United Nations A/61/161

General Assembly

Distr.: General
18 July 2006
English
Original: Arabic/Chinese/
English/Spanish

Sixty-first session
Agenda item 82 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/61/150.

I. Introduction

1. In paragraph 3 of its resolution 60/45, 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) efforts taken at the national level to strengthen information security and promote international cooperation in this field; (c) the content of relevant international concepts aimed at strengthening the security of global information and telecommunications systems; and (d) possible measures that could be taken by the international community to strengthen information security at the global level.

2. On 23 February 2006, a note verbale was sent to Member States inviting them to inform the Secretary-General of their views and assessments on the subject. The replies received are contained in section II below. Additional replies received will be issued as addendums to the present report.

II. Replies received from Governments

Bolivia

[Original: Spanish]
[13 June 2006]

General Assembly resolution 60/45 promotes the consideration, at multilateral levels, of existing and potential threats in the field of information security, as well as measures to limit the threat emerging in this field, consistent with the need to preserve the free flow of information.

General appreciation of the issues of information security

Because of the considerable progress achieved in developing and applying information technologies and means of telecommunication, such as the Internet, the fax machine and the cellular telephone, information is now available in an indiscriminate and unrestricted form, at the global level, thereby making it possible to gain access to classified information.

However, this process also brings the broadest positive opportunities for the development of civilization, the expansion of opportunities for cooperation for the common good of all States and the achievement of new goals for the benefit of mankind.

In the area of defence, information security is managed at a low level (generally by the office of the company offering the service). There are usually no relevant domestic security policies.

Efforts taken at the national level to strengthen information security and promote international cooperation in this field

With respect to the existing and potential threats in the sphere of information and telecommunications security and possible cooperation measures to address them, there is an existing procedure under which information obtained is transmitted, as appropriate, to the Ministry of Information, and regulated by the Superintendency of Telecommunications.

In the area of defence, the security measures adopted are insufficient, in the context of today's advanced technologies.

Bolivia is currently developing telecommunications projects that incorporate the highest-level information security measures, using coded transmission procedures. These projects are designed to reduce and/or eliminate the deficiencies identified.

The content of the concepts mentioned in paragraph 2 of General Assembly resolution 60/45

Bolivia believes that the measures proposed in paragraph 2 might be promoted through an evaluation of the relevant international concepts designed to strengthen the security of global information and telecommunications systems.

Possible measures that could be taken by the international community to strengthen information security at the global level

- Evaluation of information and telecommunications security issues at the international level;
- Definition of basic criteria regarding information and telecommunications security and unauthorized access to, or illicit use of such systems via the Internet;
- Development of international principles aimed at increasing the security of information and telecommunications systems at the global level and also contributing to the fight against terrorism and against trafficking in classified information;
- Expression of concern at the possibility that such measures and technologies may be used for purposes that are contrary to the goal of guaranteeing the stability and security of States;
- In the military and defence sphere, implementation of telecommunications systems equipped with security systems that incorporate advances in global technology.

Recommendations

Information security should be regarded as a State policy, enshrined in the relevant telecommunications law, and regulated and controlled by the relevant Superintendency of Telecommunications.

With respect to information security at the national level, it is necessary to implement telecommunications projects that use the latest technology with a view to ensuring that operational projects incorporate the highest-level security measures available in the telecommunications sector.

China

[Original: Chinese]
[24 May 2006]

Information technology is currently undergoing explosive development, and has become an important positive factor in the economic and social development of countries as well as in the improvement of the lives of their people. At the same time, the development and broad application of information technology have entailed unprecedented challenges to the security of individual States and of the international community as a whole. The problem of information security has already become a major factor influencing the comprehensive security of States and even global security and stability. The appropriate resolution of this problem in accordance with the collective benefit of all countries is a shared responsibility of the international community.

It is the view of China that the problem of information security not only involves the risks arising from the weakness of the basic information infrastructure, but also the political, economic, military, social, cultural and numerous other types of problems created by the misuse of information technology. Each of these two factors is worthy of equal concern when studying the problem of information security.

