United Nations A/68/156/Add.1

General Assembly

Distr.: General
9 September 2013
English
Original: Arabic/English

Sixty-eighth session
Item 94 of the provisional agenda*
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Report of the Secretary-General

Addendum**

Contents

* A/68/150.
** The information in the present report was received after the issuance of the main report.

13-47545 (E) 031013

II. Replies received from Governments

Armenia

[Original: English]
[5 July 2013]

The Concept of Information Security was adopted by Order of the President of the Republic of Armenia No. NK-97 of 25 June 2009. It states that the national security of the Republic of Armenia depends considerably on information security, which encompasses components such as information, communication and telecommunication systems. The Concept also includes a general assessment of the problems of information security of the Republic of Armenia, current challenges and threats and their root causes and peculiarities, as well as methods to address them in different spheres of public life.

An intergovernmental committee was created to coordinate the implementation of programmes related to the concept of information security.

The Concept on "Formation of Cyber Society" was approved by a Decision of the Government of the Republic of Armenia on 25 February 2010. The Council of Electronic Governance of the Republic of Armenia was created, and the general scope of cyber security was defined within the framework of the Concept on "Formation of Cyber Society". Annex 4 to the Concept sets out the activities for ensuring the cyber security of the State. A State committee and a group of experts were formed to pursue the above objectives.

The following measures were also taken at the national level in order to strengthen information security.

Pursuant to Government Decree No. 479-N of 30 April 2009, a special communication station to deal with the security of the Internet was developed and is functioning. The station ensures the security of the public information of governmental bodies uploaded on the Internet and the secure connection of the information systems of governmental bodies to the Internet.

At the beginning of 2012, the group of experts elaborated a draft national programme on the establishment of a cyber security system in the Republic of Armenia. The draft programme is at the stage of discussions in the Government of Armenia.

In 2006, the Republic of Armenia ratified the Convention on Cybercrime, opened for signature in Budapest in 2006, and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in 2012. The National Security Service and the Police of the Republic of Armenia are the competent governmental agencies implementing the provisions of the above Conventions. At the present stage, the intergovernmental group of experts is carrying out activities to bring the relevant national legislation into line with the Convention.

The Republic of Armenia develops active cooperation on cyber security in the framework of the Organization for Security and Cooperation in Europe (OSCE). Currently, the Armenian side is engaged in the negotiations in the framework of the informal working group to elaborate a set of confidence-building measures on cyber security.

The Armenian side has included one action with seven subactions in the sphere of cyber defence in its Individual Partnership Action Plan 2011-2013, which is being implemented in cooperation with the North Atlantic Treaty Organization.

Canada

[Original: English]
[3 September 2013]

Taking into account the assessments and the 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, Canada would like to share with the Secretary-General its views and assessments on the following issues.

1. Information security

Canada is concerned about the real and rising threats posed by malicious cyber activities and recognizes that addressing malicious cyber activity requires national, regional and international cooperation.

Canada has a strategic interest in preserving an open cyberspace, given its importance to Canada's prosperity, security and values of democracy and human rights. The public and private sectors of Canada both depend on a secure, robust and stable information infrastructure to conduct their daily operations. Computer-based systems, together with their Internet and network connections, form the backbone of much of Canada's critical infrastructure, including the energy, the finance, the telecommunications and the manufacturing sectors and Government information systems. The smooth operation of critical infrastructure supports our way of life and Canada's economic, political and social well-being.

National level

Since 1996, the Government of Canada has acknowledged that systems vital to operating Canada's critical infrastructure could be subject to cyber attacks and that Government has a role to play in protecting these systems from such attacks. In subsequent years, the Government has taken action. After reviewing its ability to assess and reduce infrastructure vulnerabilities, it developed and implemented a comprehensive approach to protecting Canada's critical infrastructure through partnerships, and monitored and analysed cyber attacks and threats against federal government systems. In 2010, the Government released its National Strategy and Action Plan for Critical Infrastructure and earlier this year its Action Plan 2010-2015 for Canada's Cyber Security Strategy, which aims to secure Government systems, engage in partnerships to secure vital cyber systems outside the federal Government and help Canadians to be secure online.

International level

Since 2007, Canada has been one of the key contributors to the Organization of American States (OAS) Cyber Security Programme, which assists States in the Americas in preventing, monitoring and responding to cyber threats by enhancing national-level planning and coordination, as well as regional cooperation. Through its counter-terrorism capacity-building programme, Canada has helped several OAS

member States to develop their own national cyber security strategies and join the OAS Secure Hemispheric Network of Cyber Security Incident-Response Teams.

Since 2012, Canada and other participating States of the Organization for Security and Cooperation in Europe (OSCE) have worked to develop confidence- and security-building measures to reduce the risks of misperception, escalation and conflict that may stem from the use of information and communications technologies.

Canada is also actively participating in international initiatives to combat cyber crime in a number of forums, including the Group of Eight, the United Nations Office on Drugs and Crime and OAS. Canada also participated in the most recent United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2012-13).

2. International concepts

Existing treaty and customary international law is applicable to the use of information and communications technologies by States, and is essential to maintaining peace and stability, and promoting an open, secure, peaceful and accessible information and communications technology environment. Among existing international law relevant to cyberspace are the Charter of the United Nations, international human rights law and international humanitarian law. In the most recent report of the United Nations Group of Governmental Experts, Canada was pleased to see a clear affirmation by States of the applicability of international law in cyberspace as the cornerstone for norms and principles for responsible State behaviour.

