United Nations A/64/129

General Assembly

Distr.: General
8 July 2009
English
Original: English/Russian/Spanish

Sixty-fourth session
Item 90 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

Page

I. Introduction 2

II. Replies received from Governments 2

Brazil 2

Kazakhstan 4

Lebanon 7

Lithuania 7

Mexico 9

Serbia 9

Tajikistan 11

Thailand 11

Ukraine 13

[*] A/64/50.

I. Introduction

1. In paragraph 3 of its resolution 63/37, 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 27 February 2009, 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

Brazil

[Original: English]
[11 June 2009]

1. Information and telecommunications are an essential part of modern societies, which depend on them to a large extent. The strong reliance on the constant availability of such services is inherent in today's activities, turning them into extremely valuable resources, crucial for the wealth and prosperity of nations.

2. The technological advances which made this scenario a reality have also raised a number of issues in the context of international security. Given that societies are increasingly dependent on information availability and telecommunications infrastructure, new vulnerabilities have been created that can be exploited for use in military conflicts and in criminal and terrorist activities.

3. Such exploits could potentially undermine the activities of private companies, banks, stock markets and governmental organizations. The increasing interconnection between the underlying networks of communications, while undoubtedly beneficial, gives rise to a new range of concerns that States must address at national and international levels.

4. At the same time that the developments in information and telecommunications can lead to vulnerabilities, they also represent an asset to be used as cyberwarfare. There are already national armed forces with specialized military units trained and equipped to disable or even destroy critical infrastructure by means of invasion and sabotage of information networks. Depending on the objective and the means employed, the effects of such attacks may range from "soft kills" of enemy weapon or sensor systems to cataclysmic disruptions of nationwide power grids.

5. The efficiency of this form of warfare is increased by the fact that relatively small investments are required to develop many of those capabilities. In view of these factors, cyberwarfare may well become the stepping stone of military interstate conflicts in the near future. The same tactics may also come to be used by terrorist individuals or organizations.

6. Aware of the importance of this subject for the maintenance of international peace and security, Brazil suggests that the issue be approached in two different ways. First, the international community should strive to build appropriate tools for dealing with criminal and terrorist activities involving information technology. In a separate but complementary approach, it should consider the impact of the emergence of cyberwarfare and the potential need for disarmament and non-proliferation regimes and international law concerning war to take into account its manifold effects.

7. Criminal and terrorist activities should be properly discussed in the adequate forums and the United Nations should play a relevant role in assisting Member States, as required, towards the following goals, among others:

- Establishment of emergency and alternative networks to protect critical infrastructure;
- Examination of network structure, analysing the interdependencies, and identification of effective methods of protection;
- Close cooperation between Government and private sectors, aimed at reaching the desired level of security for the information that flows among organizations;
- Establishment of protection systems to avoid or minimize the effects of cyberattacks;
- Implementation of tools and measures to enable authorities to trace the origin of cyberattacks;
- Debate on the desirability and convenience of international legally binding instruments on cybercrimes;
- Qualification of national institutions to conduct testing and evaluation of the security level of information systems;
- Creation of procedures for the mutual notification of cyberthreats among competent national authorities;
- Avoidance of discriminatory mechanisms that could prevent countries from accessing high technology in the field of telecommunications and information systems;
- Education and awareness activities regarding the importance of cybersecurity.

8. The United Nations should also play a leading role in the discussions on the use of information and telecommunications as cyberwarfare in interstate conflict situations, paying special attention to the following aspects:

- Identification, characteristics and classification of information warfare;
- Identification and classification of information weapons and means that can be used as information weapons;

- Establishment of a code of conduct for the use of information weapons;
- Guarantee that all countries have equal rights regarding the protection of their homeland against cyberattacks;
- Creation of a United Nations glossary containing definitions of the main terms related to information and telecommunications in the context of international security.

Kazakhstan

[Original: Russian]
[2 July 2009]

1. The active development of information and communications technology is responsible for widespread changes in all spheres of life throughout the world. As stated in the Okinawa Charter on the Global Information Society: “Information and Communications Technology (IT) is one of the most potent forces in shaping the twenty-first century. Its revolutionary impact affects the way people live, learn and work and the way government interacts with civil society.”

