United Nations A/62/98

General Assembly

Distr.: General
2 July 2007
English
Original: Arabic/Chinese/English/
French/Spanish

Sixty-second session
Item 95 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/62/150.

07-40782 (E) 300707 300707

I. Introduction

1. In paragraph 3 of its resolution 61/54, 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 2007, 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 addenda to the present report.

II. Replies received from Governments

Brunei Darussalam

[Original: English]
[25 June 2007]

Brunei Darussalam submitted the following report from the Royal Brunei Police Force.

I. Introduction

(General appreciation of the issues of information security)

1. Information technology, encompassing all developments in the field of information and telecommunications, has come to play a vital role in all sectors of society. Information technologies are transforming the ways we create, gather, process, manage and share information. Electronic transactions and records are the mainstream and are central to everything from commerce to health care. Computer networking is driving these changes. The exponential growth of both the Internet and the number of users each year exemplifies this transition to a networked society.

2. As a consequence, information security has become an essential component of information technology, especially in the context of the information society. However, it is a complex subject, and the appropriate measures will often depend, to a large extent, on the type and location of the information technology equipment and its infrastructure.

3. Computer networking is driving many of these changes. These transformations also raise new concerns for the security and privacy of networked information. If these concerns are not properly resolved, they threaten to limit the full potential of networking, in terms of both participation and usefulness. Thus, appropriate institutional and technological safeguards are required for a broad range of personal, copyrighted, sensitive or proprietary information.

4. The potential security threats and risks will have to be carefully assessed in every situation, and it is absolutely vital that all concerned are made aware of the threats and risks that affect them and over which they have control. Only then will they fully understand and apply the appropriate security procedures.

5. The focus will be on safeguarding unclassified information in networks, on the security or survivability of networks and on the reliability of network services to ensure information access.

6. There are three main areas to look into: (a) cryptography policy, including governmental information processing standards and controls; (b) guidance on safeguarding unclassified information in governmental agencies; and (c) legal issues and information security, including electronic commerce, privacy and intellectual property.

7. Information safeguards, especially those based on cryptography, are becomingly increasingly important. Appropriate safeguards (countermeasures) must account for and anticipate technical, institutional and social changes that increasingly shift responsibility for safeguarding information to the end users. Broader efforts to safeguard networked information will be frustrated unless cryptography policy issues are resolved. The single most important step towards implementing proper safeguards for networked information in a governmental agency or other organization is for top management to define the overall objectives of the organization, formulate an organizational security policy to reflect those objectives and implement that policy. Only top management can consolidate the consensus and apply the resources necessary to effectively protect networked information.

8. This view attempts to assess the threats and risks posed by criminal activity in information technology environments and to indicate advice that the police can give about security procedures and computer crime prevention methods. Threats to information systems may arise from intentional and unintentional acts and may come from both internal and external sources.

II. Concerns

9. The Royal Brunei Police Force is concerned about the lack of coverage for security preparation in the context of national development of e-Government initiatives.

10. So far, the Royal Brunei Police Force has not been called upon or become involved in national preparations to move into the information age. For the last three years, much legislation has been adopted to prepare the country for the information age. And many governmental and regulatory bodies have been or are being set up to spearhead the e-Government initiatives.

11. Security in terms of law enforcement preparation has been neither actively pursued nor given the same priority as other items on the national agenda. The Royal Brunei Police Force is of the opinion that security plays a very important role in national aspirations to join the information society.

12. Security is crucial for the information age. The importance of putting in a secure and reliable infrastructure cannot be overstressed.

III. Royal Brunei Police Force initiatives

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

13. Because the Royal Brunei Police Force is the leading law enforcement agency in the country, it wishes to provide assistance in spearheading the security aspects required to enter fully into the Information Age.

14. To this end, many officers have been sent overseas to train on Internet-related crimes, especially cybercrimes and transnational crimes. Initially, due to lack of funding, no further advances in procuring the required information technology equipment and software for investigating breaches in computer systems were realized. At present, the Royal Brunei Police Force has the capability to initiate investigations into cybercrime cases.