Canada also believes that addressing the security of information and communications technologies must go hand-in-hand with respect for human rights and fundamental freedoms, including the right to hold opinions without interference, as well as the rights to freedom of expression, association and assembly, and respect for privacy. The right to freedom of expression is set out in both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights. These instruments provide that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one’s choice.

3. Possible measures to strengthen information security globally

Canada is working closely with international partners, including major multilateral organizations and private sector associations, to strengthen the information security of the networks upon which Canada’s economic prosperity and security rely. Canada is also enhancing collaboration and sharing information with some of its key partners and within multilateral organizations on cyber security.

Canada has developed a new process to coordinate a national response to major cyber incidents and engage owners and operators of its critical infrastructure to develop and implement their own cyber security strategy.

There is widespread interest by other countries to enhance cyber security and prevent cyber crime. The key international instrument that deals specifically with cyber crime is the Council of Europe’s Convention on Cybercrime, which Canada

signed in 2001. Also known as the Budapest Convention, this document serves as a guideline for developing comprehensive national legislation against cyber crime and as a framework for international cooperation between States.

Germany

[Original: English]
[25 June 2013]

General appreciation of the issues of information security

The digitalization of economic, administrative and private interactions is not only ongoing, but also accelerating. This offers unprecedented opportunities both for industrialized and developing countries. At the same time, increasing dependency on information and communications technologies creates vulnerabilities and systemic weaknesses. There is also a new interconnectedness on the part of all actors, from the private user to businesses and Government organizations. The trend regarding cyber attacks is clearly towards more sophisticated malicious activities such as Advanced Persistent Threats or highly sophisticated malware going after high-value targets. These activities are driven by interest in profit or information on, respectively, the control of critical assets, systems and infrastructures with severe consequences for Governments, numerous enterprises and organizations, including providers of critical infrastructure services. Sophisticated malicious activities are notoriously hard to detect. The speed of innovation routinely outpaces attempts to secure existing technologies. The fact that malicious tools and methods can be obtained relatively easily, being commercially available on an unregulated or black market, exacerbates the risks. Our current information technology environments cannot be secured against them solely through conventional information technology security approaches.

Highly professional attackers are dedicating considerable technical and financial means to detecting weaknesses in information and communications technology systems and making use of these for their own purposes. The difficulty of reliable attribution and the resulting opportunities for “false flag attacks” pose additional risks to national and international security, in particular through misunderstanding and miscalculation. Intrusions aimed at collecting information often initially look no different from those with a destructive aim. This further increases the risk of misperceptions about incoming attacks and their possible breach of the prohibition of the use of force in international relations.

Prevailing ambiguity about what norms apply in cyberspace creates additional unpredictability. Process control systems for critical infrastructures have proven particularly vulnerable to malicious information and communications technology operations. The risks of uncontrollable collateral damage on a global scale are high, including the infection of industrial control systems with potentially physical destructive effects. A single cyber attack against core telecommunication infrastructure could cause more global disruption than a single physical attack.

Irrespective of varying degrees of information and communications technology capacity and security of different States, concrete steps to enhance resilience are often being deferred or even left off the agenda entirely as a result of the uncertainty surrounding risks to cyber security and how to address them effectively, the

complexity and the novelty of digital attacks, and the secrecy obscuring individual incidents.

Efforts taken at the national level

In 1991, the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) was established as the first and foremost central information technology security service provider for the Federal Government. In this function, BSI publishes binding minimum information technology security standards for the federal administration and serves as its central information technology incident reporting office. It furthermore operates as a neutral office for consultancy and support in the field of information technology security. Main achievements of the work done by the office were, for example, the Information Technology Security Management Standard (IT-Grundschutz), the computer emergency response team for federal agencies (CERT-Bund) as a platform for incident handling and information exchange (dating back to 1994) and the Citizen Computer Emergency Response Team (Buerger-CERT), founded in 2006, as a means to address larger parts of society and raise awareness. Moreover, BSI issues warnings on malware and security vulnerabilities in information technology products and services, informs concerned parties (including information technology vendors and general public) and delivers recommendations for countermeasures.

The 2005 national plan for the protection of information infrastructures, targeting both government and industry, was followed by the cyber security strategy adopted by the Federal Government in February 2011. Its core is critical infrastructure protection.

Since 2008, the German Government and German critical infrastructure operators have been cooperating in a public private partnership. This “CIP Implementation Plan” (UP KRITIS) maintains working groups for different aspects of cyber security, such as crisis management, exercises and availability of critical services.

The National Information Technology Situation Centre (Nationales IT-Lagezentrum), which is operated by BSI, keeps track of the national and global information technology security situation in order to rapidly detect and analyse major information technology security incidents and recommend protective measures. In case of an information technology-related crisis, it expands its capacity and becomes the National Information Technology Crisis Reaction Centre (Nationales IT-Krisenreaktionszentrum), concentrating capabilities for handling information technology crises, covering all national aspects, including governmental networks and critical infrastructures.

In keeping with the 2011 cyber security strategy, all Government authorities that deal with cyber security issues are to work closely and directly with each other and with the private sector within the National Cyber Response Centre (Nationales Cyber-Abwehrzentrum), which is led and hosted by BSI.

With regard to policy, the National Cyber Security Council (Nationaler Cyber-Sicherheitsrat) at the State secretary level addresses key cyber security issues and the position of Germany on them. This includes coordinating cyber foreign policy, including aspects of foreign, defence, economic and security policy.

