United Nations A/67/167*

General Assembly

Distr.: General
23 July 2012
English
Original: English/Russian/Spanish

Sixty-seventh session
Item 90 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

* Reissued for technical reasons on 8 April 2013.
** A/67/150.

12-43414* (E) 060812 090413

I. Introduction

1. By paragraph 3 of its resolution 66/24, the General Assembly invited all Member States, taking into account the assessments and recommendations contained in the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201), 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 that 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 16 February 2012, 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

Colombia

[Original: Spanish]
[21 May 2012]

The use of information and communications technology has undoubtedly brought about significant changes and benefits to our countries. Nevertheless, these technological advances have also increased the use of technology for criminal purposes around the world, which highlights the need to adopt urgent measures and controls that can protect the State from these new threats.

Increased criminal capacity in cyberspace and the use of new technologies to generate computer threats are common concerns for all countries, given that they have a significant impact on information security, in both the public and private spheres, including civil society, highlighting the need to implement the necessary security protocols and policies strictly in order to establish controls that can protect the State and its critical infrastructure from these new threats.

In this context, in 2005 Colombia developed the ISO/IEC 27001 standard, conceived as a management system covering the policies, organizational structure, procedures, processes and resources needed to implement information security management. The aim is to implement quality standards such as the code of best practices and control objectives contained in ISO/IEC 17799, which focuses on safeguarding confidentiality, integrity and availability, as defined below:

- Confidentiality: preventing information from being used by unauthorized individuals or processes.

- Integrity: safeguarding the accuracy and completeness of anything of value to an organization.
- Availability: ensuring that information is accessible and usable on demand by authorized entities.

The benefits of ISO/IEC 27001 can be seen in:

(a) The establishment of a clear and well-structured information security management methodology;

(b) The reduced risk of information being lost or stolen;

(c) Secure access to information by users;

(d) The review of risks to information and the respective security controls on an ongoing basis;

(e) The ability to run external and internal audits that can identify potential weaknesses in information security systems;

(f) Guaranteed compliance with existing legislation and regulations regarding information management;

(g) People have increased awareness of information security matters.

In an effort to enhance legal and operational frameworks for information security, on 5 January 2009, the Congress of the Republic of Colombia enacted Act No. 1273 which amended the Criminal Code, created a new legally protected interest, namely information and data protection, and ensured the comprehensive protection of systems that use information and communication technologies, among other provisions.

This important Act is divided into two chapters concerning “attacks on the confidentiality, integrity and availability of data and computer systems” and “computer attacks and other offences”.

The first chapter states the following:

- Wrongful access to a computer system: Any person who, without authorization or exceeding the authorization granted, accesses all or part of a computer system, whether protected by a security measure or not, or remains within the aforementioned system against the wishes of anyone who has the legitimate right to forbid it, shall be liable to a term of imprisonment of between forty-eight (48) and ninety-six (96) months and a fine of between 100 and 1,000 times the current minimum statutory monthly wage.
- Illegitimate obstruction of computer systems or telecommunications networks: Anyone who, without being authorized to do so, prevents or hinders the normal functioning of or access to a computer system, computer data contained therein or a telecommunications network, shall be liable to a term of imprisonment of between forty-eight (48) and ninety-six (96) months and a fine of between 100 and 1,000 times the current minimum statutory monthly wage, provided that the action does not constitute an offence punishable by a heavier penalty.
- Computer data interception: Anyone who, without a prior court order, intercepts computer data at its point of origin, destination or within a computer

system, or the electromagnetic emissions from a computer system that transmits them, shall be liable to a term of imprisonment of between thirty-six (36) and seventy-two (72) months.