China holds that information technology should be used in accordance with the Charter of the United Nations and the basic principles of international relations; the free flow of information should be guaranteed under the premises that national sovereignty and security must be safeguarded and that the historical, cultural and political differences among countries be respected; each country has the right to manage its own cyberspace in accordance with its domestic legislation; and in view of the imbalances among countries in the development of telecommunications, the international community should also strengthen cooperation in the research and application of information technology and conscientiously ensure that each country enjoys the freedom of information technology.

The United Nations is the appropriate setting in which to resolve the problem of information security. Although a group of Governmental experts on information security was unable to achieve substantive results in 2005, experts from various countries nevertheless engaged in a profound exchange of ideas and offered numerous valuable proposals with regard to a range of topics in the field of information security, thereby laying a solid foundation for the continued discussion and resolution of information-security problems by the international community. China supports the re-convening by the United Nations in 2009 of a Governmental experts group to carry out a deep and comprehensive study of the threats and challenges in the field of information security along with programmes and policies to address them. China will continue, as it has in the past, to support and participate in international efforts to deal with the problem of information security.

Jordan

[Original: Arabic]
[5 June 2006]

Information security is related to the concept of national security and the information security system has a direct connection with telecommunications security since it is through telecommunications that information is transmitted and exchanged through networks, whether wired or wireless. In order to protect and strengthen the security of information and telecommunications the following are required:

(a) The establishment of regulations, laws and systems to protect the confidentiality, integrity and provision of information and to counter attacks on it and the exploitation of information systems for the commission of crimes;

(b) The establishment of a national plan to underpin the function of ensuring the security of information, telecommunications and networks with the participation of those involved in the information and networks sector. The plan should ensure the following:

1. Confidentiality and reliability: ensuring that the information is not disclosed and does not become known to unauthorized persons;

2. Integrity of content: ensuring that information content is sound and has not been modified or interfered with, and that the content has not been destroyed, altered or tinkered with at any stage of handling or exchange, whether during internal treatment or through illegal interference;

3. Continued availability of the information or service: ensuring continued working of information systems and continued ability to interact with the information and to provide service to information sites and ensuring that the user of the information is not prevented from using or accessing it;

4. Non-repudiation of information-related action by the person involved: ensuring that the person who is involved in information-related action or information sites cannot deny having been involved because it can be proved that a particular action was performed by a particular person at a particular time;

(c) Establishing a strategy for information security, namely a set of rules that are applied by the persons handling the technology and the information within the establishment connected with input and working with and managing information systems. The objectives of the strategy are: to familiarize users and administrators with their obligations and duties to protect computer systems and networks as well as protecting the information in all its forms at the stages of input, processing, storage, transfer and retrieval.

Lebanon

[Original: Arabic]
[21 June 2006]

In response to the question concerning developments in the field of information and telecommunications in the context of international security, the Ministry of National Defence states as follows:

With respect to the appraisal of information security issues, armed forces information networks are closed networks to which passive security measures apply because modern technology is not available to protect the information owing to the high cost of implementation. As regards telecommunication networks, these are based on the country-wide civilian communications structure which is subject to general law and for that reason security measures are not applied to them.

In the efforts made at the national level to strengthen information security there is a significant difference in legal prosecutions in relation to the technology of informatics and telecommunications as the latter are consistently ahead of the law. In Lebanon the currently available law is No. 140 of 27 October 1999, relating to the protection of the right to the confidentiality of correspondence and conditions for its interception on the basis of a judicial or administrative request in accordance with the conditions specified in articles 2 to 13 of the law. It is worth mentioning here that the legislation is not adequate to coordinate between the security bodies and civilian businesses (ISP-GSM) with a view to standardizing efforts regarding the prosecution, investigation and prevention of potential threats in this field. This highlights the need for international cooperation in this area and for technical and legal expertise to close the gaps between the law and technology in Lebanon.

Qatar

[Original: Arabic]
[12 June 2006]

With respect to developments in the field of telecommunications in the context of international security, the Government of the State of Qatar is making great efforts to exercise complete control over the security of information and of telecommunications in order to avoid existing and potential dangers in information security, by promulgating the necessary legislation to that end.

