United Nations A/65/154

General Assembly

Distr.: General
20 July 2010
English
Original: English/Russian/Spanish

Sixty-fifth session
Item 94 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/65/150.

10-45842 (E) 130810 160810

I. Introduction

1. In paragraph 3 of its resolution 64/25, 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 the concepts mentioned in paragraph 2 of the resolution;

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

2. Pursuant to that request, on 26 February 2010, a note verbale was sent to Member States inviting them to provide information on the subject. The replies received are contained in section II below. Any additional replies received will be issued as addenda to the present report.

II. Replies received from Governments

Cuba

[Original: Spanish]
[27 May 2010]

1. Cuba fully shares the concern expressed in General Assembly resolution 64/25 with respect to the use of information technologies and media for purposes incompatible with international stability and security and which adversely affect the integrity of States, to the detriment of their security in the civilian and military spheres. 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 on this subject and a negative and irresponsible use of such means, which may give rise to tension 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 telecommunication systems may be turned into weapons when they are designed and/or used to damage the infrastructure of a State and, as a result, may endanger international security and peace.

4. In this regard, Cuba reiterates its condemnation, already expressed in various international forums, of the aggressive escalation by successive United States administrations of their radio and television war against Cuba, in clear violation of the international rules in force governing the radio-electric spectrum.

5. The United States Government did not care about the damage which it might cause to international peace and security by creating dangerous situations, such as

the use of a military aircraft to transmit television signals to Cuba without its agreement.

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 (ITU), which establish the conduct to be adopted by member countries of that specialized agency of the United Nations system.

7. Each week, broadcasters located in United States territory transmit thousands of hours of radio and television programmes on 34 different medium-wave, short-wave, FM and TV frequencies. In March 2010, there were 2,156 hours of illegal transmissions each week. Several of these 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, with the full agreement of the United States authorities.

8. The illegal radio and television broadcasts against Cuba do not provide information; on the contrary, they falsify and distort it for subversive purposes. For actions of this kind, the United States Congress annually approves a budget of over $30 million in federal funds. Since the two broadcasters commenced activities, the United States Government has spent $659.8 billion for this purpose.

9. 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 telecommunication 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 telecommunication services. The content of the television programming broadcast by the Government of the United States of America 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 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”.

– ITU Radio Regulation 8.3 establishing that internationally recognized frequency assignments recorded must be taken into account by other administrations when making their own assignments, in order to avoid harmful interference.

– ITU Radio Regulation 42.4, 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 emissions on 213 MHz resulted in harmful interference with Cuban services and requested the United States Government to take the relevant measures to halt them. Furthermore, since September 2006 the Radio Regulations Board has been requesting the United States Government to take measures to eliminate interference on 509 MHz, with no response to date. In the Summary of Decisions of the fiftieth meeting of the Board, which ended on 20 March 2009 (document RRB09-1/5), it was once again stated that the transmissions are illegal and the United States Government was requested to take all necessary steps with a view to eliminating these two cases of interference with television services in Cuba. On 26 March 2010, at its fifty-third meeting, the ITU Radio Regulations Board reiterated its conclusion that the broadcasts from the United States cause interference harmful to the Cuban stations included in the International Frequency Register and urged the United States administration to eliminate this harmful interference, requesting the Radiocommunication Bureau to monitor the situation and to act in accordance with the procedures established in the Radio Regulations.

– ITU Radio Regulation 23.3, limiting television broadcasting outside national frontiers.

10. 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 committed by the programme of radio and television broadcasts by the United States Government against Cuba.

– The report recalled that the International Telecommunication Union had determined in 2004 and 2006 that United States broadcasting on channels 13 and 20 was causing harmful interference to Cuban stations and that the State Department had taken no action in response to the ITU determination. The report also stated that the World Radiocommunication Conference, held in November 2007, had found that transmission from an aircraft was not in conformity with ITU regulations.

– The report had stated that, although United States legislation prohibited the domestic dissemination of broadcasts of that type, both the radio and television broadcasts were received in the territory of the United States, principally in Miami, and that the stations under contract aired paid political advertisements and commercials for sex services. In addition, it noted that the broadcasts against Cuba did not adhere to journalistic standards of balance and objectivity and used incendiary and offensive language.

11. Cuba recalls, moreover, that the World Radiocommunication 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*".

12. These conclusions were agreed in the plenary of the 2007 Conference and have legal standing in the work of ITU. The World Radiocommunication Conference thus

endorsed the 1990 ruling of the former International Frequency Registration Board that television broadcasts from an aerostat with programming directed to Cuban national territory were in violation of the regulations.

