United Nations A/64/129/Add.1

General Assembly

Distr.: General
9 September 2009
English
Original: French/Spanish

Sixty-fourth session
Item 91 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/64/150 and Corr.1.
** The information in the present document was received after the submission of the main report.

09-50575 (E) 230909 240909

II. Replies received from Governments

Cuba

[Original: Spanish]
[2 July 2009]

1. Cuba fully shares the concerns expressed in General Assembly resolution 63/37 with respect to the use of information technology and media for purposes inconsistent with international stability and security and which adversely affect the integrity of States, to the detriment of their security in both civil and military fields. This resolution also appropriately stresses the need to prevent the use of information resources and technologies for criminal or terrorist purposes.

2. Cuba reiterates that the hostile use of telecommunications, with the declared or hidden intent of undermining the legal and political order of States, is a violation of the internationally recognized norms in this area and a negative and irresponsible use of such means, which can give rise to tensions and situations that are not conducive to international peace and security and thereby undermine the principles and purposes enshrined in the Charter of the United Nations.

3. Cuba draws attention with concern to the fact that information and telecommunications systems can be turned into weapons when they are designed and/or used to damage the infrastructure of a State, and as a result, can put at risk international peace and security.

4. In this regard, it wishes to reiterate the condemnation already issued by the Republic of Cuba in various international forums of the aggressive escalation by successive United States administrations in its radio and television war against Cuba, in clear violation of existing international law in the field of the regulation of the radio-electric spectrum.

5. The United States Government has made no reparations for the damage that could be caused to international peace and security, and creates dangerous situations, for instance the use of a military aircraft to transmit television signals to Cuba without its consent. This attitude is inappropriate for a Permanent Member of the United Nations Security Council.

6. The radio-electric aggression against Cuba from United States territory violates the principles of international law governing relations between States and the norms and regulations of the International Telecommunication Union, which establishes the conduct to be followed for member countries of that specialized agency of the United Nations system.

7. At the end of May 2009, a total of 1,924 hours of weekly illegal transmissions from the United States to Cuba, broadcast on 30 frequencies, had been recorded. Some of these radio broadcasters belong to or offer their services to organizations linked with known terrorist elements who live in and act against Cuba from United States territory, broadcasting programmes in which they incite sabotage, political attacks and assassination, among other topics of radio-terrorism.

8. These provocative broadcasts against Cuba constitute violations of the following international principles:

– The fundamental principles of the International Telecommunication Union, expressed in the preamble to its Constitution, on the growing importance of telecommunications for the preservation of peace and the economic and social development of all States, with the object of facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunications services. The content of the television programming broadcast by the Government of the United States against Cuba is subversive, destabilizing and deceptive in character, contradicting those principles.

– Provisions CS 197 and CS 198 of the Constitution of the International Telecommunication Union stating that all stations must be effectively established and operated in such a manner as not to cause harmful interference to the radio services or communications of other member States.

– Agreement at the ninth plenary meeting of the World Radiocommunication Conference (WRC) held in November 2007, which stated in its paragraph 6.1 (g) "*that a broadcasting station operating on board an aircraft and transmitting solely to the territory of another administration without its agreement cannot be considered in conformity with the Radio Regulations*".

– Article 8.3 of the ITU Radio Regulations establishing that internationally recognized frequencies assigned and recorded must be taken into account by other administrations when making their own assignments in order to avoid harmful interference.

– Article 42.4 of the ITU Radio Regulations, prohibiting the operation of a broadcasting service by an aircraft station at sea and over the sea.

– A ruling of the ITU Radio Regulations Board which, at its 35th meeting in December 2004, established that United States transmissions on the 213 MHz frequency resulted in harmful interference with Cuban services and demanded that the United States Government must take the relevant measures to eliminate it. Furthermore, since September 2006 the Radio Regulations Board has been requesting the United States Government to take measures to eliminate interference at 509 MHz, with no response to date. In the Summary of Decisions of the fiftieth session of the Board, which ended on 20 March 2009, it was once again stated that the transmissions are illegal and the United States Government was requested to take all necessary measures with a view to eliminating these two cases of interference with television services in Cuba.