15. The Royal Brunei Police Force has taken steps to further international cooperation in this field by actively participating in various forums on enhancing law enforcement capabilities. The Royal Brunei Police Force has connections to regional and international law enforcement computer networks, which furthers its capability to pursue fugitives.

IV. Royal Brunei Police Force proposals and recommendations

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

16. The Royal Brunei Police Force presents the following as starting points for facilitating and improving security in the context of information security.

(a) Reporting and monitoring threats and vulnerabilities:

(1) Since Brunei Darussalam Computer Emergency Response Team was formed in 2004, there has been some form of control. However, this control is not complete, as BruCert is not linked in any way to the Royal Brunei Police Force and there is no mechanism to activate a fast response; e.g., monitoring or intercepting a live intrusion, etc.

(b) Education and security mechanisms for safe computing:

(1) Support for the development of educational materials and programmes about cyberspace for all users. This will provide early training in Internet security practices and behaviour.

(2) Investment in awareness campaigns that stress the need for security training for system administrators, network managers and chief information officers;

(3) Facilitation of the development and deployment of security mechanisms for information in cyberspace, mechanisms that allow each party to a transaction to decide what precautions and limitations they want.

(c) Research and development:

(1) Allocation of funds for research and development in the areas of security and survivability for unbounded systems architectures with distributed control;

(2) Development of comprehensive toolkits that support the efforts of network administrators to operate secure systems;

(3) Development of techniques for comprehensive, continuous risk identification and mitigation programmes.

(d) Use of standards:

(1) Establish and encourage acceptance of software security standards as a short-term method to jump-start the process of improving security in Internet products;

(2) Create a Government policy that Government-purchased computer equipment and software must meet specified security standards that include a requirement for a security alert service that notifies the customer of vulnerabilities and repairs.

(e) Laws and law enforcement:

(1) Support our cybercops and allocate appropriate funding to law enforcement agencies to support the training, physical resources and staff necessary to handle the cybercrimes reported;

(2) Ensure that national policy reflects the needs of law enforcement to coordinate internationally to solve crimes in cyberspace and support law enforcement in forming international hot pursuit agreements;

(3) Ensure that public policy facilitates the widespread use of encryption to protect information and users of cyberspace.

Burkina Faso

[Original: French]
[20 June 2007]

1. Burkina Faso gave expression very early on to its political will to develop the new information and communication technologies, which it considers to be a strategic tool for strengthening good governance and bringing about economic and social development.

2. As early as 1996, it undertook a wide-ranging review of the development of the new information and communication technologies, with a view to using those technologies to modernize public services and improve the effectiveness of Government actions.

3. In 1999, it drew up a plan for a national information and communication infrastructure, covering the period 2001-2005. The plan seeks to promote convergence of national polices in the sphere of telecommunications, computer technology and communication media.

4. In 2004, the Government of Burkina Faso adopted a strategy for putting the development plan for the national information and communication infrastructure into operation. With this plan, the Government undertook to guarantee that information and communication technologies would be disseminated throughout society, would be accessible to and owned by all social strata and that their potential would be mobilized for the benefit of national development strategies.

5. But, mindful of the risks arising out of the use of information systems, the Government is striving to create a legal framework directed towards protecting information, making information systems secure, protecting people's fundamental rights, and gaining the trust of business and administration.

6. Accordingly, it adopted Law No. 010-2004/AN of 20 April 2004, which provides for the protection of personal data. This law protects the fundamental rights and liberties of individuals, and their privacy within the context of the processing by computer or by other means of information containing data of a personal nature. Pursuant to this law, decree 2007-283/PRES/PM/MPDH of 18 May 2007 established a commission on information technology and freedoms. This commission is an independent administrative authority with the task of ensuring that the automated processing of personal data, whether by government or private bodies, is carried out in conformity with the law. Being empowered to both regulate and impose penalties, it can act both upstream and downstream issuing opinions and statements before the fact and monitoring activities and imposing penalties.