- Computer damage: Anyone who, without being authorized to do so, destroys, damages, erases, spoils, alters or deletes computer data, or a data processing system or its parts or logical components, shall be liable to a term of imprisonment of between forty-eight (48) and ninety-six (96) months and a fine of between 100 and 1,000 times the current minimum statutory monthly wage.
- Malicious software use: Anyone who, without being authorized to do so, produces, traffics, acquires, distributes, sells or sends, or brings into or takes out of the country, malicious software or other harmful computer programmes, shall be liable to a term of imprisonment of between forty-eight (48) and ninety-six (96) months and a fine of between 100 and 1,000 times the current minimum statutory monthly wage.
- Violation of personal data: Anyone who, without being authorized to do so, for their own benefit or that of a third party, obtains, compiles, extracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies or uses personal codes, personal data contained in files, archives, databases or similar mediums, shall be liable to a term of imprisonment of between forty-eight (48) and ninety-six (96) months and a fine of between 100 and 1,000 times the current minimum statutory monthly wage.
- Website forgery in order to capture personal data: Anyone who, with criminal intent and without authorization to do so, designs, develops, traffics, sells, executes, programmes or sends web pages, links or pop-ups, shall be liable to a term of imprisonment of between forty-eight (48) and ninety-six (96) months and a fine of between 100 and 1,000 times the current minimum statutory monthly wage, provided that the action does not constitute an offence punishable by a heavier penalty.

The second chapter stipulates the following:

- Theft using computers or similar means: Anyone who, having bypassed computer security measures, engages in the conduct set out in article 239 on manipulating a computer system, an electronic, telematic or other similar network, or impersonating a user for established authentification and authorization systems, shall be liable to the penalties prescribed in article 240 of the Criminal Code, namely, terms of imprisonment of between three (3) and eight (8) years.
- Transfer of assets without consent: Anyone who, for profit and using a computer or similar device, makes a transfer without consent of any asset to the detriment of a third party, provided that the action does not constitute an offence punishable by a heavier penalty, shall be liable to a term of imprisonment of between forty-eight (48) and one hundred and twenty (120) months and a fine of between 200 and 1,500 times the current minimum statutory monthly wage. The same penalty shall be imposed on anyone who programmes, downloads, possesses or provides computer software for the purpose of committing the crime described above, or fraud.

Act No. 1273 of 2009 was, undoubtedly, a highly significant step forward in combating computer-related crime in Colombia; nevertheless the development of different types and modes of organized crime, and cybercrime in particular, has forced Colombia to implement a comprehensive strategy to combat cybercrime with a focus on cyberdefence and cybersecurity that has made inter-agency work the predominant factor in achieving the objectives pursued by the concept of information security.

In this framework, in July 2011, the Colombian Government launched its national cyberdefence and cybersecurity policy based on three fundamental pillars:

- Adopting an appropriate inter-institutional framework for prevention, coordination and monitoring and the formulation of recommendations to address any threats and risks that arise.
- Providing specialized training on information security and broadening cyberdefence and cybersecurity lines of investigation.
- Strengthening legislation on those matters and international cooperation, and accelerating Colombia's accession to the various international instruments.

In order to implement the aforementioned strategic principles comprehensively, Colombia designed and established four authorities:

(a) First is the Intersectoral Commission, responsible for formulating the strategic vision of information management and setting policy guidelines for the management of public information technology infrastructure, cybersecurity and cyberdefence;

(b) The second body is the Colombian Computer Emergency Response Team (CERT), the national coordinating agency on matters of cybersecurity and cyberdefence;

(c) Third is the Armed Forces Joint Cyber Command, which is tasked with preventing and countering any cyber threat or attack that affects national values and interests;

(d) Lastly, the Cyber Police Centre was established; it is responsible for Colombia's cybersecurity, offering information, support and protection from cybercrime.

These institutions will allow Colombia to fulfil and implement the national cyberdefence and cybersecurity policy and to address comprehensively and effectively this new type of crime that is growing exponentially around the world.