2. The current era of increasing scientific and technological progress has seen a marked trend towards computerization and the creation of extensive data processing systems. The Internet impinges on almost all areas of public and social life and the number of its users continues to grow. Information resources, data processing systems and computer networks have therefore become the most vulnerable links in a State’s national infrastructure.

3. Criminal communities are seeking to take advantage of the potential of modern information and communications technology, given that the Internet still remains a virtually free and uncontrolled space. According to experts from the International Chamber of Commerce, the number of Internet-based crimes is increasing in proportion to the number of Internet users. According to the International Criminal Police Organization (INTERPOL), the Internet community has one of the fastest growing crime rates in the world.

4. These offences can be roughly divided into three categories:

(a) Universal, State and public offences, which represent a threat to national and public security (including calls to overthrow the existing order, attempts to devalue sovereignty or to undermine independence and national interests, terrorist propaganda, chauvinism, xenophobia, all forms of extremism, and discrimination on ethnic, racial, religious, gender and other grounds);

(b) Universal civil offences, which constitute a threat to individual rights and freedoms (including violations of individual rights and freedoms, the use of compromising material, the exertion of pressure on individuals, the discrediting of individuals, the dissemination of confidential information, the use of another person’s Internet services, the forgery of documents and copyright infringement);

(c) Traditional offences, which threaten the foundations of morality and decency (including pornography, paedophilia, other forms of sexual perversion, drug addiction and alcoholism).

5. The emergence of such information demonstrates that national legislation to regulate legal relationships arising from Internet use is inadequate and that a new supranational approach is required. At the international level, there is still no single regulatory approach for determining and assessing threats to international information security, nor are there any mechanisms in place for international cooperation to address such threats. At the same time, all of the international security concepts so far put forward by individual countries in the field of information technology lack universality.

6. This situation can be explained by the technological gap between the most and the least developed countries, latent political differences and conflicting ways of assessing developments and events in cyberspace, and a number of other factors.

7. The current international instruments of the United Nations and European organizations (such as the Organization for Security and Cooperation in Europe) mainly prioritize information technology threats from common crime and terrorism. However, they neglect the possibility that information technology advances may be misused as information weapons during armed conflicts to dominate the information space and to threaten national sovereignty and identity. Such instruments also ignore natural and man-made threats to national information infrastructures.

8. A key element for protection from such threats could be provided not only by international information security arrangements with military and political partners, but also by political and legal agreements on the mutual non-use of information as a weapon, joint mechanisms to minimize the negative consequences of an injurious act and to rehabilitate national information infrastructures and other measures.

9. It should be noted that representatives of the Republic of Kazakhstan are involved in similar efforts already under way within the framework of the Collective Security Treaty Organization (CSTO) and the Shanghai Cooperation Organization (SCO), where experts are working on the possibility of concluding relevant intergovernmental agreements. In particular, pursuant to the SCO plan of action to ensure international information security, adopted in Bishkek by a decision of the Council of Heads of SCO member States dated 16 August 2007, a group of international information security experts from SCO member States drew up a draft intergovernmental agreement on cooperation to ensure international information security. This agreement was signed in Yekaterinburg on 15 June 2009 during a meeting of the Council of Heads of SCO member States.

10. It should be pointed out that this agreement is without parallel anywhere in the world and that its signature will be of international significance, in view of the possibility that other States will to accede to it.

11. In addition, within the framework of CSTO, an interim working group on information policy and security reports to the Organization’s Committee of Secretaries of Security Councils. The group has developed a programme of joint activities in order to establish an information security system for CSTO member States.

12. CSTO member States conducted joint preventive exercises as part of the “Proksi” operation, which was based on a unified plan for cooperative activities among the security and internal affairs (police) agencies.

13. In view of the scale and transboundary nature of the Internet, we propose that Member States of the United Nations should prepare and adopt an international convention on information security. One of the main pillars of such a convention should be efforts to combat Internet-based crime.

14. This instrument should seek to promote mutually beneficial international cooperation in the area of information security and to prevent the emergence of negative geopolitical consequences from global information and communications systems.

15. The convention also needs to establish organizational, technical, policy and social mechanisms for the receipt and use of information, with a view to protecting the constitutional system, sovereignty and territorial integrity of all United Nations Member States, as well as ensuring political, economic and social stability, law and order and the rule of law. It must also include mechanisms enabling the exercise of constitutional, human and civil rights.