– Article 23.3 of the ITU Radio Regulations, limiting television broadcasting outside national frontiers. A report issued in January 2009 by the General Accounting Office (GAO) of the United States of America, an official government agency, recognizes the violations of international norms and domestic legislation incurred by the programme of radio and television broadcasts by the United States Government against Cuba.

9. Cuba recalls, moreover, that the World Radiocommunications Conference (WRC-07) which met in Geneva, Switzerland from 22 October to 16 November 2007, adopted conclusions that found transmissions from aircraft from the United

States to Cuba to be in violation of the Radio Regulations. The conclusions endorsed by the plenary stated that "*a broadcasting station operating on board an aircraft and transmitting solely to the territory of another administration without its agreement cannot be considered in conformity with the Radio Regulations*". These conclusions were agreed at the plenary level of the 2007 Conference and have legal standing in the work of ITU. The World Radiocommunications Conference thus endorsed the 1990 ruling of the former International Frequency Registration Board, that television broadcasts from an aircraft with programming directed to Cuban national territory were in violation of the regulations.

10. The hostility of the Government of the United States of America against Cuba has been manifested through the economic, financial and trade embargo imposed for almost 50 years, which also affects the information and telecommunications field. This can be shown through the following examples, among many others:

- Cuba does not have the right to access the services offered by many websites; when it is recognized that the link is being established from an Internet address with the Cuban domain name .cu, access is denied.
- Without prior notification, the Office of Foreign Assets Control (OFAC) has recently blocked .com domains related to Cuba.
- Another illustration is the public announcement in May 2009 by the technology company Microsoft that it was discontinuing its service "Windows Live Messenger IM" for Cuba and other countries "because of its obligation to observe United States law". On connecting to this tool, a message reads: "Microsoft has discontinued Windows Live Messenger IM for users in countries under United States embargo, therefore Microsoft will no longer offer Windows Live service in your country".
- Other web pages have also denied access from the domain name .cu: Cisco Systems (http://tools.cisco.com/RPF/register.do) technologies for connection, routers for Internet access servers, including equipment in the field of digital video; SolidWorks (http://www.solidworks.com/sw/termsofuse.html) automated design systems and Symantec (http://www.symantec.com/about/profile/policies/legal) anti-virus protection software.
- With complete cynicism and hypocrisy, the United States falsely accuses Cuba of preventing its citizens from accessing the global network, while the very different reality is that Cuba is unable to connect to the fibre-optic cables that surround the Cuban archipelago, owing to the embargo laws applied by the United States.
- The *Empresa de Telecomunicaciones de Cuba S.A. (ETECSA)* has experienced losses on the order of US $53,769.80 up to December 2008, basically owing to the lack of access to the United States market to purchase specialized equipment. It is forced to find intermediaries, thus greatly increasing the prices of the products needed to guarantee its services.

11. This attitude by the United States erodes the spirit, the intentions and the conclusions that prevailed among the nations of the entire world when they met in Switzerland and Tunisia during the World Summit on the Information Society. The Summit strongly urged States, when building the information society, to take the necessary measures to avoid and refrain from adopting unilateral measures that were

not in keeping with international law and the Charter of the United Nations, prevented the full achievement of the economic and social development of the population of the countries affected or adversely affected the well-being of their citizens.

12. The twelfth session of the Commission on Science and Technology for Development, held in Geneva from 25 to 29 May 2009, in reviewing the progress made in the implementation and follow-up to its recommendations, provided an important forum for Cuba once again to denounce the application of the embargo policy by the United States Government, in particular unilateral coercive measures against the development of communications technologies and access to information, as well as the implementation of a policy of aggression against Cuba's radio-electric spectrum, which violates the conclusions adopted at the two phases of the aforementioned Summit.

13. The discussion in the General Assembly about development in the field of information and telecommunications in the context of international security is very pertinent and its timeliness and importance increase every day. Actions such as those described above by the United States of America against Cuba confirm the need for that debate and the urgency of finding solutions to put an end to such manifestations of State terrorism.