Not only has Colombia developed a cyberdefence and cybersecurity policy; but it has also undertaken a number of important sectoral initiatives to formulate effective information security policies. The most important of these are detailed below:

Initiative	*Leading agency*	*Scope*
Information security model for the Government Online strategy	Government Online Programme-Ministry of Information Technology and Communications	This security model refers to the set of strategic policies that form the basis for the Government Online objectives, such as “Protection of individuals’ information” and “credibility of and confidence in Government Online”. It establishes the following as key elements of information security for government agencies: (a) the availability of information and services; (b) the integrity of information and data; and (c) the confidentiality of information.
Recommendations made to the Government for the implementation of a national cybersecurity strategy	Telecommunications Regulatory Commission	In this document, the Communications Regulatory Commission gives the Government recommendations on a national cybersecurity strategy and proposes suitable instruments for collaboration and cooperation between the Government and all levels of the private sector; identifies ways to deter cybercrime; recommends the implementation and development of legal frameworks concerning cybersecurity that are consistent with international standards; makes recommendations for the development of systems to address network security incidents, including monitoring, analysis and responses to those incidents; and proposes guidelines for the implementation of a national cybersecurity culture to improve levels of protection of critical information infrastructure in Colombia.
Colombian Computer Security Coordination Centre for Internet service providers	Colombian Information Technology and Telecommunications Association	The Colombian Computer Security Coordination Centre is in direct contact with the security centres of its affiliates (the largest Internet service providers in Colombia). It is able to coordinate the handling and resolution of requests and reports concerning computer security problems.

Leaving national information security capacities to one side, it is important to mention a series of measures that, in Colombia's view, should be taken at the international level to strengthen information security.

- Strengthen communication channels between United Nations Member States in order to coordinate efforts in the transnational fight against crimes that affect information and data.
- Formulate international and regional instruments focused on the legal definition of punishable acts that threaten cybersecurity and cyberdefence in each State.
- Formulate and codify protocols to address computer incidents, leading to global policies on information security.
- Strengthen preventative and legislative activities in relation to "hacktivist" groups, particularly at universities and colleges, in order to reduce young people's involvement in these organizations that threaten the normal development of States' digital infrastructure.
- Standardize legislation with emphasis on prevention, assistance and follow-up of activities relating to information security.
- Consolidate and implement technology, with a focus on the adoption of best practices in information security management. It is important to note here that plans for investment in cutting-edge technology must be in place, together with Government support for technology development projects.
- Provide opportunities for the exchange of information and knowledge regarding the universal standards on the matter.

Legislation of the Republic of Colombia on information security

Act/Resolution	*Subject*
Act No. 527 (1999) (e-Commerce)	Defines and regulates access to and use of data messages, e-commerce and digital signatures, establishes certification authorities and contains other provisions.
Act No. 599 (2000)	Promulgates the Criminal Code, which maintains the framework of the criminal offence of "unlawful violation of communications", establishes the legal right of copyright and includes some acts indirectly related to computer crime, such as the offer, sale or purchase of devices capable of intercepting private communications between persons. It defines wrongful access to a computer system (article 195), whereby any person who wrongfully gains entry to a computer system protected by security measures or remains within the aforementioned system against the wishes of anyone who has the legitimate right to forbid it, shall be liable to a fine.
Act No. 962 (2005)	Enacts provisions to streamline the administrative procedures of State agencies and entities and of individuals who perform public functions or deliver public services. It provides for an incentive for members of the public to use integrated technology in order to reduce the waiting times and costs of administrative formalities.

Act/Resolution	*Subject*
Act No. 1150 (2007)	Introduces measures to enhance the efficiency and transparency of Act No. 80 (1993) and enacts other general provisions on public procurement. It specifically establishes the possibility of the public administration issuing administrative acts and documents and giving notifications electronically, to which end it envisages the development of an electronic public procurement system.
Act No. 1273 (2009)	Amends the Criminal Code, creates a new legally protected interest, namely “information and data protection”, and ensures the comprehensive protection of systems that use information and communications technologies, among other provisions.
Act No. 1341 (2009)	Defines principles and concepts of the information society and the information and communications technology framework, establishes the National Radiocommunications Agency and contains other provisions.
Resolution No. 2258 (2009) of the Communications Regulatory Commission	Concerns the network security of network and telecommunications service providers. This resolution amends articles 22 and 23 of Resolution No. 1732 (2007) of the Communications Regulatory Commission and articles 1.8 and 2.4 of its Resolution No. 1740 (2007). This regulation establishes the requirement that network and/or telecommunications service providers that offer Internet access must use security models, in accordance with the specific characteristics and needs of their network, that help to improve the security of access to their networks, in line with the security frameworks defined by the International Telecommunication Union, adhering to the principles of data confidentiality, data integrity and availability of network elements, information, services and applications, as well as authentication, access and non-repudiation measures. It also establishes requirements to be met by network and telecommunications service providers concerning the inviolability of communications and information security.
Circular No. 052 (2007) (Superintendence of Finance of Colombia)	Sets minimum security and quality requirements for handling information via media and distribution channels of products and services for clients and users.