Furthermore, a platform for cooperation and information exchange was initiated at the national level in October 2012: The Alliance for Cyber Security (Allianz für Cybersicherheit) facilitates close cooperation between partners in the economic, academic and administrative fields and, particularly, with enterprises of special public interest.

The CIP Implementation Plan is currently being updated after four years of activity. It will be opened for more operators of critical infrastructures and will set up a number of new working groups within the sectors of the critical infrastructures. In addition, cooperation with the new Alliance for Cyber Security will be established.

International interconnections in cyberspace mean that coordinated action at the international level is essential. Within the European Union and international organizations, Germany therefore strongly advocates strengthened cyber security while, at the same time, protecting the social and economic benefits in cyberspace.

In its cyber security strategy, in view of the global interconnection of information technology, Germany advocates developing broad, non-contentious, politically binding norms of State behaviour in cyberspace. They should be acceptable to a large part of the international community and should include measures to build trust and increase security.

Confidence- and security-building measures in cyberspace

Cyberspace is a public good and a public space. As such, we have to consider cyberspace security in terms of the resilience of infrastructure and the integrity and failure safety of systems and its contained data. Being a public space, States have to promote security in cyberspace, particularly regarding security against crime and malicious activities, by protecting those who choose to use authenticity tools against identity theft and securing the integrity and confidentiality of networks and data.

Cyberspace is global by nature. Ensuring cyber security, enforcing rights and protecting critical information infrastructures requires major efforts by the State at the national level and in cooperation with international partners. At the national level, Germany has a distinct culture of cooperation between a large number of computer emergency response teams throughout economic, academic and administrative bodies. In this context, CERT-Bund is a well-established focal contact point for these teams. At the European and international level, CERT-Bund is closely cooperating with a set of other governmental computer emergency response teams, with the Forum for Incident Response and Security Teams (FIRST) network being the most important global forum for computer emergency response teams to interconnect in cyberspace.

Against this backdrop, Germany is ready to work on a set of behavioural norms addressing State-to-State behaviour in cyberspace, including, in particular, confidence-, transparency- and security-building measures to be signed by as many countries as possible. Germany therefore actively participated in the 2012/13 Group of Governmental Experts tasked “to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures with regard to information space …” (General Assembly resolution 66/24).

Germany outlined possible elements of such a code of conduct on international norms at the Organization for Security and Cooperation in Europe (OSCE) conference on cyber security, held on 9 and 10 May 2011, as follows:

(a) Confirmation of the general principles of availability, confidentiality, competitiveness, integrity and authenticity of data and networks, privacy and protection of intellectual property rights;

(b) Respect for the obligation to protect critical infrastructures;

(c) Enhanced cooperation aimed at confidence-building, risk reducing measures, transparency and stability through:

(i) Exchanges of national strategies, best practices and national perceptions referring to the international regulation of cyberspace;

(ii) Exchange of national views on international legal norms pertaining to the use of cyberspace;

(iii) Establishment and notification of points of contact;

(iv) Establishment of early warning mechanisms and enhancement of cooperation between computer emergency response teams;

(v) Upgrading of crisis communication links to encompass cyber incidents, support for the development of technical recommendations that advance robust and secure global cyber infrastructures;

(vi) Responsibility to combat terrorism comprising the exchange of practices and enhanced cooperation to address non-State actors;

(vii) Support for cyber security capacity-building in developing countries, and the development of voluntary measures for cyber security support to large-scale events.

Along these lines, Germany submitted a position paper to the United Nations Group of Governmental Experts in July 2012. We strongly welcome the recommendations of the Experts on norms, rules or principles of responsible behaviour of States and confidence-building measures in cyberspace, as well as the emphasis the Experts placed on a multi-stakeholder approach to cyber security.

In 2011 and 2012, Germany supported projects on international cyber security and confidence- and security-building measures being carried out by the United Nations Institute for Disarmament Research (UNIDIR) and the Institute for Peace Research and Security Policy at the University of Hamburg. The first Berlin Cyber Conference, held in December 2011, provided a platform for international discussion on risks, strategies and confidence-building in international cyber security. The second Berlin Cyber Conference, held in September 2012, focused on the Internet and human rights. A main conclusion was that security, freedom and privacy online are complementary concepts. Germany also supported the 2012 UNIDIR Cyber Security Conference, held in Geneva on 8 and 9 November 2012, with a focus on confidence-building measures in assuring cyber stability.

Moreover, we see the necessity to start a debate on international cooperation in the framework of attribution of cyber attacks, which are usually very difficult to trace, State responsibility for cyber attacks launched from their territory when States do nothing to end such attacks, despite being informed about them, and the

responsibility of States not to facilitate areas of lawlessness in cyberspace, for example, by knowingly tolerating the storage of illegally collected personal data on their territory.