14. Cuba strongly supports this exercise by the General Assembly and, consequently, joined the 178 Member States that voted in favour of resolution 63/37, in contrast to the attitude of the United States of America, the only country that voted against it.

15. Cuba will continue to spare no effort in offering its support to the peaceful global development of information and telecommunications technologies and their use for the good of all humanity, and is ready to collaborate with all other countries, including the United States of America, to find solutions that overcome the obstacles that prevent the achievement of these goals.

Mali

[Original: French]
[9 July 2009]

Views and assessments on implementation of the resolution on developments in the field of information and telecommunications in the context of international security

General appreciation of the issues of information security

1. The main types of attacks on information systems are denial-of-service attacks, which seek to disable the system, and intrusions with the aim of misappropriating information.

2. The threats to which government systems, or the systems of sensitive companies, are exposed are threats or incidents affecting the confidentiality, integrity and availability of their essential information infrastructure.

3. Among others, these include:

- threats orchestrated by a foreign Government or a terrorist or extremist group with a political agenda
- threats carried out for the purposes of espionage, sabotage, foreign interference or political violence (terrorism)

4. The use of information technology is emerging as an alternative to more traditional threats such as destruction, electromagnetic jamming, physical intrusion or control of internal information sources.

5. Cyberattacks may target individuals as well as companies or public institutions. In the case of attacks that call into question national defence or security, Government departments, essential operators and companies operating in strategic or sensitive areas are at particular risk. However, the consequences will vary according to whether attacks target sites or services accessible by the public, operational systems or, more directly, persons holding sensitive information.

6. It is particularly difficult to trace the origin of a cyberattack. A whole series of computers, which may be located in several different countries, are generally used to carry out the attack. Tracing it back to its point of origin would involve extremely lengthy investigations subject to the vagaries of international legal cooperation. The perpetrators have many different methods of concealment, which range from taking over computers without their owners' knowledge to using anonymous public computers, such as those found in Internet cafés.

7. Even so, most Government departments and observers attribute these attacks to groups of hackers, apparently using increasingly sophisticated methods.

National efforts and international cooperation to strengthen information security

(a) National efforts

8. Mali does not currently have any legislation in force regarding information security.

9. The establishment of a legal and regulatory framework is one of the main priorities of the national strategic plan on information and communications technology (ICT) adopted by the Government in June 2005.

10. The Malian Government has obtained a credit (No. 4033 MLI) from the International Development Association (IDA) to finance its Growth Support Project. It plans to use part of this credit for a consultation exercise on technical assistance for the preparation of Mali's ICT legal and regulatory framework.

11. With regard to the selection of consultants by World Bank borrowers, a request for expressions of interest (No. 001/2009/SPM/UCP-PAC) has been issued in accordance with the terms of reference drafted by the Malian Information and Communication Technology Agency in May 2008.

12. The legal and regulatory framework is expected to include legislation on freedoms; business; e-commerce; intellectual property; data security and confidentiality; crimes and offences in cyberspace; and unrestricted access to public information or information constituting the shared heritage of humanity.

(b) International cooperation to strengthen information security

13. Cyberattacks cross borders and can be directed against several States simultaneously. Network surveillance and the development of responses in the event of an incident warrant international cooperation and assistance. More generally, protecting information systems from illegal activities is now a concern shared by many States.

14. Mali has opted for a regional approach to the development of telecommunications sector regulations, leading to ratification of the relevant directives of the West African Economic and Monetary Union in 2006 and the Economic Community of West African States supplementary acts in 2007.

15. The International Telecommunication Union is working to establish an international framework for the promotion of cybersecurity (the Global Cybersecurity Agenda), in which the Malian State is particularly interested. This promotion of cybersecurity has led to the establishment of a High-Level Experts Group responsible for proposing a long-term strategy that encompasses legal measures; technical measures to remedy software flaws; the prevention and detection of cyberattacks; and crisis management.