Cuba

[Original: Spanish]
[21 May 2012]

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, which can give rise to tensions and situations that are not conducive to international peace and security.

Cuba fully shares the concern expressed in General Assembly resolution 66/24 with respect to the use of information technologies and means for purposes inconsistent with international stability and security and which adversely affect the

integrity of States, to the detriment of their security in the civilian and military fields. This resolution also appropriately stresses the need to prevent the use of information resources and technologies for criminal or terrorist purposes.

In this regard, Cuba reiterates its condemnation of the aggressive escalation by successive United States administrations of their radio and television war against Cuba which violates the international rules in force governing the radio-electric spectrum. That aggression is being perpetrated without considering the damage that could be caused 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.

During 2011, an average of 2,193 hours of illegal transmissions against Cuba were broadcast on 30 frequencies from the United States 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, broadcasting programmes that include incitement to sabotage, political attacks and assassination, among other topics of radioterrorism.

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

- The fundamental principles of the International Telecommunication Union, as set out in the preamble to its constitution. 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, whatever their purpose, 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 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”.
- 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.
- 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 Radio Regulations Board, which at its 35th meeting in December 2004 established that United States transmissions 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 50th meeting of the Board, which ended on 20 March 2009 (document RRB09-1/5), it was once again stated that the transmissions were illegal and the United States

Government was requested to take all necessary steps with a view to eliminating those two cases of interference with television services in Cuba.

- Radio Regulation 23.3, limiting television broadcasting outside national frontiers. A report issued in January 2009 by the General Accounting Office 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 World Radiocommunication Conference, which met in Geneva in 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 have legal standing in the work of the International Telecommunication Union. 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.

At its 54th meeting, held in July 2010, the Radio Regulations Board of the International Telecommunication Union adopted the following decision:

> After carefully considering the report of the Director and the submission from Cuba (document RRB10-2/3 (Add.1)), the Board noted with regret that interference to the broadcasting stations of Cuba by the transmissions from the United States is continuing, and decided to maintain its previous decisions in this matter.
>
> The Board also noted the request to the "Bureau, in its capacity as Executive Secretary of the Board" to raise the issue of harmful interference to the VHF/UHF broadcasting stations of Cuba at the forthcoming Plenipotentiary Conference. Recognizing the sovereign right of every Administration to raise any issue at the Plenipotentiary Conference, the Board confirmed that the two representatives of the Radio Regulations Board at the 2010 Plenipotentiary Conference and its Executive Secretary will be ready to provide any relevant information and advice that might be required at the forthcoming Plenipotentiary Conference.

More recently, in February 2012, the World Radiocommunication Conference conferred a mandate on the Director of the Radiocommunication Bureau of the International Telecommunication Union to follow up and report at the next Conference, to be held in 2015, on the interference that the United States is causing to Cuban radio and television services through its acts of radio-electric aggression.

The Conference thus confirmed the validity of the conclusion adopted at its previous meeting, which recognized the illegality of the United States Government transmitting anti-Cuban radio and television broadcasts using aircraft.