13. The hostility of the Government of the United States of America towards Cuba has been manifested through the economic, financial and trade embargo imposed for almost 50 years, which also affects information and telecommunications.

– Cuba is not able to access the services provided 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 blocked .com domains related to Cuba.

– Because of the laws on the economic, trade and financial embargo imposed by the Government of the United States of America, Cuba is unable to connect to the fibre-optic cables that surround the Cuban archipelago, forcing the country to pay for satellite services involving bandwidth restrictions, serious problems acquiring the necessary technologies and high connection costs.

– The Internet is being used to conduct defamatory campaigns against Cuba for subversive purposes and in order to discredit the country.

14. This attitude 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, in 2003 and 2005.

15. The Summit strongly urged States, in building the information society, to take steps with a view to the avoidance of, and refrain from, any unilateral measure not in accordance with international law and the Charter of the United Nations that impedes the full achievement of economic and social development by the population of the affected countries and that hinders the well-being of their population.

16. The discussion in the United Nations General Assembly about developments in information and telecommunications in the context of international security is very relevant and becoming ever more timely and important. Actions by the United States against Cuba such as those described above confirm the need for this debate and the urgency of finding ways to end such manifestations.

17. Cuba strongly supports this exercise by the General Assembly and will continue to spare no effort to contribute to the peaceful global development of information and telecommunication technologies and their use for the good of all humanity. It is also ready to collaborate with other countries, including the United States of America, to find solutions that will overcome the obstacles preventing the achievement of these goals.

Greece

[Original: English]
[28 June 2010]

1. Information security issues have been more extensively addressed than in the past. Counter-measures to the modern threats that are inherent to the advent of the globalization of networks and systems are certainly considered. Measures to

preserve the free flow of information are studied and applied in the national and cross-border context.

2. Current international and multinational concepts are followed and studied. International guidance on risk assessment is needed. Cyber defence should also be addressed. National sovereignty rights for information security in global sharing should be maintained.

3. It is understood that all Member States should continue to inform the Secretary-General on their views and assessments on the corresponding questions. In this respect the following points are noted:

(a) All information security issues are highly appreciated in general;

(b) Ways to preserve the free flow of information and provide for the required degrees of confidentiality, integrity and availability are studied and applied within the national and cross-border context;

(c) The concepts for the interconnection of networks that provide for capabilities enabled and shared at both the national and international levels should be drafted and agreed. Risk assessment for the interconnection of networks must prevail and relevant international guidance should be available. Further to that, and since a very serious concern for every nation has been the need to take measures for its cyber defence, coherent international guidance is needed for cooperation, efficiency and economy. Last but not least, the requirement for a nation to preserve its sovereignty and maintain its own base of information cannot be overlooked and every concept drafted should account for that;

(d) Possible measure to be taken by the international community to strengthen information security at the global level are the following:

(1) Relevant international concepts should be detailed and agreed;

(2) A guidance plan for a harmonized generic infrastructure, covering basic legislation matters, could be proposed, in order to deliver to a number of certified users the required information security for electronic handling of all correspondence and messaging, providing multiple ways of communication;

(3) Concepts followed by multinational alliances and small nations' constellations should be harmonized and expanded to be applicable at the global level. The agreement to specify the threat and its negative effect could be more than the engineering of any sophisticated measures devised, since they could also be used by adversaries;

(4) In parallel to all of the above, the nation's sovereignty should be understood as the basic reference for every attempt of globalization. An international concept for defining the national information exchange gateways, with scenarios reflecting the desired level of integration, should be drafted and used as a guide, for all efforts at the national, multinational and international levels.

Mexico

[Original: Spanish]
[18 May 2010]

General overview of information security problems

1. In Mexico, the banking and financial institutions, as well as the units of the Federal Government dealing with public security and national security, are the organizations making the greatest effort in the area of computer security. There is a Cybercrime Unit and a cyberpolice unit within the Federal Public Security Secretariat to deal with public security cybercrime.

2. On the other hand, although individual efforts to combat cybercrime are being made in the three branches of government, the Federal Government does not have a cybersecurity policy governing strategies to combat cybercrime in Mexico, the legislation on the subject must be strengthened, judges need more tools for dealing with and punishing cybercrime, and the regulations on Internet service providers also need to be expanded so that they are required to keep a record of activity on their platforms and to provide information in the event of an incident. There is also a need for domestic agreements and cooperation arrangements with other countries for combating cybercrime and cyberterrorism undermining national security.