On 27 and 28 June 2013, the third Berlin Cyber Conference, held on the theme "Securing the Freedom and Stability of Cyberspace: The Role and Relevance of International Law", and organized by the Federal Foreign Office in close cooperation with the University of Potsdam, endeavoured to provide international legal assessments of cyber operations not transgressing the threshold of armed attack and thus not engaging the law of armed conflict. Consistent with existing international norms and principles, States are responsible for the actions of those within their sphere of control that affect the security and stability of information and communications technology. Every State should consider how to minimize or end malicious cyber activity originating from within its sphere of control or travelling over its networks. States bear responsibility for internationally wrongful cyber activity attributable to them, including the internationally wrongful activity in cyberspace of any State-backed proxies acting on the State's instructions or under its direction or control, in accordance with existing norms of State responsibility under customary international law. States should take all necessary measures to ensure that their territories are not used by other States or by non-State actors for purposes of unlawful use of information and communications technology against other States and their interests. These necessary measures should include appropriate national legislative and regulatory frameworks needed to meet international responsibilities. Internationally wrongful cyber activity can affect States in three main ways: (1) as countries of origin of malicious cyber activity with possibly damaging effects; (2) as transit countries, whose information and communications technology infrastructures are instrumentalized for malicious cyber activity; and (3) as target countries, where damage caused by malicious cyber activity occurs. In all these scenarios, States are obliged to exercise due diligence, which can be of both material and procedural in nature and can range from prevention, i.e., the period preceding potential harm, to containment, i.e., the onset of the actual, ongoing detrimental cyber activity, to follow-up, i.e., the period after malicious cyber activity has been pursued.

Cyber security in the Organization for Security and Cooperation in Europe

The Organization for Security and Cooperation in Europe has been discussing cyber security issues for several years. At the OSCE summit held in Astana in 2010, the Heads of State and Government of the 56 participating States of OSCE underlined that ''greater unity of purpose and action in facing emerging transnational threats" must be achieved. The Astana Commemorative Declaration mentioned cyber threats as one of these emerging transnational threats.

Germany actively participated in the OSCE conference held in Vienna in 2011, held on the theme "Exploring the future OSCE role", on a comprehensive approach to cyber security. In the course of the conference, concrete recommendations for OSCE follow-up activities were discussed. In May 2012, an informal working group was established by Permanent Council Decision 1039 (PC.DEC/1039) and tasked to elaborate a set of draft confidence-building measures to enhance interstate cooperation, transparency, predictability and stability, and to reduce the risks of misperception, escalation and conflict that may stem from the use of information and communication technologies. Germany submitted a non-paper to the group in June 2012 containing German suggestions for a first set of confidence-building

measures within the OSCE framework. Germany regrets that it was not possible to reach consensus for the adoption of such a first set of confidence-building measures at the Dublin Ministerial Council in December 2012, but welcomes the fact that the group resumed its work in 2013.

Germany will continue to actively support OSCE discussions on exploring the future OSCE role in the field of cyber security.

Military aspects of cyber security

As military forces, too, increasingly rely on information technology to master ever more complex scenarios at all levels of command, the protection of the information and the means to process it has become a first order task.

However, in military thinking, information security is challenged not only by a potential adversary, in an operational understanding, using weaponry for the physical destruction of information infrastructure, but also by irresponsible users, malfunctioning technology, criminals or simply accidents.

Hence, the efforts to be undertaken range from awareness-raising of each single user and securing the trustworthiness of the supply chain for information technology, to responsive defences to fend off cyber attacks and an overall resilient information technology architecture.

In essence, a comprehensive risk management is required, with measures to strengthen information security on a national and global scale.

At an early stage, the German armed forces (Bundeswehr) established resilient command and control architectures, security techniques and procedures and an information technology-security organization, encompassing all branches of the armed forces, and including an independent computer emergency response team with the capacity to intervene in case of critical disruptions to the operations of information technology. Adapting personal and technical abilities to the continually increasing level of threat is a perpetual task.

The German armed forces are collaborating closely with the Federal German Ministry of the Interior in its efforts and strongly support the strengthening of information security in the North Atlantic Treaty Organization (NATO) and the European Union and the formation of policies and better coordination of capacities to this end. Furthermore, the armed forces hold regular exchanges with a number of countries in the context of information security, both at the policy and working levels.

The German armed forces welcome initiatives and work together with other departments of the Federal German Government on international motions to further protect the utility of worldwide information networks, for example, the development of a voluntary international code of conduct in cyberspace.

Cyber defence in NATO

Cyber security has been identified by NATO as one of the key emerging security challenges. The strategic concept adopted by Heads of State and Government at the NATO summit held in November 2010 in Lisbon, stated that “cyber attacks ... can reach a threshold that threatens national and Euro-Atlantic prosperity, security and stability”.

As tasked in the Summit Declaration, NATO Defence Ministers adopted a NATO policy on cyber defence and a cyber defence action plan in June 2011. Since then, NATO has been implementing the action plan continuously.

The policy focuses on the protection of NATO networks and national networks of member States that are connected to NATO networks or process NATO information for core tasks of NATO (including the development of common principles and criteria to ensure a minimum level of cyber defence in all member States). To reduce the global risks emanating from cyberspace, NATO intends to cooperate with partner nations, relevant international bodies such as the United Nations and the European Union, the private sector and academia.

Germany welcomes the commitment of NATO regarding cyber security and actively supports the discussions.

Islamic Republic of Iran

[Original: English]
[7 June 2013]

In the view of the Islamic Republic of Iran the use of information and telecommunications technologies and means brings about many opportunities for all States and humanity as a whole. Today information and telecommunications are essential parts of modern societies. They are extremely crucial resources for the wealth and prosperity of nations. Iran believes that every effort should be made, at the national and international levels, to provide the grounds for the broadest possible use of information and telecommunications technologies and means by all nations and to ensure that those technologies and means remain among the main driving forces of development in all societies.

