubtedly the progress achieved in informatics and telecommunications has constituted a technological revolution which extends to all human activity. The combination of informatics and telecommunications advances expands the potentialities of both branches to unimaginable heights.

2. The introduction of high-speed personal computers with enormous operational capacity, the use of new materials which speed up the transmission of information and the proliferation of communication satellites are but a few examples of the success achieved.

3. The current globalization process is one of the tangible outcomes of the so-called technological revolution. Distances are becoming shorter and communication and the flow of information operate in real time. Industrial processes have changed drastically and informatics tools are rapidly redesigning productive processes, achieving heretofore unknown levels of efficiency.

4. These changes affect not only the civilian but also the military industry. Today informatics is an essential component of modern weapons and their systems. In the past decade, we were witness to various armed conflicts showcasing sophisticated weapons with hitherto unknown destructive potential and deadly precision in hitting their targets, in large part the fruit of the latest informatics applications.

5. Informatics tools have demonstrated their potentialities. Software, for example, has found a wide range of applications, including the ever-intensifying proliferation of highly destructive programmes which are infected or can transmit viruses, and are capable of doing irreparable damage anywhere in the world, in a relatively short time, as a result of the increase in informatics networks and the degree of access to such networks.

6. The dependency being created by these technologies calls for collective thinking with the aim of ensuring the proper use of all these means.

7. The very fact that the item is included in the agenda of the General Assembly shows that the international community has become aware of the potential threat to international peace and security when such technologies are not used for peaceful purposes.

8. Furthermore, the hostile use of telecommunications in some cases, on the avowed or hidden pretext of subverting the legal and political order of States, is another negative manifestation of the use of such means, whose impact can sow tension and breed situations that are detrimental to international peace and security, in flagrant violation of the principles and purposes of the Charter of the United Nations.

9. General Assembly resolution 56/19 affords us an opportunity to analyse all aspects of information and telecommunications in the context of international security, including the possibility of strengthening and expanding existing international law in this field.

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

10. A number of essential notions are discussed below.

1. The standardization of norms and procedures

1l. The lack of a common code of ethics for all users, in view of the voluntary nature of participating in Internet networks and the use of satellites and other means of communication is a threat to the security of information transmitted through such means.

12. Requirements such as *confidentiality, integrity and availability* ensure efficient network use. These aspects guarantee that each piece of information is viewed by authorized users only, is not altered and can be accessed when needed.

13. When these requirements are not respected, security is diminishes or sacrificed. Each manufacturer of informatics means must guarantee that its software or hardware does not permit hacking or generate

informatics weapons capable of harming any element of information systems. In general, these principles are valid for any provision of services or manufacture of products or information and communication technologies systems.

14. This will be possible insofar as each manufacturer of informatics systems establishes better controls over production processes, technologies and systems, and also ensures follow-up, for the same purposes, in the subsequent operation and use of such systems and technologies. Similarly, there is a need for cooperation mechanisms which facilitate mutual warning by suppliers and users of any violation detected and set out producers' responsibilities with regard to resolving security problems connected with the products they sell.

15. In order to generate technology in a secure environment, minimum standards must be developed. Technology must also be certified, as this will help standardization mechanisms. In this connection, Cuba is prepared to cooperate with any interested countries, drawing on its modest experience in this field.

2. Unauthorized interference with information or telecommunication systems

16. International regulations to prevent attacks on these systems must be strengthened. States cannot deal with this problem in isolation. The level of interdependence created by the universality of information networks and telecommunication systems rules out the possibility that this task could fall to one State alone.

17. Already existing international norms must be respected. Information or telecommunication systems of another State should be accessed only with the consent of the State concerned, and in such forms and to such extent as it determines.

18. An attack on the information or telecommunication systems of other States can undermine international peace and security. Such tactics are already used as tools to carry out hostile policies.

19. Cuba suffers from this attacks of this nature which are instigated, tolerated and executed by the Government of the United States of America. To illustrate how serious this is, we wish to point out that our country has for decades been subjected to radio and television attacks by the United States with the avowed purpose of subverting its internal order and overthrowing its Government.

20. To that end, for example, from January 2001 to March 2002, an overall average of 15 radio and television stations broadcast false and tendentious information that was clearly subversive in content from the territory of the United States.

21. During that period, these stations broadcast, on a daily basis, between 312 and 319 hours on medium-wave, short-wave and frequency modulation bands. That means 2,257 hours a week on average. If television signals are included, the total figure would come to 2,288 hours a week.

22. Since 1990, the United States Government has invested more than $20 million a year in these radio and television attacks, and around $24 million during this fiscal year alone.

23. In most cases, the information incites civil disobedience and the commission of acts of vandalism and terrorism. Recently, a radio programme by the United States Government even caused an incident designed to create internal disorder in Cuba, in which, moreover, the diplomatic mission of a third country was involved, sparking tension which could have prejudiced Cuba's diplomatic relations with that country.

3. Misuse of information and telecommunication systems

24. These systems are used outside internationally agreed procedures and norms and in violation of the relevant national regulations. Those States which have not yet done so should take all necessary measures to strengthen such national regulations.

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

26. At present, virtually no sphere of society nor any human activity can escape the influence of information or telecommunication systems, which means that the impact of misuse of such means is incalculable.

4. Information and telecommunication systems are dual-use technologies

27. One peculiarity of historic developments in this field is that the rise in the use of new technologies has oscillated between civilian and military applications. In other words, many of the technologies used extensively in civilian life today had their origin in the military branch, and vice versa.

28. Thus, the efforts of the international community in this area should be channelled in two directions: prevention, suppression and eradication of the use of information and telecommunication systems for hostile purposes, and the empowerment of international cooperation to use them peacefully.