7. Finally, regulatory bodies have been established to meet the security needs of the information society. One is the Higher Council on Information, under the directorate-general responsible for coordinating development programmes for information and communication technologies, part of the Ministry of Postal Services and Information and Telecommunications Technologies.

8. However, given that the information society does not recognize national boundaries, Burkina Faso takes the view that international cooperation is fundamental in order to render information systems secure. Although, on the other side of the digital divide, in terms of security, the countries of the South are as exposed, as the countries of the North. Collaboration between countries is therefore essential to ensure the security of States, institutions, companies and individuals and of information networks and systems. The only way to combat cybercrime effectively is by enhancing international cooperation.

9. Burkina Faso is pleased to note that the United Nations is interested in the question of information security, and believes that now is the time to draw up an international instrument on security of information technology on the one hand and protection of personal data on the other. In any event, the progress being made in information technology, including telematics, together with the questions of international security, will have to be examined from the point of view of human rights to ensure that the world does not become a society under surveillance, dominated by the dehumanizing reactions of the entire security apparatus.

Chile

[Original: Spanish]
[13 June 2007]

1. Chile attaches great important to information security in the context of international security. We share the global concern at the possibility that information technology can potentially be used for purposes that are inconsistent with the objective of maintaining international stability and security and may adversely affect the infrastructure of States. We believe that it is necessary to prevent information technology from being used for criminal purposes.

2. In the legislative sphere, progress has been made in adopting a number of laws and regulations with respect to the security and confidentiality of electronic documents and the efficient transmission of documents between State administrative organs and between them and the citizens.

3. Because of the importance of this topic, Chile participated actively in the two phases of the World Summit on the Information Society which were held in Geneva, in December 2003, and in Tunis, in November 2005.

China

[Original: Chinese]
[15 May 2007]

1. The rapid development and broad application of information technology are currently playing a positive role in promoting economic and social development and in improving people's lives in countries throughout the world. At the same time, information security has become a major factor influencing the general security of individual countries and even the security and stability of the world as a whole. The appropriate resolution of this issue in accordance with the collective benefit of all countries is a shared responsibility of the international community.

2. It is the view of China that the issue of information security involves not only the risks arising from the weakness and interconnected nature 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. Both of these factors are worthy of concern when studying the issue of information security.

3. 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 the freedom of information technology for all countries.

4. The Chinese Government has always attached great importance to the question of information technology. It has drawn up and progressively implemented a national information-security strategy, and formulated a series of information-security laws, regulations and standards. A great deal of work has been done to strengthen network security monitoring, improve coordination and handling mechanisms, develop research on network-security technology, and construct network-security emergency response systems. Capabilities for protecting the security of basic information networks and important information systems are continuously growing stronger.

5. China actively participates in international cooperation in the field of information security. In June 2006, the heads of the member States of the Shanghai Cooperation Organization signed the "Statement of the Heads of the member States

of the Shanghai Cooperation Organization on international information security", in which it was decided to establish a group of experts on international information security. China has constructively participated in the work of that group.

6. China holds that the United Nations is the appropriate setting in which to explore the issue of information security. From 2004 to 2005, a group of Governmental experts engaged in discussions 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 exploration of information-security issues 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 effective 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.

Cuba

[Original: Spanish]
[16 May 2007]

1. The outcome that Cuba has achieved at this time in respect of information and communication technologies is highly social in character, devoid of any consumerism, and is training a new type of specialist, totally committed and with ethical values that are unrelated to the models promoted by the globalized neoliberal world.

2. The substantial improvement in technological infrastructure and the massive and thorough preparation of human capital from an early age are examples of the enormous efforts being made by the Cuban State to move swiftly towards a computer literate society as a means of improving the country's quality of life, efficiency and competitiveness.

3. Based on this policy, Cuba has organized a rational and efficient use of computer resources, as regards both equipment and connectivity, in a massive social form. Priority is given to key areas such as health, education, scientific centres, cultural institutions and businesses, that ensure the nation's economic and social development.

4. However, this development has come up against a cruel and prolonged economic, commercial and financial blockade imposed by the United States of America, which has been tightened under the present administration.