Without a doubt, achieving such a noble goal is dependent, to a large extent, on ensuring full respect for the sovereign right of any State in the field of information and telecommunications, including the development, acquisition, use, import and export of, and access to, information and telecommunications technologies and means and related services without any restriction or discrimination. Indeed, ensuring constant availability, reliability, integrity and security of information and building a safe and secure information and telecommunications environment is in the interest of all nations and therefore of utmost necessity. It is an undeniable fact that the adoption of any measure to deny or restrict the transfer of advanced information and telecommunications know-how, technologies and means, as well as the provision of information and telecommunications services, to developing countries would have adverse effects on their overall development and therefore, should be avoided.

At the same time, information and telecommunications technologies and means have the potential of being used for illegal purposes, including for adversely affecting the social, cultural, economic, political and security infrastructures and interests of States. On the one hand, ever growing dependence of societies on information availability and telecommunications infrastructure, and on the other hand, the exploitation of information and telecommunications technologies and means for illegal purposes, particularly by criminals and terrorists, including State terrorism, demonstrates the existing vulnerabilities and the extensive effects of any potential threat originating from the information and telecommunications.

Accordingly, taking all appropriate infrastructural, legal and technical measures at the national level to strengthen the security of information and telecommunications technologies and means and to prevent their use for illegal purposes is essential.

Nevertheless, owing to the complex nature and unique features of information and telecommunications technologies and means, including borderless space, dynamism, anonymity, speed and rapid technological advances, as well as the increasing interconnection between the underlying networks of information and telecommunications, it seems that ensuring the security of information and telecommunications merely through the adoption of national measures is impossible. For that reason, and taking into account the growing cases of use of such technologies and means in many countries for illegal purposes, all States should both act nationally and cooperate internationally.

While noting the ongoing efforts within the United Nations and other international organizations on the issues related to information and telecommunications, the Islamic Republic of Iran is of the view that the most appropriate international mechanism for consideration of the developments in the field of information and telecommunications in the context of international security is to launch a process within the United Nations with the equal participation of all States. Iran firmly believes that the main purpose of that process should be to develop a common understanding between States about the importance of enhancing security of information and telecommunications, the nature, scope and severity of threats to information and telecommunications technologies and means, and finding the ways and means to prevent those threats. Such a process can lead to the adoption of a programme of action that will set the necessary measures by Member States and be conducted in the format of international conferences every five years to produce political outcomes ranging from declarations to codes of conduct. Nevertheless, the ultimate goal of that process should be the progressive development of solid international legal foundations for strengthening and ensuring the security of global information and telecommunications and preventing the use of information and telecommunications technologies and means for illegal purposes.

In the view of the Islamic Republic of Iran, consideration of the issues related to the developments in the field of information and telecommunications in the context of international security should be carried out on the basis of the following principles and elements:

(a) As a general principle, international law is applicable and therefore should be applied to the use of information and telecommunications technologies and means by States. For that reason, in their use of these technologies and means, States must observe the purposes and principles of the United Nations and their obligations under its Charter, in particular Article 2, paragraph 3, to settle international disputes by peaceful means, the prohibition in Article 2, paragraph 4, on the threat or use of force in any manner inconsistent with the purposes of the United Nations, as well as the prohibition set out in Article 2, paragraph 7, on intervention and interference in the internal affairs of States;

(b) Nothing shall affect the sovereign right of States in the field of information and telecommunications, including the development, acquisition, use, import and export of, and access to, information and telecommunications know-how, technologies and means as well as all related services, without restriction or discrimination. Accordingly, States should seriously refrain from adopting any

measures to deny or restrict the transfer of advanced information and telecommunications know-how, technologies and means, as well as the provision of information and telecommunications services, to developing countries;

(c) Ensuring the security of information and telecommunications at the national level is exclusively the responsibility of individual States. However, owing to the global nature of information and telecommunications, States should be encouraged to cooperate in preventing the threats resulting from the malicious use of information and telecommunications technologies and means;

(d) The right to freedom of expression should fully be respected. At the same time, this right, in no case, should be exercised contrary to the purposes and principles of the United Nations, national laws and the principles of protection of national security, public order, public health or morals and decency;

(e) States are responsible for their internationally wrongful activities using information and telecommunications technologies and means that is clearly attributable to them;

(f) Building a safe and secure information and telecommunications environment for the benefit of all nations should be the main guiding principle and, therefore, States should refrain, under all circumstances, from the use of information and telecommunications technologies and means for hostile, restrictive or other illegal purposes, including the development and use of information weapons; to undermine or destabilize political, economic or social systems of other States or to erode their cultural, moral, ethical or religious values; and the transboundary dissemination of information in contravention of international law, including the Constitution and regulations of the International Telecommunication Union, or national legislation of targeted countries;

(g) States should raise awareness, at the national and international levels, about the need to preserve and improve the security of information and telecommunications through the responsible use of relevant technologies and means, aimed at developing an international common culture of the information and telecommunications security.

Japan

[Original: English]
[12 August 2013]

General appreciation of the issues of information security

Japan is of the view that cyberspace serves as a basic infrastructure for socioeconomic activities for both the public and private sectors. Cyberspace facilitates economic growth, employment and development, as well as democracy and the protection of human rights by securing free flow of information and freedom of expression thereof. Use of cyberspace is essential to the lives of people and has been prevailing globally.