The hostility of the United States Government towards Cuba has been manifested through the economic, financial and trade embargo imposed for over fifty years, which also affects information and telecommunications:

- The information and communications technology sector has been hit hard by the embargo. From 2010 to 2011, total losses were calculated at US$ 7,396,394.
- Cuba continues to have no access to 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.
- With complete cynicism and hypocrisy, the United States continues to falsely accuse 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, forcing the country to pay for expensive satellite services.
- On 6 October 2010, the social network Twitter acknowledged full responsibility for blocking messages sent by cell phone from Cuba to its platform. Similarly, in April 2011 it acknowledged that access to certain Twitter tools was being restricted in Cuba on the grounds that they were being accessed from a country that is under a ban.
- As of February 2011, the financial firm Syniverse stopped making payments to the Cuban Telecommunications Corporation (ETECSA) for cell phone roaming charges on the grounds that its bank could not conduct transactions with Cuba, which led to the non-collection of US$ 2.6 million and other difficulties.

The discussion in the General Assembly about developments in the field of information and telecommunications in the context of international security is very pertinent and important. Actions such as those described above by the United States Government against Cuba confirm the need for that debate and the urgency of adopting measures to put an end to such actions.

Cuba supported General Assembly resolution 66/24 and will continue to contribute to the peaceful global development of information and telecommunications technologies and their use for the good of all humanity.

Panama

[Original: Spanish]
[10 July 2012]

Twenty-first century economies have become increasingly based on the service sector, which is especially evident in first world economies. Electronic commerce is nothing more than the most recent expression of this sector of the economy, facilitating commercial transactions and reducing costs and time for delivering goods and services around the world. Electronic governance is the State version of electronic commerce that allows States to meet a large quantity of citizens' demands quickly and efficiently through various technologies (web-based and mobile).

Because of the widespread use of information and communications technologies to support electronic commerce and governance, efforts must be made to ensure that these technologies meet the minimum requirements of the State's clients and citizens for confidentiality, integrity and availability. However, many of the efforts currently under way focus on technical solutions to global problems, which means tackling the problem from various angles.

We believe that the first task for States that wish to promote electronic commerce and governance should be to develop legal frameworks based on international standards that have been previously adopted by other States and are widely accepted, while also creating a hostile environment for criminals and terrorists who use these resources to carry out their activities. Only those countries that adopt legal and technical protective measures can hope to reap the economic benefits of providing an enabling environment for electronic commerce and governance.

At the same time, efforts should continue to develop technologies and policies that defend States' cyberspace, where the interests of different countries meet, through national cybersecurity strategies that can be implemented within clearly defined and realistic time frames. In addition to contributing to international peace, these strategies should be aimed at conserving countries' national security and stability.

Panama has taken the following measures at the national level to strengthen information security and contribute to international cooperation:

(a) Establishment of the Computer Security Incident Response Team, by Executive Order No. 709 of 26 September 2011;

(b) Amendment of the substantive law (Criminal Code) to incorporate new criminal offences related to cybercrime and its subsequent submission to the National Assembly for adoption (Bill No. 377);

(c) Discussion and amendment of the Code of Criminal Procedure in order to align it with the new offences added to the Criminal Code;

(d) Establishment of a working group to discuss the responsibility of Internet service providers in the sphere of information security, headed by the National Authority for Government Innovation and the National Public Services Authority. There is also discussion of implementing the outcome of the group's deliberations at the regional level (the Technical Commission for Telecommunications in Central America/International Telecommunication Union) through national regulators in the Central American region;

(e) Establishment of a working group on handling digital evidence, headed by the Public Prosecutor's Office and with the participation of the National Authority for Government Innovation;

(f) Formal request for technical assistance to the Organization of American States (OAS) to develop the inter-American cybersecurity strategy;

(g) Advanced training in incident handling facilitated by the OAS/CERT Coordination Centre (CERT-CC), carried out in Panama in April;

(h) Evaluation of the United Nations Office on Drugs and Crime (UNODC) proposal for a programme to build Panama's capacity to combat cybercrime;

(i) Regular participation in the Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas and meetings of the OAS Inter-American Committee against Terrorism;

(j) Formal request for accession to the Convention on Cybercrime made by note verbale of 31 January 2012, from the Ministry of Foreign Affairs to Carlos Arosemena, Ambassador of Panama in Brussels.