The content of international concepts aimed at strengthening information and telecommunications security

16. International information security should be based on existing international law (*jus ad bellum*), which defines how to counter threats to international peace and security, and international humanitarian law (*jus in bello*), which relates to the means and methods of warfare; the protection of States that are not party to the conflict; and persons and property that are or could be affected by the conflict.

17. The Charter of the United Nations is the cornerstone of international law concerning the maintenance of international peace and security.

18. It is widely acknowledged by international law experts that these rules establish a universal mechanism for maintaining international peace and security. Since information and communications technology is now being developed or used as a means of destruction (in other words, “information weapons”) and the international community has not yet agreed on the place of information security within existing international law, the Charter of the United Nations could be interpreted in such a way as to give international actors a considerable degree of freedom to use information and communications technology both to take aggressive actions and to settle international conflicts and disputes.

19. This surprising situation is attributable to the fact that hostile actions in the information area are not yet explicitly considered within international law as being on a par with hostile actions undertaken with conventional weapons, even though, in view of the interconnectivity of today’s world and its dependence on information and communications technology, such an attack would be just as devastating as a conventional attack, if not more so. The difficulties are exacerbated by the absence of any generally accepted interpretations of concepts such as “acts of aggression” (Art. 1), “force” (Art. 2, para. 4) and “armed attack” (Art. 51) in relation to information security.

20. General Assembly resolution 3314 (XXIX) of 14 December 1974 defines an act of aggression.

21. Although this resolution was not adopted by consensus, its "soft law" provisions provide the United Nations Security Council and all members of the international community with criteria for determining an act of aggression.

22. The use of an information weapon could be interpreted as an act of aggression if the victim State has reasons to believe that the attack was carried out by the armed forces of another State and was aimed at disrupting the operation of military facilities, destroying defensive and economic capacity, or violating the State's sovereignty over a particular territory.

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

23. In order to strengthen information security at the global level, and address the threat of information and communications technology being used for hostile purposes, the international community should increase its involvement in such areas as:

(a) Supporting States in increasing awareness of and responsibility for information security among different actors (public bodies, companies and users);

In this connection, the coordination of States' policies for supporting the industrial and technological base in terms of secure products should receive considerable attention. Major emphasis should also be placed on cooperation between States and the private sector.

(b) Strengthening States' capacity by making available to them the human resources and technical expertise needed to monitor traffic and hence to detect the abnormal flows by means of which cyberattacks are transmitted;

(c) Reorganizing the policies of the various international agencies working in the field of information system security, attributing specific areas of competence to each of them;

(d) Establishing indicators in the area of information security to help countries manage their information and communications technology infrastructure more effectively. These indicators could relate to such matters as:

- data recovery in the event of a disaster
- use of standards
- performance monitoring (benchmarking)
- electronic transfer
- collaboration with the International Criminal Police Organization (INTERPOL)
- access platforms.

Conclusion

24. To conclude our assessment, it appears that questions regarding information security and the use of information and communications technology for malicious

purposes are of increasing concern. Such technology certainly offers countless advantages; however, in view of its uncontrolled development, it could lead to disasters with incalculable consequences.

25. No satisfactory responses have as yet been found to the legal issues raised by the development of this technology, owing to the existence of diverse and often inappropriate regulatory frameworks.

26. It is therefore the role of States to oversee the harmonious development of these tools in order to ensure that better progress is made towards a more secure information society.

Spain

[Original: Spanish]
[8 July 2009]

Position of Spain on developments in the field of information and telecommunications in the context of international security

Introduction

1. Information security is a key aspect of the information society. Technological advances have driven continuous, rapid growth in the capacity to process and store information, in multiple formats. Meanwhile, in the area of communications, available bandwidth has increased very significantly and, as a result, huge amounts of information can now be sent and received, almost in real time and without the need for particularly complex infrastructure.

2. While these technological advances improve access to information of all types, they also facilitate the use of, or access to, information for unlawful purposes, especially the use of information technology and telecommunications systems for hostile or criminal purposes, or even for the commission of terrorist acts or acts of aggression, between States or transnational actors.

3. Over the past year, the growing trend in Internet use by criminal organizations, and, in particular, terrorist groups, has been confirmed. Such organizations and groups essentially take advantage of two of its characteristics, namely, its global nature and the high degree of anonymity that it can offer.