16. At the national level, the Republic of Kazakhstan has developed a draft law amending and supplementing certain of its legislative acts on information and communications networks. This draft law is currently under consideration by the Senate.

17. This draft law proposes to strengthen standards governing the dissemination of information in the Republic of Kazakhstan via information and communication networks.

18. The main national efforts to increase information security and to facilitate international cooperation in this area are being undertaken by national security agencies. Activities to identify and prevent international computer crimes are carried out on an ongoing basis.

19. For example, in 2008 the National Security Committee and the Federal Security Service of the Russian Federation put an end to the activities of hackers from a transnational organized criminal group that had been extorting large amounts of money from companies doing business online by threatening their websites with "distributed denial-of-service attacks".

20. The preventive exercises carried out in the area of information security demonstrate that new forms of Internet-based crime have emerged, such as extortion, blackmail, human trafficking, pimping and the dissemination of materials promoting pornography, cruelty and violence, and terrorism and extremism.

21. For example, 45 cases of the distribution of pornography were identified in 2008. The increased availability of child pornography on the Internet should also be noted: one case of the distribution of child pornography was identified in 2005-2006; 7 cases were identified in 2007; and 14 cases were identified in 2008, including two from the Kazakh Internet community.

22. It must also be noted that efforts to combat information security and high-technology crimes are inadequate due to the lack of a clear legislative framework for information security issues.

23. Existing regulatory and legal acts in this sphere need to be further improved by taking current realities into account.

24. In our view, drawing on the experience of advanced countries, it would be appropriate to update existing criminal legislation in order to increase the punitive measures imposed for this category of crimes.

25. Furthermore, bearing in mind the transborder nature of computer crimes, law enforcement agencies need to continually expand their area of operational coordination in order to ensure a rapid response to Internet attacks. The results of cooperation between Kazakh law enforcement agencies and the special services and law enforcement bodies of other countries point to an increased level of computer attacks from the Kazakh Internet community. At the same time, victims of Internet attacks have difficulty responding promptly when transmitting information about attacks, since the Republic's relevant State bodies do not have an official service responsible for receiving and transferring information on computer incidents, such as the Internet information security centres in other countries (commonly known as computer emergency response teams).

26. In this connection, we believe that law enforcement agencies need to establish selected specialized units to identify, suppress and detect information security-related crimes. Such units should be equipped with advanced tools to combat these types of crimes.

27. Kazakhstan has also submitted its nominations for the group of governmental experts to be established in accordance with paragraph 4 of General Assembly resolution 63/37, entitled "Developments in the field of information and telecommunications in the context of international security".

Lebanon

[Original: English]
[22 May 2009]

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 all related matters including security and all the matters related to information crimes.

2. Once the law mentioned above enters into force, the Ministry of Telecommunications will arrange for the matters concerning (b), (c) and (d) [of paragraph 3 of resolution 63/37] with other Ministries and all Administrations concerned.

Lithuania

[Original: English]
[26 May 2009]

1. Lithuania attaches great importance to the issue of information security both on its national and international agenda. The issue of cybersecurity is an important element of national security.

2. Cooperation on international level is of great importance in order to enhance the protection of communication and information systems as well as raise the awareness. Lithuania welcomes the fact that the issue of information security is

gaining greater attention on the agendas of international organizations such as the United Nations, the European Union, the North Atlantic Treaty Organization (NATO), the Organization for Security and Cooperation in Europe and participates actively in their work to address this issue. Lithuanian institutions cooperate closely with their partners. Lithuania is a party to the Council of Europe Convention on Cybercrime since 1 July 2004.

3. Lithuania is one of seven NATO members who sponsored the establishment of the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia which received a status of NATO Centre of Excellence on 14 May 2008.

4. The "Safer Internet plus" — a multi-annual community programme on promoting safer use of the Internet and new online technologies was adopted by the Decision of the European Parliament and of the Council on 11 March 2005. The main tasks are education of the society on the issues of the safer Internet and hotline implementation.

5. During the General Assembly of INHOPE on 28 and 29 May 2008, in Dublin, the Lithuanian hotline became the member of INHOPE.

6. At the national level, in 2000, the first evaluation of the condition of the information infrastructure took place and marked the beginning of the complex involvement to address this issue. Among the main areas of evaluation were the level of the comprehension on the issue of information security, existing policy and the level of cyberprotection of the State institutions.