With respect to possible measures that could be taken by the international community to strengthen information security at the global level, we believe that the following recommendations should be considered:

(a) Adoption of a common legal framework that would allow collaboration between States through expeditious mutual legal assistance based on internationally accepted procedures;

(b) Development of national and regional cybersecurity strategies;

(c) Promotion of the regular exchange of information between States through national incident response teams to facilitate the flow of information, especially information related to the prosecution of crime and terrorism;

(d) Development of public awareness programmes on local and international regulations applicable to each State.

Qatar

[Original: English]
[18 May 2012]

The State of Qatar's national efforts in the information security arena are based on taking a holistic approach that considers both the security of information assets as well as the safety of individuals using those assets. The strategy is aligned with Qatar's 2030 Vision, which highlights human, social and economic development as key pillars and is driven by international endeavours such as the ITU Global Cybersecurity Agenda and the critical information infrastructure protection principles of the Group of Eight.

Currently, the national cybersecurity programme in Qatar (Qatar Computer Emergency Response Team, an Information Security Centre of Excellence initiative), a Government-sponsored organization under the auspices of the Supreme Council for Information and Communications Technology, forms an important cornerstone of Qatar's cybersecurity agenda, which includes critical information infrastructure protection and Government information and communications technology mission assurance branches.

The Qatar Computer Emergency Response Team works with Government agencies, private and public sector organizations and Qatar's citizens to ensure that online threats are monitored and risks are contained. Its established practices for investigating threats include state-of-the-art digital forensics, malware analysis and threat monitoring system capabilities as well as channels to enhance security preparedness and response through situational training programmes. Following is a brief description of its functions:

Threat intelligence

Security Operation Center. Security analysts will utilize internally developed tools (threat monitoring systems) to proactively alert Government agencies and critical organizations about threats associated with eradication tools.

Threat monitoring system. The system is an in-house tool that aggregates and analyses threat intelligence information from a number of sources in order to detect and mitigate the impact of infected computers or local websites.

Malware analysis lab

The objective of the lab is to build the capability to measure, analyse and provide protection from malware threats on a national level. Currently, the lab produces a detailed report on the behaviour of the malware on infected machines; types of targeted system; the sources of malware based in the country; and any Internet connection with the command and control server. It also helps to measure the weight of every collected malware, in order to evaluate the risk associated with specific malware threats by volume of the malware, and to provide detection of malware through all anti-virus engines existing in the market.

Public incident handling

The Qatar Computer Emergency Response Team aims to minimize the number of infected machines in the State of Qatar by providing essential support to the public and to the critical sector. In order to achieve this goal and provide the right guidance, Qatar has expanded its incident response service to cover home Asymmetric Digital Subscriber Line (ADSL) Internet users via the public incident handling portal. It provides various steps, guidelines and basic software tools to scan and remove infections from home ADSL machines.

Cybersecurity training

The Qatar Computer Emergency Response Team conducts cybersecurity-related training and workshops for information technology professionals from Government organizations and other Gulf Cooperation Council countries.

Cybersecurity awareness

The Qatar Computer Emergency Response Team builds a foundation of human knowledge about cybersecurity issues and best practices, focusing on corporate employees.

It works to protect critical infrastructure, in view of the fact that a number of industry sectors such as finance, energy and information and communications technology, are critical to sustaining Qatar’s economy, its population and its Government. As a result, it aims to protect the information systems that underpin these critical sectors as follows:

- Developing national protection strategies, best practices frameworks and tools, raising awareness with stakeholders.
- Directly assisting owners and operators of critical infrastructures in improving supervisory control and data acquisition (SCADA) network safeguards.
- Understanding industry sector issues and cross-sector dependencies and implementing sector-specific protection strategies.
- Working with international information infrastructure protection organizations for determining transnational solutions.