Measures adopted at the national level to enhance information security and contribute to international cooperation in this area

3. Efforts are being made in Mexico to create certainty as regards information security:

(a) Certain cybercrimes are covered in the following laws: Federal Criminal Code, Federal District Criminal Code, Federal Code of Criminal Procedure, Coloma Data Protection Act, and Criminal Codes of the states of Aguascalientes, Sinaloa, Tabasco and Tamaulipas;

(b) On 30 April 2009, the Official Gazette of Mexico published the Decree adding section XXIX-O to article 73 of the Political Constitution of the United Mexican States, authorizing Congress to legislate on the protection of personal data in the possession of individuals;

(c) On 1 June 2009, the Decree was published adding a second paragraph to article 16 of the Constitution, recognizing that all individuals are entitled to protection of their personal data and the right to access, correct and delete such data, as well as to express their objection, in the manner established by the law, which establishes grounds for waiving the principles governing data processing for reasons of national security, law and order, public safety and health or to protect the rights of third parties;

(d) The Computer Security Incident Response Team of the National Autonomous University of Mexico deals with security problems in academia and provides support and technical advice to the Mexican authorities in dealing with cybercrime;

(e) There is a cyberpolice unit in the federal police force to follow up investigations on public security crimes;

(f) An executive report on cybervulnerability is being prepared by the Federal Government to inform senior government authorities about global cyberincidents in order to organize and support initiatives promoting cybersecurity in Mexico;

(g) It is planned to create a national CSIRT[1] within the Federal Government to coordinate efforts to combat cybercrime at home and abroad;

(h) Cybervulnerability is an item on the National Risk Agenda;

(i) There are programmes, coordinated by public and private bodies, to raise the awareness of the general public for the prevention of cybercrime;

(j) Mexico participates in various forums and has goodwill agreements with other countries on the subject of cybercrime.

Measures which the international community could take to strengthen global information security

4. The following are measures to strengthen global information security:

(a) Adoption of suitable legislation or updating of existing legislation as necessary for the protection of information in cyberspace;

(b) Training of judges in cybersecurity issues so that they can understand the nature of cybercrime and deliver appropriate sentences;

(c) Establishment of national Computer Security Incident Response Teams to coordinate efforts to deal with major security incidents and serve as contact points with other countries;

(d) Ongoing communication between national Computer Security Incident Response Teams so that they can coordinate their response in the event of a regional or global incident;

(e) Organization of forums for sharing experience and training security teams that are members of the international community;

(f) International arrangements for collaboration to combat cybercrime in order to facilitate investigations and form a united front.

Panama

[Original: Spanish]
[21 June 2010]

1. There are institutions in the Republic of Panama combating inappropriate use of the Internet for criminal purposes including terrorist acts, including the National Security Council and the Institute of Forensic Medicine and Science with its Department of Law and Order.

2. The National Security Council does intelligence work to combat organized crime, including terrorism, in connection with a possible attack on the property and integrity of the national territory.

[1] CSIRT Computer Security Incident Response Team.

3. The Institute of Forensic Medicine and Science has a Department of Law and Order, created by Act No. 69 of 27 December 2007, which investigates cybercrime.

4. Our Criminal Code criminalizes, suppresses and punishes use of the Internet for terrorist purposes. Article 289 states “Any person using the Internet to provide training for the commission of terrorist acts or to recruit others to commit such acts shall be punished by imprisonment for five to ten years.”

5. Other legal texts punish the use of the Internet for criminal purposes and provide criminal, civil and administrative penalties, governed by Act No. 14 of 18 May 2007, title VIII, chapter I (Computer security crimes), Act No. 51 of 22 July 2008 regulating electronic documents and electronic signatures and provision of services and include other provisions on the development of e-trade and Act No. 38 of 8 February 1996 enacting rules to govern telecommunications in the Republic of Panama.

Qatar

[Original: English]
[25 May 2010]

1. The State of Qatar is convinced that information and communication technology should be used in accordance with the Charter of the United Nations and the basic principles of international relations. Moreover, free flow of information must be guaranteed without prejudice to national sovereignty and while maintaining security and respect for cultural, political and moral differences among nations.

2. Efforts at the national level are based on the interest in security communications and to enhance it from time to time in order to keep up with its advancement at the national and international levels.