7. The Ministry of the Interior of the Republic of Lithuania was assigned the role of coordinator of the security of information technologies in the State institutions by the resolution of the Government of the Republic of Lithuania (No. 291, 14 March 2001).

8. A number of measures were developed and implemented with the aim to safeguard the information security, as it was set in State Information Technology Security Strategy (until 2004) and State Strategy on the Electronic Information Security at the State Institutions until 2008.

9. The inter-institutional working group for cybersecurity issues was established by a decree of the Prime Minister of Lithuania on 17 June 2008. On 21 November 2008, the working group submitted a report for the Government with proposals and recommendations for improving cybersecurity in Lithuania.

10. The Government of Lithuania is planning to prepare in the near future the draft of the Law on Electronic Communication Networks and Information Security and the new Electronic Information Security Strategy with the aim to further improve State capabilities in the field of information security and cyberdefence in particular. Among the objectives of the aforementioned strategy are the efficiency of institutional structure as the framework to defend against cyberattacks, security and resiliency of data transfer infrastructure, effective prevention of critical information infrastructure against cyberthreats, high level of compliance with policies and requirements through second- and third-party audit policy.

11. Since 2005 the Communications Regulatory Authority of Lithuania has carried out surveys on electronic communications networks and information security with the aim to flush out outstanding issues. The Communications Regulatory Authority carries out national computer emergency response team functions.

12. Lithuanian national computer emergency response team, CERT-LT, is tasked to promote security in the information society by preventing, observing, and solving information security incidents and disseminating information on threats to information security. The new website www.cert.lt was opened on 30 September 2008. On 16 January 2009 CERT-LT became an accredited member of the Trusted Introducer — the trust network for computer security incident response team and computer emergency response teams in Europe.

13. Lithuania seeks to ensure that international attention to the issue of information security remains high and the efforts to address this issue increase. Lithuania strives to participate actively in, and contribute to, the future work of the international community to achieve greater information security.

Mexico

[Original: Spanish]
[8 June 2009]

1. The main perceptions regarding security issues relate to the possible vulnerability of the information systems that regulate countries' defence systems and the risk of information technology and telecommunications being used by terrorists for violent or dissuasive purposes.

2. In this context, concerned by the development of telecommunication security in the world, Mexico attended the World Telecommunication Standardization Assembly, which was held in South Africa in October 2008 and, together with other members (Canada, Paraguay and Uruguay) of the Inter-American Telecommunication Commission (CITEL), it submitted a draft resolution inviting universities to participate actively in the meetings of the International Telecommunication Union so as to strengthen its work.

3. Moreover, in the regional sphere, Mexico acted as Vice Chairman of the twentieth meeting of the Permanent Executive Committee of CITEL, during which it offered States of the region a course, through the federal telecommunication committee, on the question of harmful interference with satellite systems. The States agreed to hold the V Regular Assembly of CITEL in Mexico during the first quarter of 2010.

4. Mexico has taken a number of measures to strengthen international security in the field of information and communication; inter alia it has a cyberpolice unit which, in addition to preventive actions relating to crimes committed via the Internet and other IT tools, has a specific focus on preventing and dealing with reports of crimes against minors.

Serbia

[Original: English]
[9 June 2009]

1. There is a need for States to consolidate their legal norms in the field of cyberspace as it is no longer limited to the territory of one country and the individuals and/or groups engaged in the destabilization and/or unauthorized use of

the information and telecommunications systems may not often be in the country in which an accident occurs. The resolution is an initial step and a solid basis for a balanced recommendations-based approach to the consolidation of legislations at the international level, aimed at strengthening international security, on the one hand, and ensuring a free flow of information, on the other.

2. Tougher laws are needed, primarily at the State level, which must conform to users technical skills and level of education and be buttressed by continued user education and the establishment of specialized agencies that would plan, organize and control the technical aspect of this field.

3. In assessing the respect of the principle of information security in the field of information and telecommunications systems, the following has been established:

Problems

- Daily generation of new types of malicious programmes that threaten the security of information and telecommunications systems
- Numerous attempts to hack the official Internet sites of the Ministry of Defence and the Armed Forces of the Republic of Serbia
- Promotion of terrorist ideas on the Internet

Security procedures and cooperation

- Application of appropriate anti-virus software at all levels of the use of information and telecommunications systems in the Ministry of Defence and the Armed Forces of the Republic of Serbia
- Continued protection against hackers raids of the official Internet sites of the Ministry of Defence and the Armed Forces of the Republic of Serbia
- Participation in conferences and seminars aimed at raising awareness of the danger of cybercrime and cyberterrorism.