29. This would call for, inter alia, analysis of the following elements related to information and telecommunication systems:

(a) The design and universal application of procedures to prevent unauthorized access to systems;

(b) Transparency in the use of such means;

(c) The planning of specific measures to protect information systems linked to weapons of mass destruction and other sophisticated weapons;

(d) The adoption of measures to prevent unauthorized access to information systems of electrical and nuclear power stations, electrical power stations or other facilities that are strategically vital to a country;

(e) The exchange of information between States on illegal activities involving individual or legal entities under their control or jurisdiction, out of a basic desire to prevent illegal acts;

(f) Increase in international cooperation designed to facilitate transfers of technology and the training or consolidation of the relevant national capacities;

(g) Prohibition of the installation of means in outer space for military uses;

(h) Strengthening of the basic principles of international relations on non-interference in the internal affairs of States through, inter alia, the adoption of measures prohibiting the use of information and telecommunication systems for those purposes.

5. Information weapons

30. Information and telecommunication systems can become weapons when they are designed and/or used to inflict damage on a State's infrastructure. Examples include attacks on national networks with foreign software or from internal sources within the State itself that are planned or conceived abroad; radio or television broadcasts through unauthorized means or without the consent of the State attacked; and influencing the conduct of persons with a view to destabilizing societies, overthrowing governments or altering the political and social order of countries.

6. Terrorism applied to information and telecommunication systems

31. Terrorism must be combated and rejected in all its forms and manifestations, irrespective of its origin or perpetrators. These technologies are not immune from being used to commit acts of terrorism. Their widespread distribution, the relatively easy access to them, the cost-impact ratio of their use, make them attractive to terrorists.

32. There could be actions as dissimilar and as dangerous as, inter alia, interruption of automated systems at airports; interference with the navigation systems of commercial flights; damage to the control systems of electrical power plants, water supplies and roads; and damage to communication networks.

33. Assessing progress in information and telecommunications in the context of international security inevitably means addressing terrorism-related issues. An immediate framework for addressing this matter might be the negotiations being conducted in the United Nations on the international fight against terrorism with a view to establishing international norms and regulations and other relevant multilateral initiatives.

34. Cuba is prepared to analyse these and any other basic notions which may be proposed and believes that the United Nations, as the supreme guarantor of international peace and security, is the ideal organ for discussion of such issues.

35. International institutions specializing in information and telecommunication systems should also be involved in the debate.

Appropriateness of elaborating international principles to strengthen the security of global information and telecommunication systems and help fight terrorism and crime in the field of information

36. Clearly, there is a need to strengthen international law in the field of information and telecommunications. It would not spring from a void; there are already existing related international principles, regulations and procedures which must be taken into account. National experiences should also be considered.

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

38. Both methodologies must address the basic notions outlined above and others which may be proposed, particularly unauthorized interference with or misuse of information systems and information resources; aspects of sovereignty related to these issues; the peaceful use of means of information and telecommunications in all their aspects; the prevention, suppression 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 to suppress related criminal acts.

Panama

[Original: Spanish]
[24 June 2002]

1. The Republic of Panama recognizes the danger inherent in the fact that significant technological developments in the field of information and telecommunications have transformed the so-called “cyber battlefield” into a new threat to international security: technology has an influence not only on armed conflict itself but also on its resolution (intelligence, targets, quality versus quantity of weapons).

2. An attack in which new information and telecommunications technologies are employed may cause more damage than, for instance, a conventional bombardment. Computers today regulate financial information as well as the flow of oil and gas through pipelines and traffic through the Panama Canal. They also control, among other things, water reserves and reservoirs, air traffic and emergency services. Thus, the definition of basic notions related to information security, including unauthorized interference with or misuse of information and telecommunication systems and information resources, requires protection systems tailored to this new form of violence. However, such protection systems (firewalls, for example) require considerable financial and human resources, which are not easily obtainable in many of our countries.

3. Consequently, strengthening the security of global information and telecommunications systems requires the establishment of a secure system that allows States to exchange information with a view to monitoring and preventing activities or communications by individuals or networks of individuals who use communications technology to plan criminal activities. For technologically advanced countries, however, that need implies a commitment and an obligation to provide, transfer and build the capacities of less advanced countries. Likewise, those countries must undertake not to use their technological advantage for commercial or industrial espionage against the rest of the less technologically advanced countries.

4. In spite of the damage they can cause, the Internet and the new information and telecommunications technologies are tools which, when properly used, can contribute to international security by providing the necessary means to achieve human security.

Syrian Arab Republic

[Original: Arabic]
[28 August 2002]

The response of the Syrian Arab Republic concerning developments in the field of teleinformatics in the context of international security is as follows:

- The embargo on possessing and importing teleinformatics technology in the developing States Members of the United Nations should be lifted.
- The United Nations should play an active legislative and concrete role in eliminating the digital divide between the technologically and

scientifically advanced States and the developing States.

– Laws preventing States, organizations and individuals from obtaining illegal access to teleinformatic systems of other States should be established, and such legislation should provide for the prosecution of parties who violate it.

– Resolutions of the International Telecommunications Union protecting the radio frequency ranges assigned to each State Member of the United Nations against jamming or illegal interference by any other State or any other party should be implemented.

– International standards and rules on the dissemination of information regarding the history, civilization and culture of peoples in databases and information networks (Internet) must be established, banning disinformation through the dissemination of erroneous information and calling for the adoption of appropriate measures, including the means to take action against parties who commit violations.

– An international authority, with international support, should be created. Its role would be to provide justification and proof to States requesting it to cooperate in security matters concerning the teleinformatics regime. This international authority would be responsible for, inter alia, providing material and technological support to such States with a view to enabling them to fulfil their obligations and to train their own specialized technical personnel through technological cooperation in the security of teleinformatics systems.