5. Cuba's Internet connection dates back to 1996 when the United States Government granted Cuba a licence for such access. At present, however, even though international fibre-optic cables pass very close to the coast of Cuba, this blockade has prevented Cuba from connecting to them and, as a result, the country is compelled to use a satellite channel with an outgoing bandwidth of a mere 65 Mbps and an incoming bandwidth of 124 Mbps. Fibre-optic connection would not only permit faster Internet connection but would also result in significant cost reductions. The laws state that, prior to any addition to or modification of the channel, a licence must be obtained from the United States Department of the Treasury.

6. As regards technological infrastructure, the United States blockade not only prevents us from acquiring computer equipment and programmes from United States companies but, because of its extraterritorial nature, it also affects our commercial operations with the firms of other countries; downloading of software and data — including the data — is blocked if the Internet Protocol (IP) number is identified as being Cuban.

7. Given that the Internet is a global common area there certainly are challenges that need to be overcome, not only relating to its governability by all mankind and the consequent inclusion of all countries in its administration but also relating to the eradication of scourges that are universally condemned, such as dissemination of pornography, incitement to terrorism, racism, fraud, dissemination of fascist ideologies and all forms of cybercrime.

8. Another major challenge — about which the rich countries are silent — is the need to do away with the selective and elitist nature of the Internet; currently, the inequalities and barriers that exist in the real world, are being transferred into cyberspace, resulting in what is known as the digital divide.

9. There are millions of people throughout the world who are nowhere near to becoming "internauts" given that they cannot even read or write and that their main daily concern is dealing with hunger, thirst and disease. With political will on the part of Governments, international cooperation and a modicum of the resources that the so-called developed world currently lavishes on advertising, overconsumption and the arms race, the Internet could become a vehicle for bringing about a cultural and educational revolution that would promote knowledge, foster education, culture, cooperation, solidarity and the ethical and moral values so necessary in this new century, as well as safeguarding humanity's nobler feelings and casting aside inhuman, selfish and individualist behaviours.

10. Moreover, security agencies have paid special attention to the topic and most use these technologies to assist the Government. By investing huge amounts of funds they have developed a variety of means and programmes to strengthen existing technologies or create new ways to intercept communications, access databases and systems and create systems for identifying and monitoring vehicles and individuals. These complex networks are made up of antenna systems, listening stations, radars and satellites, supported by submarines and spy planes, all linked to supercomputers and specialized applications.

11. It would be very naive to believe that, in collaborating with said agencies, the companies that supply services and technologies, do not provide them with information to help them with their intelligence-gathering and spying. After all, according to the provisions of the United States Patriot Act, the Government is authorized to demand information — regardless of whether or not it is confidential — from any firm, if it considers such information to be relevant to national security.

12. Given that knowledge is the heritage of mankind as a whole, it is essential to democratize the presence and distribution of the capital that information represents; the latter should be used for the purpose of promoting peace and development, since these are essential for continued progress in the new millennium.

Lebanon

The following letters were received from the Permanent Mission of Lebanon to the United Nations representing communications between the Mission and Lebanon's Ministries of Telecommunications, Interior and Defense.

Ministry of Telecommunications

[Original: English]
[4 June 2007]

1. We are issuing a new law covering the information and communications technology sector in Lebanon, which is in the final approval phase by the Chamber of Deputies. This law shall cover security and all matters related to information crimes.

2. Once the law mentioned above enters into force, the Ministry of Telecommunications will arrange the matters concerning points b, c and d with other ministries and all administrators concerned.

Ministry of Interior

[Original: Arabic]
[23 May 2007]

1. At the national level, information is exchanged between the various Internal Security Forces units by means of wire (telephone and facsimile) and wireless communications (such as operations rooms in various locations), although these methods remain vulnerable to violation and interception by eavesdropping. It should be recalled that, some time ago, the Directorate-General started to expand the TETRA communications network adopted by the Internal Security Forces by using it in certain parts of Lebanon prior to being deployed throughout the country. Moreover, the Security Forces were recently supplied with a network of locked cellular lines, in accordance with Council of Ministers decision No. 47 of 15 September 2006.