3. National efforts can be summarized as follows:

– Setting security strategies and policies and promulgation of laws to restrict the use of this technology for purposes that are not in accordance with the goals of the protection of the stability of security

– Establishing a mechanism to reinforce the security of information in order to guarantee the protection of the infrastructure of the sensitive information of Qatar

– The Office of Internet Security and Intelligence seeks to monitor government networks and the national network in order to address threats to the State of Qatar through the Internet

– Management of Internet incidents and coordinating efforts to resolve them aims to guarantee the resolution of Internet-related issues after reporting them, with minimum downtime. In the State of Qatar this is done by the Qatar Computer Emergency Response Team (Q-CERT)

– A more effective role for information and awareness to improve the level of technical skills and qualifications of employees in Qatari institutions

– Providing support to Qataris in dealing with Internet-related issues

– Follow-up on the latest advancements in the field of modern technological science related to the security and safety of the Internet, and ensuring the assessment of technical products, its security and services

– Advancing international relations in order to deal with Internet-related issues. The State of Qatar has participated in the Forum of Incident Response and Security Teams (FIRST) and the Meridian Process.

4. The most important measures that the international community can take to promote the security of information at the national level are the following:

– The United Nations should continue to lead the discussion and provide more clarification regarding the use of information and wired and wireless communication technology in electronic warfare, and whether existing principles of international law are sufficient to provide an appropriate framework to determine appropriate behaviour online regarding aggressive acts

– The establishment of an international ad hoc committee for the security of wired and wireless information and providing comprehensive studies related to this issue

– The State of Qatar encourages all Member States to create teams to address computer emergencies at the national level

– Contracting with specialized security institutions in the communication field

– Raising security awareness through symposiums and meetings at the local and international levels

– Encouraging States to cooperate in order to combat espionage and electronic piracy

– Usage of encrypted and secured equipment to transfer information and documents in a secured manner to ensure its confidentiality when it is exchanged

– Updating protection systems and convening regular workshops to take stock of the latest in science in the area of the advancement of information security.

Ukraine

[Original: Russian]
[12 May 2010]

Achievements in the use of information technology and telecommunications in the context of international security

1. The growing role of information technology in the various spheres of activity in society has led to concern for information security. As advanced information technology enters the everyday life of States and societies, the opportunities for cyberattacks against information and telecommunications systems, against the information resources of State bodies and against commercial entities on the part of criminal elements and individuals, seeking to commit criminal acts, have grown.

2. Half of all recorded computer crimes involve unauthorized access to computer information. Computer crime for profit is growing, as is the material damage it causes. The number of crimes committed by transnational hacker groups is also growing.

3. Computer crimes are rarely reported and efforts to determine the full extent of such crimes are usually frustrated, as the government and business entities that fall victim to such attacks always try to hide that fact, so as not to risk losing their authority, and they are reluctant to reveal the losses suffered and the weakness of their information protection systems. As a result, cases of such crimes are often not reported, which speaks to the need to develop concerted prophylactic and preventive measures, which should be at the core of information protection systems.

4. A computer crime is usually only the first step in a series of criminal acts, like the traditional types of crime, namely, theft, extortion, fraud and so forth. These crimes are constantly becoming more sophisticated and hidden and their execution improving, causing huge economic and political harm in practically all countries of the world. Furthermore, most experts see a direct link between the information sovereignty of States and matters of national security.

5. Efforts to combat crime in the field of information technology encounter many problems of a legal nature resulting from the non-material and frequently ephemeral nature of computer evidence. The complex issues involved in dealing with the problems encountered in cybercrime make international cooperation even more necessary. For that reason all countries must in the end establish appropriate and mutually compatible legal, procedural and normative tools.

6. In practice the investigation of computer crime has shown the imperative need for cooperation between the law enforcement agencies of States.

7. In international practice joint measures are usually taken to investigate computer crime. The Ukrainian Security Service participates actively in joint operations by law enforcement agencies and special services as part of efforts to combat child pornography, fraud perpetrated via the Internet and international terrorism.

8. Furthermore, there is a need to strengthen efforts aimed at further developing cooperation in the provision of information security, protecting shared interests and introducing steps for their protection, mainly in the form of bilateral and multilateral agreements. A successful solution to the problems of information security can be found only if there is effective cooperation between the government bodies of the various States, especially since the required legal basis is already in place.