At the same time, there is a growing need for protecting privacy and intellectual property rights and ensuring the security of cyberspace in order to fully enjoy the benefits of the “positive side” of cyberspace. In addition, cyber attacks have been conducted throughout the world and have become transnational global

threats. These attacks can be carried out by various entities and methods from all over the world. It is not possible for a country alone to tackle the rising number of cybercrimes and cyber attacks; the cooperation of the international community, including relevant States and stakeholders, is essential to address the challenges.

On the basis of these perspectives, Japan is striving to build safe and reliable cyberspace by primarily focusing on securing free flow of information and freedom of expression while giving due attention to the balance between the protection of privacy and assurance of security.

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

Efforts at the national level to strengthen information security

Risks surrounding cyberspace have become more serious recently, and maintenance of cyber security has become an important agenda, with respect to our national security and crisis management and social and economic prosperity, as well as the safety and peace of the Japanese people.

In this context, Japan developed a cyber security strategy in June 2013, covering the period 2013-2015. With this strategy, Japan will take actions to improve information security of the Government agencies and critical infrastructures and to strengthen the capability to take countermeasures against cyber attacks.

Specifically, Japan has incorporated the following measures into the strategy: promote information-sharing concerning cyber attacks with public-private partnership; improve information security literacy not only for the Government and industries, but also for the Japanese people; raise awareness on cyber security; strengthen the capability to take countermeasures against cyber attacks through international cooperation; and increase our contribution in the development of international rules related to cyber security.

Efforts at the national level to promote international cooperation

With regard to the development of international norms on the use of cyberspace, we must with urgency start developing realistic and feasible norms of behaviour to address current issues in a non-legally binding form to cope with the rapidly advancing cyber technologies. Japan will continue to take part in these efforts actively in international forums.

Regarding confidence-building measures, Japan is actively engaged in bilateral consultations with interested States and regional dialogues, including the Asean Regional Forum, with the aim of “improving transparency” and “promoting information-sharing”. In addition, in an effort not to create security gaps in cyberspace, Japan is providing capacity-building assistance to developing countries in Asia, Oceania and Africa, such as developing and strengthening computer emergency response teams. Japan is also promoting information-sharing internationally by strengthening coordination with national computer emergency response teams of other States. Japan believes these efforts contribute to building confidence with interested States.

Content of the concepts mentioned in paragraph 2 of resolution 67/27

Japan believes that existing international law, including the Charter of the United Nations and international humanitarian law, is applicable to the use of cyberspace. However, given the unique characteristics of information and communication network technologies, further consideration is needed on how individual rules and principles would be applied.

Considering the significant role that international law has played in securing legal stability and predictability in the international community, we believe that defining and clarifying how existing international law applies to cyberspace would complement the development of specific international norms on cyberspace and also contribute to building a stable cyberspace.

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

International norms for the use of cyberspace

There are no international norms that regulate cyber attacks or cyber espionage in security, economic and social arenas. In addition, the validity of legally binding norms in cyberspace remains unclear at this stage. It is hard to ascertain the future overview of cyberspace at this time, as the speed of development of cyber technology is quite fast. Furthermore, forming a consensus on legally binding norms will take a very long time. Therefore, with respect to the legal nature of the norms, Japan considers it important to begin by discussing establishing non-binding general norms of behaviour.

Confidence-building measures

As an accumulation of confidence-building efforts among States can positively affect the development of international norms, the international community must continue to promote these efforts. In advancing confidence-building measures, securing transparency and information-sharing is necessary; however, the level of measures taken varies from State to State, as each State has the authority to determine the level at its disposal. It is, therefore, necessary to encourage information-sharing through global frameworks such as those under the auspices of the United Nations and regional frameworks.

Netherlands

[Original: English]
[7 August 2013]

The Netherlands warmly welcomes the opportunity to offer its response to resolution 67/27.

General appreciation regarding issues of information security

The Netherlands supports safe and reliable information and communications technology and the protection of an open, free Internet respecting human rights. It is essential for our prosperity and well-being and serves as a catalyst for sustainable economic growth.

Cyberspace offers opportunities, but also makes our societies more vulnerable. The cross-border nature of threats makes international cooperation crucial. Many measures will be effective only if implemented or coordinated internationally. In this connection, the Netherlands attaches great importance to public-private partnerships, building bridges through confidence-building measures and raising awareness of individual responsibility on the part of all information and communications technology users.

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

The Netherlands is working nationally and internationally for a secure digital environment. At national level, the Netherlands implements the national cyber security strategy, called “Strength through Cooperation”. It will update this strategy in 2013 and publication is foreseen for the second half of 2013. The revised strategy will address the comprehensive view on cyberspace, taking into account the economic opportunities, openness and freedoms, and security.

The Netherlands has the National Cyber Security Council to ensure a collaborative approach between the public sector, the private sector and academic and research institutions, and to advise high-level decision makers in the field of cyber security. It also has the National Cyber Security Centre to identify trends and threats and help manage incidents and crises. The task of the Centre is threefold: to conduct cyber threat analyses based on information from public and private parties; to react to cyber threats and incidents; and the operational coordination of information and communications technology crisis situations. The Centre includes the existing government computer emergency response team. Over the past year, it has expanded its capacity and established strong relationships with key information-sharing and analysis centres. The international annual conference organized by the National Cyber Security Centre brings together experts from Governments, private companies, law enforcement and technical experts to exchange best practices. The Netherlands has implemented a substantive set of measures to improve cyber security and is very willing to share the models it has used with third countries.