4. The development of the information society and information technology must therefore be balanced with the simultaneous development of modern, up-to-date national and international regulations that are appropriate to the new technological environment and capable of responding to the challenges posed by the need to protect information, in order to prevent its unlawful use, without limiting individuals' rights and freedoms.

Misuse of the Internet for terrorist purposes

5. At present the main threats arising from the use of the Internet by terrorist organizations are as follows:

(a) Use of the Internet as a weapon, i.e., its use as a means to launch attacks against critical infrastructure information systems or the infrastructure of the Internet itself. Attacks of this kind by common criminals are relatively frequent; however, the attack suffered by Estonia in 2007 made it clear that a State's information infrastructure can also be subject to an attack of this type. The considerable increase in new harmful software over the last two years and the "botnets", or networks of zombie computers, that are used to carry out attacks against information technology systems, are directly related to this type of threat.

(b) Use of the Internet as a medium for other activities, essentially:

- Communication. Criminal organizations are increasingly communicating via the Internet instead of using other means such as fixed or mobile telephony. The tools most frequently used to communicate over the Internet are electronic mail, instant messaging programmes and forums.
- Dissemination of propaganda and terrorism-related materials. There are currently thousands of websites that incite violence or are related to terrorist activities; this trend has been accentuated with the emergence of "blogs". Preventing terrorist organizations from using the Internet in this way is quite a complex matter since such websites can be very easily migrated. The phenomenon is transnational since the server that hosts the website may be located in a different country from the one where it is administered, while the terrorist organization in question may operate in a third country.
- Recruitment. The Internet is sometimes used as a means of carrying out recruitment activities, mainly through forums and instant messaging programmes.
- Financing. The Internet also provides opportunities for terrorist organizations to carry out activities aimed at securing funding. The possible involvement of terrorist organizations in Internet fraud as a means of obtaining financing is of particular interest.
- Dissemination of training manuals. Terrorist organizations disseminate manuals on terrorist techniques, manufacture of explosives and weapons handling via the Internet.
- Information-gathering to prepare terrorist attacks. The Internet is a very important source of information that is often used by terrorist organizations to obtain information on the targets of their activities.

Measures taken at the national level to combat Internet use by terrorist organizations

Legislative measures

6. Among the measures adopted by different States, Spain has made great efforts in this regard over recent years, and particularly in 2007. It has included in its legal system a series of laws relating to information security and the free exercise of the rights and freedoms recognized in the Universal Declaration of Human Rights and the Spanish Constitution. Comprehensive legislation and regulations have been developed, incorporating both purely national elements and European Union directives, with the aim of meeting these objectives. In this connection, new

information security criteria have been applied, based on the premise that, in order to achieve a reasonable degree of protection, as well as to maintain the confidentiality of information, it is in most cases essential to preserve the integrity and availability of the information. In particular, the following laws and regulations have been enacted (in chronological order):

- Organization Act No. 5/1992 of 29 October 1992 on the regulation of the electronic processing of personal data, with the aim of establishing precautionary mechanisms to prevent breaches of privacy resulting from the processing of information; and implementing regulations.
- Organization Act No. 15/1999 of 13 December 1999 on the protection of personal data, which aims to guarantee and protect, in relation to the processing of personal data, public freedoms and the fundamental rights of individuals, especially their honour and their personal and family privacy; and implementing regulations.
- Royal Decree-Law No. 14/1999 of 17 September 1999 on electronic signatures, adopted with the aim of encouraging companies, citizens and public authorities to quickly incorporate new technologies for secure electronic communications into their activities, and transposing into Spanish law Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Act No. 59/2003 of 19 December 2003 on electronic signatures updated this framework by incorporating the amendments advisable in light of the experience gained since its entry into force.
- Act No. 11/2002 of 6 May 2002, governing the National Intelligence Centre, and Royal Decree No. 421/2004 of 12 March 2004, which governs the National Cryptological Centre. By means of these two instruments, the National Intelligence Centre is mandated, among other duties, to coordinate the action of the various Government agencies that use encryption methods and procedures, guarantee the security of information technology in that area and ensure compliance with regulations relating to the protection of classified information.
- Act No. 34/2002 of 11 July 2002 on information society services and electronic commerce, which aims to incorporate into Spanish law Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (“Directive on electronic commerce”). It also partially incorporates Directive 98/27/EC of the European Parliament and of the Council of 19 May 1998 on injunctions for the protection of consumers’ interests, since, in accordance with the provisions of that Directive, it governs actions for an injunction against conduct contravening the provisions of the Act.
- General Telecommunications Act No. 32/2003 of 13 November 2003, governing the operation of networks and provision of services in the area of electronic communications.
- Act No. 59/2003 of 19 December 2003 on electronic signatures, already mentioned.