9. Given the need to combat the threats of cybercrime and cyberterrorism, the Ukrainian Security Service maintains contacts with the law enforcement agencies and special services of foreign States.

10. It should be pointed out that cybercriminals often select as their targets networks established by government offices. Furthermore, the success of efforts to track down and punish criminals depends on the quality of the international links that are established and on the optimization of national legislation to meet current standards.

11. Bearing in mind the continuous global growth in computer crime, the existence of links between criminal hacker groups in various countries and the fact that

cyberthreats bear no relation to national borders, it is vital that international cooperation in the fight against cyberthreats be expanded.

12. With a view to implementing the decisions of the World Summit on the Information Society (first phase held in Geneva from 10 to 12 December 2003; second phase held in Tunis from 16 to 18 November 2005), Ukraine adopted an Act on basic principles for the development of the information society in Ukraine for 2007-2015. Its fundamental priorities are integration into the global information environment and development of the information society. The Act is intended to enable the latest information and communication technologies to be used in an atmosphere of better security.

13. In addition, a plan for the development of telecommunications in Ukraine has been drawn up and adopted. It provides for logistical and technical efforts to ensure the secure operation of all components of Ukraine's telecommunications infrastructure, including:

- establishing and introducing gradually a normative and legal basis to protect information, through technical means and encryption, ensuring harmonization with European and global standards;
- developing up-to-date information protection methods using technology to address comprehensively the task of protecting information in telecommunication networks;
- establishing systems to legally intercept information in telecommunication networks in the instances provided for by the law;
- establishing a State coordination centre for security in public information and telecommunication networks and helping to establish State and non-governmental centres to react and respond to incidents on those networks.

14. The normative and legal basis for information protection in Ukraine also includes Acts on the fundamental principles of national security; on information; on information protection and information and telecommunication systems; issuances of the President and Cabinet of Ministers on the technical protection of information in Ukraine; rules for the protection of information and telecommunication systems and networks and procedures for connection to global data-transmission networks. It also includes a large number of normative acts registered with the Ministry of Justice and having as their purpose to regulate connection of information systems to global data-transmission networks, licensing of particular types of activity and procedures for assessing information protection.

15. Normative and legal acts provide that the requisite protection of information should be achieved using only protected information and communication technology systems, in other words, those incorporating a comprehensive information protection system as a single body of legal and logistical measures, software and hardware, intended to counter threats. The comprehensive system, and its information-protection components, must be certified as compliant with information-protection standards.

16. In order to regulate the requirements for comprehensive information protection systems and their components, Ukraine has developed and introduced some 50 technical standards laying down criteria for the assessment of information protection, the classification of information and communication technology,

procedures for achieving information protection requirements for the individual components of a comprehensive information protection system depending on the variety of information and communication technology involved, the ultimate purpose, the field of use and the type of information processed.

17. Ukraine has also created its own national system of criteria for assessing the security of information technologies. The system is based on a set of regulatory instruments on protecting information in information and telecommunications systems from unauthorized access; these instruments have been harmonized with similar instruments of European Union countries and with international standards, in particular standard 15408 of the International Organization for Standardization/ International Electrotechnical Commission.

18. In addition, a national system of organizational and technical measures is being established in Ukraine with a view to preventing unauthorized acts against the information and telecommunications systems of the State authorities, law enforcement, customs and tax authorities, credit and financial institutions and others, in particular attempts to interfere with their work through the Internet.

19. As specified in article 16, paragraphs 10 and 11, of the Act on the State Service for Special Communications and Information Protection, and in order to improve coordination between State agencies for the detection of threats to information in information and telecommunications systems, to deal with the consequences of implementation of such threats and to organize international cooperation in such matters, the appropriate Computer Emergency Response Team (CERT-UA) has been created within the Service and is operational.

20. Reflecting the global trend towards networks of rapid reaction facilities, CERT responds to computer emergencies. International coordination of the activities of such facilities is provided by the international Forum for Incident Response Security Teams (FIRST), a forum for teams responding to security incidents.

21. On 13 July 2009, CERT-UA (www.cert.gov.ua) became a full member of FIRST.

22. Among its activities for 2009, CERT-UA processed 461 reports from CERTs in 30 countries (Australia, Austria, Belgium, Canada, China, Denmark, Finland, France, Estonia, Germany, Hungary, India, Israel, Italy, Japan, Korea, Lithuania, Malaysia, Netherlands, Norway, Pakistan, Poland, Portugal, Romania, Russian Federation, Saudi Arabia, Spain, Taiwan, Turkey, United States of America) of unauthorized acts in the Ukrainian segment of the Internet (distribution of harmful software, distributed denial-of-service (DDoS) attacks and other attempts to commit unauthorized acts).