Qatar recently established a Supreme Council for Communications and Information Technology which comprises a legal department the task of which is to complete the draft Electronic Law of the State and to submit it to the competent authorities, ensure its ratification and bring it into force during the current year. The purpose of the draft law is to prevent the use of computer hardware or technology for criminal or terrorist purposes. The law also requires the competent authorities to define criminal and terrorist purposes so as to make the Member States fully cognizant thereof so that they can carry out their obligations more comprehensively and try to arrive at standard definitions in connection with concepts on which agreement has not been reached internationally in order to facilitate discussion in international forums.

United Arab Emirates

[Original: English]
[17 June 2006]

The United Arab Emirates realizes the growing danger of cybercrime and recognizes that crimes committed in cyberspace do not end at the conventional State borders. Modern information and communications systems make it possible to perform illegal activities from any location and against anyone anywhere.

In order to successfully combat cybercrime, effective action is necessary at the national and international levels.

The United Arab Emirates has taken considerable efforts in strengthening information security at the national level, including:

- **United Arab Emirates cybercrime law**

  The cybercrime law was approved and published in early 2006. It covers the following:

  - Access crimes (unauthorized access, virus dissemination, hacking, identity theft)
  - Data crimes (interception, modification, theft, privacy)
  - Network crimes (interference, modification, destruction)
  - Other related crimes (enabling the commission of crimes, drug trafficking, trafficking in persons, money-laundering, terrorist acts).

  The law also addresses censorship and objectionable material. Non-compliance with the cybercrime law will lead to imprisonment or financial penalties or both.

- **National Computer Emergency Response Team (CERT) Initiative**

  The Telecommunication Regulatory Authority of the United Arab Emirates is looking into establishing a national Computer Emergency Response Team to improve security, respond to cyberattacks, provide early warning and information about cyberthreats, coordinate all incident response activities and build awareness through training and education in the country.

- **Internal service providers code of conduct**

  The United Arab Emirates is on the verge of drafting an enforceable code of conduct for Internet service providers (ISPs) which will force Internet service providers to be efficient and more proactive in reducing bulk e-mails which may contain viruses. ISPs will be expected to proactively scan traffic for open relays, botnets and networks of compromised personal computers used for sending spam. ISPs will also be required to include clauses in their contracts allowing them to disconnect users if they are intentionally or unintentionally relaying spam. Non-compliance with any part of the code will lead to penalties or sanctions.

  The Internet code of conduct is intended to require service providers to abide by high standards of conduct and business practice within the ISP community.

- **Bilateral agreements**

  The ISPs in the United Arab Emirates have actively engaged in bilateral agreements between neighbouring countries in combating spam and have been successful in reducing spam being relayed outside the country. The United Arab Emirates promotes and encourages international cooperation with regard to combating cybercrime, and supports the exploration of memorandums of understanding in terms of information-sharing and cross-border enforcement support.

- **Awareness campaigns/education**

  The Government/Telecommunication Regulatory Authority and the industry are working side by side in promoting awareness and educating people about the benefits that technology offers them and the dangers associated with cybercrime.

  For instance, the Telecommunication Regulatory Authority recently released the "Wireless Security Guidelines" and the "Web Hosting policy". The former provides details on how to set up a wireless network and what steps should be taken for successful secured deployment. The latter outlines the acceptable use of the service, which includes: usage policy; spam policy; policy on intellectual property violations; and policy on illegal contents.

- **Importance of technical measures in the context of international security**

  Several technological measures already exist to aid in securing cyberspace, including:

  – Deployment of public key infrastructures (PKI), and the development of secure protocols;

  – Development of quality software, firewalls, anti-virus programmes, electronic rights management systems, encryption, etc.;

  – Use of smart cards, biometric identification, electronic signatures, role-based technologies, etc.

However, as cyberspace becomes more and more complex and its components more sophisticated, new and unforeseen threats are emerging. Hence, the need for an increased effort to develop security technologies and to always consider security at the outset of the design process of any future technology.

- **Possible measures to strengthen information security at the global level**

  – International collaboration is a must since cybercrime is a borderless crime and cannot be controlled by conventional methods;

  – Common legal framework set in place will allow smooth exchange of information and collaboration between countries. In addition, a global definition of cybercrime needs to be addressed, bearing in mind that the specific definitions will vary from country to country;

  – Law enforcement authorities should be accustomed to dealing with crimes committed in cyberspace. They should be able to search and seize data stored on computers to avoid destruction of criminal evidence.