- Measuring the maturity of information infrastructure protection organizations in the country and evaluating progress.

Furthermore, cybersecurity programme of the Supreme Council for Information and Communications Technology continues to work with the legislative body in drafting laws and standards to constantly improve the nation's information and communications technology safeguards in addressing emerging contemporary threats.

The Supreme Council recommends adoption/development of the following possible measures, through the international community:

- Establishment of international legal frameworks harmonized at the regional level in all countries, within five years.
- Establishment of a computer incident response team in all countries that do not currently have one, within three years.
- Development of national cybersecurity strategies, aligned with international cooperation principles, including critical information infrastructures protection (CIIP), within five years.
- Development of cybersecurity-related curricula aimed at building capacity and raising awareness in various constituencies (e.g., Governments, academia, private sector, schools).
- Emphasizing the importance of online safety awareness programmes for children and youth.

Turkey

[Original: English]
[31 May 2012]

Information and communication technologies are rapidly penetrating into both daily life and business processes. Various data critical for individuals, institutions or Governments is stored digitally and transmitted in cyberspace. Despite its benefits, technology carries some risks, in terms of the inability to sustain the confidentiality and integrity of digitally stored data and the availability of information systems. Vulnerabilities in information and communications systems — stemming from faulty design, configuration and operation and inadequate technical abilities and lack of training or security awareness in employees and users — provide an appropriate environment for those risks to materialize.

In order to avoid or mitigate risks and remedy vulnerabilities, efforts to develop cybersecurity are increasingly becoming important at national and institutional levels. In this regard, building technical and administrative capacity and increasing the security awareness of executives, employees and users in public and private institutions are regarded as essential parts of these efforts.

The awareness of high-level executives of the Turkish Government about the need to increase national information security is well established. In addition, the Information and Communications Authority of Turkey specifically focuses on researching best practices and emerging threats in cyberspace, organizing and conducting national cybersecurity exercises, increasing institutional and technical capacity for responding to emergency situations and performing regular audits of

electronic communications operators in order to ensure that adequate policies, processes, programmes and controls are in place to properly handle electronic communications security incidents.

Researching international concepts regarding global threats, the specific vulnerabilities of information systems and best practices in terms of mechanisms of information, as well as expert knowledge-sharing with other international organizations, are considered to be relevant in order to strengthen the security of global information and telecommunications systems.

Multilateral conventions to address cooperation on, and forensic approaches to, information and communications security incidents in cyberspace, as well as information sharing on malware databases, could prove to be useful instruments for strengthening global information security.

Ukraine

[Original: Russian]
[31 May 2012]

General appreciation of the issues of information security

The rapid introduction of information and communications technologies into all spheres of life and the globalization of information links have led to a worldwide shift of unlawful activities into cyberspace. Today computer crime, also known as cybercrime, for which State borders do not exist, threatens not only the rights and freedoms of individuals but also the national interests and security of States.

In recent years there has been a marked rise in computer attacks against critical national infrastructure, causing damage to States through the distortion of important information and the disruption of production processes at factories, the supply of utilities and energy, and transportation systems.

An assessment of cybercrime in 2011 in individual States in which the information systems of State bodies and agencies were the targets of hacker attacks that blocked their activities reveals the enormous threat that cyberattacks pose to society and the unpredictability of their consequences.

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

Some developed countries have addressed these threats by establishing national anti-cybercrime systems headed by a single coordinating body. This approach makes it possible to effectively pool the strengths and resources of the relevant governmental and non-governmental entities to counter and neutralize cybersecurity threats.

This was one of the main considerations guiding the review of approaches to assessing new threats and challenges, including in the sphere of information security, the organization of high-level State events on the establishment of a single nationwide anti-cybercrime system, the drafting of a bill on cybersafety and the establishment and strengthening of cooperation with foreign intelligence services and law enforcement agencies.