2. At the international level, information and, in particular, security information, is exchanged between the Internal Security Forces and other international organizations through the International Communications Division within the Directorate-General of the Internal Security Forces, which has a station for the transmission and reception of security information through the Beirut International Criminal Police Organization (Interpol) office within the Division, which at present uses a regular communications system based on Internet technology and characterized by rapid information exchange. Confidentiality is safeguarded through specialized networks, maintained in conjunction with Interpol, which is responsible for overseeing the administration of the network and updating it.

3. • With regard to subparagraph (a) relating to the general appreciation of the issues of information security, the Internal Security Forces strive to use effective technical means with regard to wire and wireless information and communications security and encounter numerous challenges in so doing, the main one being the standardization of the information security and data protection structure on the basis of appropriate and satisfactory criteria in

order to establish, implement and document the management of information security systems, as well as measures for the regulation of such systems.

- With regard to subparagraphs (b) and (c) relating to efforts to strengthen and enhance information security at the national level and international participation in this sphere, we have had practical and realistic experience in evaluating intrusion risks, based on the condition of the information network. We have made progress in improving the security of our information network, using modern techniques and the solutions and procedures established for systems protection and evaluation of the immunity of systems to intrusion, interference and viruses, as well as in establishing plans that would prevent the disruption of work should systems come under attack and in training competent personnel capable of dealing with emergencies efficiently.

- With regard to subparagraph (d) on possible measures that could be taken by the international community in order to strengthen information security at the global level, we propose first of all to adopt a preventive policy in order to stop individual acts of intrusion and cooperate at the international level to that end. Following that, we propose to draft a law on combating acts of sabotage against and intrusion into information networks and to consider such acts as crimes punishable by law, and, lastly, to exchange experiences with Member States and benefit from their experiences in order to achieve significant qualitative progress in this sphere.

In this regard, it should be noted that the Directorate-General has taken the following steps:

(a) The Directorate-General established an office within the Internal Security Forces dedicated to combating information crime. The principal tasks of the office include reporting information crimes and risks to digital information security, in addition to investigating and prosecuting the perpetrators of such crimes.

(b) A number of specialized officers from the Security Forces participated in the preparation by the Parliamentary Committee on Technology of a draft law on combating information crime. The draft law is now awaiting approval by Parliament.

(c) The Security Forces participate actively in Interpol activities and contribute to the operations of its Regional Working Party on Information Technology Crime — Middle East and North Africa, of which the Vice-Chairperson and one member are Internal Security Forces officers specialized in information technology. Furthermore, the Chief of the Office on Combating Information Crime liaises with Interpol on issues relating to information security and combating information crime, in particular as regards information security.

In view of the threats to security in general, at both national and international levels, and to information and communications systems in particular, a forward-looking strategy needs to be established that takes into consideration technical progress in order to protect information and find means of responding to any violations. In this regard, the following points should be noted:

1. *Information speed and security criteria*

The means whereby information is transferred and stored have advanced with considerable speed due to technological developments, but the difficulties involved in monitoring systems, instruments and content have made it necessary to impose protection measures at all levels. International information security management standards have been established in ISO 17799.

2. *Lebanon and information security*

Lebanon lacks numerous measures at the legislative and executive levels that would ensure a secure information environment. No legislation or administrative measure obliging government departments and institutions to apply information security management standards (ISO 17799) exists, although some directives similar to international standards are applied at present by the Banque du Liban and some private banks. Moreover, no legislation exists on the basic principles of the encryption of private communications networks.

The issue of implementation

Ministry of Telecommunications Circular No. 4/2 of 19 December 2005 concerning keeping files on information traffic is not respected. No legislation exists to regulate Internet cafes, and the monitoring of communications via satellite in Lebanese airspace is ineffectual.

In this regard, it should be noted that, following the terrorist attacks of 11 September 2001, the United States of America established the Department of Homeland Security and adopted a nationwide monitoring system for all communications networks, in order to ensure analysis and surveillance. Moreover, strict legislation on data encryption and network access was established.