An example of public-private partnership being used in the sector of nuclear security are the technical meetings that the Government organized in which the nuclear industry could indicate its needs in the field of information security. This information was used by the Government to improve the “design-based threat”. Keywords are “realistic” and “proportionality”.

Internationally, the Netherlands contributes actively to the efforts of the European Union, the North Atlantic Treaty Organization (NATO), the Organization for Security and Cooperation in Europe (OSCE), the Internet Governance Forum and other partnerships. The Netherlands takes a positive view of the Joint Communication of the European Commission and the High Representative for Foreign Affairs and Security Policy, which calls for the creation of an open, free and secure cyberspace for the European Union and which has been endorsed by the European Council. The European Union is taking up this challenge with its international partners and organizations, the private sector and civil society. The Netherlands fully supports the European Union aims to ensure a secure Internet while promoting openness and freedom on the Internet, to encourage the development of confidence-building measures and norms of behaviour and to apply

existing international law in cyberspace. We strongly believe that security and right of access are key elements in safeguarding the continuing development of the Internet. To this end, the European Union has taken core values, namely, human dignity, freedom, democracy, equality, the rule of law and respect for fundamental rights, as its guiding principle. The Netherlands endorses those core values and sees them as the basis for any cyber security strategy. The Netherlands agrees that, in order to promote a robust and resilient cyberspace, both the public and private sectors need to develop their capabilities and work together efficiently.

On the operational level, the Netherlands promotes practical cooperation between cyber security centres (including computer emergency response team organizations) and the strengthening of the International Watch and Warning Network. The rapid growth in cybercrime calls for effective enforcement to maintain confidence in digital society. Regarding enforcement, the Netherlands encourages more cross-border investigation with enforcement agencies from other European countries and beyond. The Netherlands is a party to the Council of Europe's Convention on Cybercrime and encourages others to accede to the Convention.

Concerning nuclear information security, the Netherlands shares within the European Nuclear Security Regulators Association information on policy approaches and best practices on nuclear security, including cyber. The Netherlands participates actively in the International Atomic Energy Agency technical meetings that aim to share information on cyber and information security.

The Netherlands believes that freedom, transparency and security go hand in hand and strengthen each other. That is why the Netherlands started the Freedom Online Coalition, which currently counts 21 member Governments. The Freedom Online Coalition is committed to promoting Internet freedom and to stressing the importance of digital rights. To this end, the coalition of like-minded Governments coordinate their efforts and work with civil society and the private sector in a multi-stakeholder process to support the ability of individuals to exercise their human rights and fundamental freedoms online. To further the goal of keeping the Internet open and free for all, members of the Coalition established the Digital Defenders Partnership, a fund to support innovative solutions for the protection of bloggers and online activists in danger and for the deployment of emergency Internet services in countries where the Internet is not free or accessible. The contribution of the Netherlands to this fund amounts to €1,000,000 for the duration from 1 October 2012 to 31 December 2014.

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

The starting point of the Netherlands is an open Internet that promotes innovation, stimulates economic growth and safeguards fundamental freedoms. The Netherlands emphasizes the importance of continuing dialogue on the development of standards of State behaviour aimed at safe use of cyberspace. It is keen to contribute actively to this dialogue. The Netherlands notes with appreciation the significant work done by different international and regional actors and stakeholders, such as the Council of Europe, the European Union, OSCE and the United Nations Group of Governmental Experts regarding confidence-building measures in the field of cyber security.

Within the process of the Nuclear Security Summit, information security plays a central role. The Work Plan of the Washington Nuclear Security Summit and the Seoul Communiqué state that the Nuclear Security Summit States aim “to prevent non-state actors from obtaining the information or technology required to use such material for malicious purposes; and to prevent the disruption of information technology based control systems at nuclear facilities”. As the Chair of the Nuclear Security Summit, the Netherlands supports all efforts to contribute to this objective.

Within the Nuclear Security Summit process the Netherlands supports the leadership of the United Kingdom of Great Britain and Northern Ireland in the implementation and sharing of best practices of information security in the nuclear sector. This is done by developing and strengthening national measures, arrangements and capacity for the effective management and security of such information; to enhance related national security culture; to engage with national scientific, industrial and academic communities to further raise awareness, develop and disseminate best practice and increase professional standards; and to support, drawing on and collaborating with IAEA, other key international organizations and partner countries to facilitate mutual achievement of these aims. The Netherlands attaches great importance to an inclusive Internet governance model, involving the private sector and knowledge institutions in this dialogue and is keen to share experience and best practices with others.

The intensive international exchange of knowledge and information among all stakeholders and organizations is essential for making cyberspace more secure and reliable and fully gain its full potential, both in terms of development and bringing societies across the world closer together. The Netherlands therefore welcomes the cyber conferences held in London and Budapest and the upcoming conference in Seoul.

Lastly, the Netherlands is of the opinion that the development of norms for State conduct does not require a reinvention of international law, but rather needs to ensure consistency in the application of existing international legal frameworks. We encourage continued dialogue and reflection to attain consensus regarding the practical effect of the application of existing rules and international law to cyberspace.

Oman

[Original: Arabic]
[26 June 2013]

The Ministry of Transport and Communications wishes to transmit the following information regarding General Assembly resolution 67/27 on developments in the field of information and telecommunications in the context of international security:

1. General appreciation of the issues of information security

The rapid developments that have taken place in information technology and telecommunications have been accompanied by growing risks. Hackers are using increasingly advanced techniques to access information around the globe. The most important challenges faced by States and institutions are an absent or inadequate culture of information security among information and communications technology

users, lack of qualified personnel and differences in legislation regulating e-communications around the world. States must join forces and cooperate to combat information security threats, enhance their response preparedness, raise global awareness of the issue and share pertinent information and expertise.