In June 2011, in cooperation with the agencies of 11 States (Canada, Cyprus, France, Germany, Latvia, Lithuania, Netherlands, Romania, Sweden, United Kingdom and United States), the Security Service of Ukraine put a stop to the criminal activities of a group of hackers. Using malware spread via the Internet, this group had stolen over $72 million from foreign banking institutions.

In October 2011, the Security Service of Ukraine organized and conducted in Yalta, Ukraine, the annual round of talks on cyberdefence by experts from Ukraine and the North Atlantic Treaty Organization. The outcome reaffirmed Ukraine's position on the need to develop the information security system further with the participation of the public and private sectors and using the lessons learned in other States.

At the initiative of the Security Service, the issue of establishing a separate commission on cybersecurity will be discussed at the thirty-second Meeting of Heads of Special Services and Security and Law Enforcement Agencies of the Commonwealth of Independent States.

The content of the concepts mentioned in paragraph 2 (General Assembly resolution 66/24)

The following principal threats to national security, including information security, are defined in Ukrainian legislation:

- Restrictions to citizens' freedom of speech and access to information.
- Cybercrime and cyberterrorism.
- Disclosure of State secrets or any other secret information protected by law, or of confidential information that is State property or is used to meet the national needs and interests of society and the State.
- Attempts to manipulate public perception, including by disseminating misleading, incomplete or biased information.

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

The main way in which the international community can strengthen information security is to create an enabling environment that allows individual States to ensure their own information security and to develop effective cooperation in this regard.

To establish mechanisms that will effectively counter existing and potential threats to information security, the international community should take the following measures:

- Implement consultative mechanisms for cooperation on cyberdefence to facilitate the exchange of experience in drafting legislation and regulations in this area.
- Establish systems for the exchange of information on cyberspace monitoring and for early notification of cyberattacks and the exchange of information on technical aspects of cyberattacks, tracing the origins of attacks and effective countermeasures.

- Cooperate on addressing the harmful effects of cyberattacks, sharing lessons learned, and developing technological solutions and organizational recommendations on deterring cyberattacks.
- Develop international legal instruments to establish standard terminology and rules, such as a Code of Internet Conduct.

Owing to the need to counter these threats, partner intelligence services and law enforcement agencies should work together in the following areas:

- Develop mechanisms for the prompt sharing among intelligence services of information concerning the activities of organized criminal groups, including terrorist groups, aimed at unauthorized interference in the information resources of national Internet infrastructure or the information systems of government offices or businesses.
- Exchange information on crimes relating to unauthorized access to the computer systems of financial institutions, including for the purpose of forging bank cards, or unauthorized interference in the functioning of bank computer systems for the purpose of stealing confidential information or impeding operations.
- Collaborate during operations to track persons committing cybercrimes using national Internet infrastructure and document their unlawful activities.
- Exchange experience and current practices in the examination of software and hardware (cyber forensics) while investigating crimes committed using computer technology and share methods and techniques of examining computer equipment in order to document criminal activities.
- Establish joint training programmes for the staff of intelligence services and internships for their experts.
- Participate in joint symposiums, seminars and conferences on countering cybercrime.

One form of cooperation could be to establish a system for monitoring the resources of national Internet infrastructure in order to ensure the early detection of threats and a system for identifying the best tools to use in neutralizing those threats.

One possible mechanism for coordinating the cybersecurity activities of State bodies, telecommunications service providers and other actors in national information and communications technology infrastructure aimed at preventing unlawful uses of computers and information technology could be to establish national computer incident response centres and have them work in close collaboration with one another.

The main tasks of such national centres could include the following:

- To collect, analyse and compile in the relevant databases information on current cybersecurity threats.
- To monitor and detect web-based mechanisms and resources whose operations are contrary to the regulations governing the use of national Internet infrastructure.

- To develop recommendations for Internet users to protect the interests of individuals, society and the State in the area of information and recommendations on providing advisory services and technical support to users.
- To receive urgent reports of hacker attacks, provide emergency assistance to stop them and promptly notify Internet users and users of other information systems (including local and corporate systems) about cybersecurity threats.
- To collaborate and exchange information with similar centres in other countries.