Recommendations

Establish an international agency, charged with:

– Assessing problems in data and telecommunication channels protection

– Monitoring the “threat” factors in the field of international cyberterrorism and cybercrime

– Assessing problems of international security in the field of information and telecommunications systems and recommending solutions

– Designing education programmes, aimed at raising awareness of the danger of cybercrime and cyberterrorism

– Organizing knowledge and experience exchanges at intergovernmental levels

Tajikistan

[Original: English]
[20 May 2009]

1. Nowadays, the telecommunications sphere is considered to be a very important factor for development of the economy as well as for stabilization and security of any State.

2. Tajikistan has provided all the necessary conditions for the development of the telecommunication sphere thanks to the existing free competition and licensing of alternative operators and providers of services, and by introducing new services.

3. It is essential to pay attention to ensuring security of functioning of information and telecommunication infrastructures, to increasing the level of protection of the corporate informative systems, and through this, to counteract spreading of the ideology of terrorism, extremism and violence.

4. Tajikistan is prepared to support the above initiative and to collaborate in the sphere of development of international information safety.

Thailand

[Original: English]
[3 June 2009]

General appreciation of the issues of information security

1. The world has now entered the information society age, in which information technology is used to make life more convenient, for instance, in financial transactions and in the exchange of news and information. Nonetheless, not only does information technology provide benefits, but it also provides opportunities for its illegal and immoral use by certain groups thereby giving rise to problems such as stealing information through the information system, cyberattacks, the forging of electronic documents, infiltration of government databases to steal personal data, and violation of privacy. Nevertheless, information and communications technology (ICT) is needed for the economic development of each country. The increased complexity of technology, the shortage of well-trained personnel on information security, and the lack of sufficient resources can lead to a reduction of information security of computer systems and networks, which can lead to the loss of people’s trust, especially in areas of banking, e-commerce, and administration. It is thus necessary to identify and forecast the problems involved in order to establish safeguards and security measures against these risks. To achieve this, countries should cooperate in establishing information security measures in order to set an international standard for all countries to abide by.

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

2. The Royal Thai Government has set national security policy as one priority policy area within the Government strategic plan for the years B.E. 2552-2554

(2009-2011). Currently, the Government has legal measures in place to promote information security so that information networks are not used immorally and do not affect national security. Such measures include laws on computer crime, on electronic transactions, on electronic signatures, and on electronic money transfers.

3. The Ministry of Information and Communications Technology has placed great importance on ensuring information security on Internet networks, on resolving the issue of inappropriate and illegal websites, and has set up an Internet security operation centre with the purpose of monitoring information technology threats as well as coordinating with other agencies to tackle the use of information networks as a threat to national security. The Centre also aims to end the illegal use of information networks and to set up a system for monitoring viruses and junk e-mails.

4. With regard to international cooperation, a coordinating body should be established as the focal point. The body should set policies to prevent and combat inappropriate information, measures to tackle information security threats and preventive measures as a guideline for joint actions.

Examination of relevant international concepts aimed at strengthening the security of global information and telecommunications systems

5. Shared international concepts and principles to promote global information security is a necessity as the cyberworld today is interconnected and borderless. Therefore, the problem of information security that arises in one country can spill over and affect another country.

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

6. Possible measures the international community could take are the exchange of information, the exchange of preventive measures, and the exchange of measures to combat threats to information security. There should also be greater cooperation in developing the information technology capacity of various countries to be at an equal level, especially the transfer of technology and know-how of developed countries to lesser developed ones to help build the latter’s capacity. Training programmes should also be set up covering issues of awareness, prevention, detection, management and response to minimize risks and threats to information security.

7. Furthermore, it is necessary to create a coordinating mechanism to interconnect the work of various agencies concerned to set the direction and policy regarding national information security to be at a certain standard and to move in the same direction.