- Act No. 11/2007 of 22 June 2007 on citizens' electronic access to public services, which governs communications through the use and application of electronic, information and telematic techniques and methods, between citizens and public authorities.
- Organization Act No. 10/2007 of 8 October 2007 governing the police database of DNA identifiers. The Act establishes a single database incorporating all files of the State security forces and bodies containing identifiers obtained from DNA analysis carried out as part of a criminal investigation, corpse identification procedures or missing person enquiries.
- Act 25/2007 of 18 October 2007 on the preservation of data relating to electronic communications and public communications networks, which is having a positive impact on investigations carried out in this field.
- Royal Decree No. 1720/2007 of 21 December 2007, adopting the implementing regulations of Organization Act No. 15/1999 of 13 December 1999 on the protection of personal data.
- Act No. 56/2007 of 28 December 2007 on measures to promote the information society.
- Criminalization of the following cybercrimes related to the Internet activity of terrorist organizations:
  - Computer sabotage, article 264 of the Penal Code;
  - Threats, article 169 and following of the Penal Code;
  - Justification or glorification (apologie) of terrorism, article 578 of the Penal Code.

Other measures

- Creation of specialist police groups to combat use of the Internet by criminal groups.
- Participation in the Check the Web project developed by the European Police Office (Europol).
- Creation of a Computer Emergency Response Team (CERT) to improve the security of public authorities' information systems.
- Creation of the National Centre for the Protection of Critical Infrastructure.

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

- Internet use by terrorist organizations is a transnational phenomenon that often requires joint investigations in different countries. The investigation and prevention of terrorist activities on the Internet therefore depends to a major extent on the existence of international agreements and other tools of international cooperation. In this respect, it is important to move towards harmonizing legislation in order to be able to combat more effectively the presence of these criminal groups on the Internet. International police cooperation is also a key element since speed is crucial in this type of investigation owing to the volatility of electronic evidence.

- Private sector involvement in combating cybercrime. The cooperation of the private sector is essential since most Internet services are in the hands of private companies. The private sector has long been dealing with Internet-related threats and its knowledge and experience in this area could be very valuable.
- Awareness-raising among end users so that they pay attention to the security of their information systems. Greater awareness of the problem would reduce the number of computers used by cybercriminals to carry out their activities, particularly in relation to botnets.
- With regard to possible measures that could be taken by the international community to strengthen information security at the global level, States should sign a convention (similar to the International Convention for the Safety of Life at Sea), in which they would undertake to harmonize their legislation so as to enable the prosecution of Internet crimes, with the aim of ensuring, as far as possible, that anonymity, economic interests and the absence of legislation do not make the Internet an ideal breeding ground for crime and terrorism. That goal should be balanced with the need to preserve freedom of information and free access to information.
- In view of the diffuse nature of the Internet and the volatility of connection records, as determined by the legislation of each country, procedures for international legal and police cooperation should be expedited so that criminal offences can be prosecuted rapidly and efficiently.

7. In conclusion, Spain considers that the international community should adopt all measures to protect information that are deemed necessary, basing its action on an integrated global vision and, if possible, creating a single authority that would lay down rules and standards common to all countries, establish a balanced and comprehensive set of specific protection measures and enable the harmonization of the policies and actions of the various national and international organizations involved.