3. *Means of combating and preventing information crime*

Cyberspace, as a network using the Transmission Control Protocol/Internet Protocol (TCP/IP) communications protocol, has shown itself to be a fragile and insecure environment which has allowed criminal groups to attack and, on occasion, destroy it, because priority has been given to commercial and marketing objectives. Moreover, cybercrimes are distinguished by speed and the absence of controls or limits, while means of combating them are slow, coordination non-existent and the legislation adopted inadequate.

Numerous improvements have been made to the functioning of Internet protocols both with regard to users and encryption, including the IPv6 protocol. Serious research has continued into security techniques for information networks capable of shielding them from intrusion and destruction.

International agreements on combating cybercrime, in particular the Budapest Convention on Cybercrime, provide for rapid cooperation between States and have led to:

– The establishment of a 24/7 communications network parallel to the Interpol network, specialized in information crime;

– The formation of a steering committee and party regional working subcommittees to encourage technical cooperation and, also, update and enhance the skills of the offices engaged in combating information crime.

However, it appears that the Budapest Convention has not been able to guarantee a rapid and immediate response to viruses that could be released onto the network.

Proposals

- Enhance the effectiveness and improve legislation on information security and, consequently, the application of information security protection standards.
- Enhance the effectiveness and improve security efforts in all security services, in order to protect information systems and means.
- Enhance the effectiveness and improve the specialized machineries within the Ministry of Telecommunications and ensure that they interact with the security services and public and private institutions, in order to create a secure environment for information systems.
- Keep abreast of new developments, in particular with regard to the implementation of Internet protocols such as IPv6, adopt the technical means necessary for the identification of all persons entering the Internet network, and adopt the Digital ID (Digital Certificate) system.
- Strengthen coordination between machineries for the protection of the law in the area of information security, establish unified international standards at the technical level in order to facilitate follow-up, monitoring and coordination and, as a minimum, unify legislative systems in order to maintain national security in accordance with international security requirements.

The Directorate-General for General Security reports that its security communications occur inside Lebanese territory and that there are no external communications. Systems for the protection of internal communications are being improved with the expertise and support of friendly security machineries. However, the necessary equipment is still not in place due to the unavailability of financial and technical resources.

Ministry of National Defence

[Original: Arabic]
[1 May 2007]

The Ministry of National Defence indicates that Lebanon:

- Is committed to ensuring that information technology and wire and wireless means of communication should not be used for purposes incompatible with the concepts of international stability and security;
- Is taking the measures necessary at the national level (improvement and modernization of the relevant regulations and laws) in order to strengthen information security, and encourages the exchange of available information to the parties concerned.

Lebanon respects and cooperates with the United Nations resolutions on the protection of the security and confidentiality of information and prevention of its abuse in any manner and the need to prevent information sources or technology from being used for criminal or terrorist purposes.

Mexico

[Original: Spanish]
[22 May 2007]

1. Mexico supported the resolution on "Developments in the field of information and telecommunications in the context of international security", put forward by the Russian Federation in the General Assembly and attaches great importance to promoting a wider exchange of views on that subject and related concepts. Mexico is of the view that presentations by experts or discussions on the topic might take place in conjunction with the work of the First Committee or other disarmament forums.

2. Most international verification mechanisms arising from international legal instruments or political agreements on export control rely on information media and telecommunications for their effective implementation, and it is of fundamental importance to examine the status of developments in those areas. Moreover, the development of ballistic missile systems and the modernization of nuclear arsenals necessarily entail development of information and telecommunications. In addition, developments in space technology and satellites are unquestionably linked to international security issues.

3. Mexico has consistently drawn attention in the Conference on Disarmament to the urgent need for the Conference to adopt a programme of work which includes as one of its main areas "prevention of an arms race in outer space", an issue linked to that of the vulnerability of space-based information and communications technologies.

4. Mexico considers it important to extend the mandate of the group of governmental experts on the subject, established pursuant to resolution 58/32 and to be re-established in 2009, and believes that broad discussion should be promoted in the interim until that date.