8. Efforts by some international agencies to promote international cooperation in strengthening information security should be encouraged, namely the International Telecommunication Union (ITU). The ITU has organized an international conference to exchange experiences and explore measures to resolve the problems arising from the misuse of information technology. Study groups have also been set up to find measures to strengthen information security, the results of which Governments and agencies concerned can apply and use.

9. Computer emergency response teams should also be set up in each country with the assistance of countries that have experienced success in establishing these teams.

10. The protection of critical infrastructure of each country from cyberattacks and the rapid assistance or cooperation among the international community should be addressed and measures on how to solve or minimize such risks jointly explored.

11. Greater awareness of the issue of information security at the United Nations should be encouraged with, perhaps, discussion on the possible rules and regulations regarding information warfare and the issuance of annual reports on the threats and vulnerabilities of information security.

Ukraine

[Original: Russian]
[20 May 2009]

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 getting 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. In cooperation with the national police of the Kingdom of the Netherlands and the Federal Security Service of Russia we carried out a coordinated operation at the end of 2008 to stop the illegal activities of an international criminal hackers group that was stealing funds from clients of various finance and credit institutions by interfering in their automated systems without authorization.

12. Bearing in mind the continuous global growth in computer crime, the existence of links between criminal hackers 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.

13. Pursuant to the international Convention on Cybercrime, a fully viable and convenient mechanism has been set up in the form of a 24/7 network with national points of contact spanning the countries of the Group of Eight and other States covered by the Convention.

14. In accordance with the Decision of the President of Ukraine regarding the establishment within the National Security Service of a 24/7 point of contact, an interdepartmental working group composed of staff from the National Security Service, the Ministry of Internal Affairs, the Office of the Public Prosecutor and the Ministry of Justice is developing a bill regarding amendments to the Act ratifying the Convention on Cybercrime, a bill regarding amendments to the Telecommunications Act and a bill regarding the structure and overall staffing of the National Security Service, as well as a Presidential Decree on the organization of the functions of the 24/7 point of contact.

15. As part of the process of implementing the Decision of the President, the National Security Service is currently taking steps to register the point of contact within the international network.

16. The work accomplished to date should leave the contact point better placed to deal effectively and efficiently with exchange of information and cooperation against cybercrime on a worldwide scale.

17. 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.

18. 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.

19. 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.

20. 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 legislative 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.

21. In order to regulate the requirements for comprehensive information protection systems and their components, Ukraine has developed and introduced some fifty 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.

22. 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 (ISO/IEC 15408).

23. 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.

24. The international community has responded to such acts by establishing an advanced and widespread system for rapid response to incidents that endanger the security of information resources: computer emergency response teams. The international organization known as the Forum for Incident Response and Security Teams coordinates the actions of such teams at the international level.

25. With a view to establishing a legal and regulatory basis for such activities, the management of the Ukrainian State Service for Special Communications and Information Protection issued Order No. 94 of 10 June 2008 approving the procedure for coordination between central and local government, military units, companies, institutions and organizations, irrespective of their form of ownership, with regard to preventing, detecting and dealing with the consequences of unauthorized acts against State information resources in information and telecommunications systems.

26. In implementation of this Order, a related website and e-mail address have been set up (www.cert.gov.ua).

27. Drawing on international experience in ensuring the security of information resources, Ukraine is taking steps to establish, within the State Service for Special Communications and Information Protection, a post of national coordinator for the prevention of violations of information security in information and telecommunications systems (computer emergency response team of Ukraine (CERT-UA)), the holder of which will be accredited with the Forum for Incident Response and Security Teams. In that connection, a meeting was held on 17 March 2009 between management representatives of the State Service for Special Communications and Information Protection and a senior adviser on information security from the Finnish Communications Regulatory Authority.

28. During the period 2006-2008, Ukraine received more than 200 reports from the computer emergency response teams of Finland, Australia, Austria, Slovenia and other States of unauthorized acts on the Internet by Ukrainian users, even though CERT-UA was not at the time accredited with the Forum for Incident Response and Security Teams. As a result of these acts, more than 250 e-mails were sent to the

relevant Internet providers with the aim of locating the sources of the harmful software and viruses. In addition, in May 2007 steps were taken to prevent distributed denial-of-service (DDoS) attacks on Estonian servers from sources in Ukraine, and in October 2007 a DDoS attack on the website of the President of Ukraine was averted.

29. 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.

30. 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.

31. 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.