23. It should be added that Ukraine has created a legal and regulatory framework and made efforts to ensure cooperation between the State Service for Special Communications and Information Protection and the law enforcement agencies with a view to implementing measures to safeguard the security of State information resources in information and telecommunications systems and improving the effectiveness of the system for responding to unauthorized acts against those information resources.

24. Thus, in Ukraine, information can now be protected at all stages of the establishment of information and telecommunications systems and the

comprehensive information protection systems within them, irrespective of the type and criticality of the information being processed and the type and complexity of the information and telecommunications system. Moreover, all the basic approaches to the elaboration of requirements, design, development, security assessment and protection of information resources in information and telecommunications systems as a whole correspond to the approaches employed by the State security services of the Member States of the United Nations and the member States of the European Union.

25. With a view to training specialists in the field of information security and computer engineering, an Institute for Information Protection has been set up as an academic and scientific department of the State University of Information and Communications Technologies.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[2 June 2010]

1. The United Kingdom is pleased to respond to General Assembly resolution 64/25, Developments in the field of information and telecommunications in the context of international security.

2. We consider this to be a most important topic, vital to individual nations, their commerce, the protection of their citizens and in the broader context of international security. The United Kingdom devotes considerable effort so as to make cyberspace a safer place for all nations and we welcome international activities in this sphere, as we believe that all nations should cooperate in promoting a safe and resilient environment in cyberspace.

General appreciation of the issues of information security

3. We believe that a secure cyberspace is vital to today's world. Citizens, commerce, critical national infrastructure and government are increasingly dependent on the Internet. Any event that adversely affects the Internet service within a nation is likely to have consequences for that nation, perhaps of a severe nature. It is an unfortunate fact that there is likely to be a number of threat actors, both external and internal to any nation, who may attempt to disrupt or manipulate the Internet service for any of a number of reasons.

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

4. The United Kingdom continues to work domestically and internationally so as to promote safer cyberspace. Domestically, we published our National Cyber Security Strategy in June 2009. This document underpins the national effort on information security. The Strategy calls for two new organizations, the Office of Cyber Security and the Cyber Security Operations Centre. The organizations have been established and continue to grow. There are three computer emergency response teams (CERTs) run by the United Kingdom government and which provide a specialist service to United Kingdom critical national infrastructure, military and other government networks. Internationally, we are also active in this work. Our

United Nations involvement includes membership of the Group of Governmental Experts. We co-sponsored the United Nations resolution on the creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures. We have membership of relevant International Telecommunication Union (ITU) bodies. We participate in activities of the Organization for Security and Cooperation in Europe. With our full support and participation, the European Union (EU) has begun work on several initiatives on the protection of critical national infrastructure in the EU. We participated in the EU engagement with the ASEAN Regional Forum work on cybersecurity. Similarly we participate in a number of activities within NATO as part of protecting that organization's networks. The United Kingdom has long been a leading nation within MERIDIAN (www.meridian2007.org), FIRST (Forum on Incident Response and Security Teams, www.first.org) and the EGC (European Government Certs Group, www.egc-group.org).

5. The United Kingdom National Cyber Security Strategy is available for download from the Cabinet Office web page at www.cabinetoffice.gov.uk.

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

6. We encourage all nations to establish national computer emergency response teams. We encourage all nations to enact effective domestic legislation on cybercrime. We believe that whereas e-crime is not the only malicious activity in cyberspace, it is the most prevalent, and that a reduction of criminal activity will benefit all. We believe that the Council of Europe Convention on Cybercrime represents a suitable instrument for combating international e-crime. Additionally, we believe that the toolkit developed by the ITU and promoted in the United Nations provides a good basis for nations to perform a self-assessment of their readiness to cope with potential attacks on critical national infrastructure. We welcome efforts within many forums to promote information security best practice.

Relevant international concepts

7. The primary international concept is that of international law. There is considerable debate, particularly at cyber conferences, about the applicability of existing international law to cyberspace. The United Kingdom has examined this issue, and our view is that the existing principles of international law, on both the use of force and the law of armed conflict, provide an appropriate framework within which to identify and analyse the use of cyberspace in the context of hostilities.