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

- The Telecommunications Regulatory Authority was established in 2002 and the Information Technology Authority in 2006, to regulate the telecommunications and information technology sectors;
- Relevant legislation has been promulgated, namely the Electronic Transactions Act, issued by Royal Decree No. 69/2008, and the Telecommunications Regulatory Act, issued by Royal Decree No. 30/2002;
- The International Telecommunication Union and the International Multilateral Partnership Against Cyber Threats (IMPACT) recently established the first cybersecurity centre for the Arab region in Oman;
- In order to address technical risks and threats, the Information Technology Authority established a National Computer Emergency Response Team in April 2010;
- Through the Information Technology Authority, Oman is a member of numerous relevant regional and international agencies, including the Organization of the Islamic Conference Computer Emergency Response Team (OIC-CERT), the Gulf Cooperation Council Computer Emergency Response Teams (GCC-CERT) and the Forum of Incident Response and Security Teams (FIRST). Many Omani institutions have obtained ISO certification;
- The competent institutions continuously update their strategies;
- Government authorities have access to a range of information security technologies and programmes;
- A centre has been established to safeguard Government networks;
- Hosting services have been established that offer safeguards for Government websites;
- Technical support is provided to strengthen information security;
- A range of policies and standards on information security have been adopted;
- A series of specialist training sessions have been held on information security;
- Various awareness-raising campaigns have been organized;
- Programmes have been conducted to evaluate information emergency response preparedness;
- A number of pertinent regional and global workshops and conferences have been convened;
- Awareness-raising events have been held at the local level;
- All sectors of society have been involved in efforts to promote information security;

- The Oman National CERT Ambassador Programme to foster information security was launched in January 2012;
- A website to strengthen children's online security has been created (cop.cert.gov.om);
- Awareness-raising visits have taken place in schools, universities, Internet cafes and other places frequented by young people;
- Workshops have been held in order to raise awareness among students and teaching staff;
- The Centre has played an active part in public events in order to reach as many young people as possible and inform them of security risks and responses;
- The Centre has conducted "Train-the-trainer" programmes to provide young nationals with relevant qualifications;
- The first information security operations centre in the Middle East has opened.

3. The content of the concepts

- Oman continuously monitors and reviews these international concepts in order to keep abreast of efforts to strengthen the security of global information and telecommunications systems.
- Consideration must be given to the specificities of countries and their legislation on e-transactions.
- Stakeholders must comply with the particular values and principles that each country seeks to uphold.

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

- Regulating e-transactions and information and inter-State cybersecurity by establishing an international organization under the auspices of the United Nations, as was proposed at the Cyberdefence Conference held in Oman in March 2013;
- Promoting cooperation among States with a view to safeguarding the information and communication technology sector, upon which most countries depend to a great extent in their efforts to promote development. Such cooperation must take place under the auspices of an international organization;
- Sustaining coordination among States to strengthen information security and share cutting-edge experiences;
- Collaborating in response to information security incidents and designating focal points for each country;
- Participating in policy and regulation formulation and sharing best practices;
- Sharing specialized expertise and knowledge and exchanging visits;
- Convening symposiums and workshops for information security personnel;

- Organizing joint international programmes to raise awareness and disseminate a culture of global security;
- Fostering academic collaboration and formulating relevant programmes and curriculums;
- Encouraging and fostering joint research and development programmes in that area.

Turkey

[Original: English]
[10 June 2013]

General appreciation of the issues of information security

Information security has become a necessity in the globalized world as the use of information technologies grows. Information security and cyber security are issues that must be managed with the cooperation of all related parties. In Turkey, the National Cyber Security Board, a central mechanism to coordinate the related parties and follow relevant studies, was established by the Cabinet decision on enforcement, management and coordination of the national cyber security studies, which was published in the Turkish Official Gazette, No. 28447, of 20 October 2012.

The national cyber security strategy and the action plan for 2013-2014 were approved on 20 December 2012, at the first meeting of the National Cyber Security Board.

The goals of the strategy and the action plan are as follows:

- To establish an infrastructure that enables the availability of the services, processes and data provided through information technologies by governmental organizations
- To ensure the security of information systems used in critical infrastructures that are operated by the Government or the private sector
- To determine the strategic cyber security actions to minimize the effects of cyber attacks and shorten the recovery time after attacks
- To constitute an infrastructure that facilitates the investigation on cyber crimes by judicial authorities and law enforcement bodies.

The main areas of the action plan are the following:

1. Regulations
2. Studies to facilitate judicial processes
3. Establishment of a national computer emergency response team
4. Strengthening the national cyber security infrastructure
5. Training and raising awareness of human resources about cyber security
6. Development of national technologies for cyber security
7. Expanding the scopes of the national cyber security mechanisms.

The action plan consists of 29 action lines to be carried out under the above-mentioned main areas.

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

The Turkish national regulatory body, the Information and Communication Technologies Authority (BTK), mandated by the Electronic Communications Law (No. 5809), conducts a range of activities to contribute to efforts to meet national and international information security requirements.

In this context, the activities of the Authority in the field of cyber security are stated below.

1. Regulation and inspections

Several requirements for the authorized operators are defined in the by-law on Security of Electronic Communications and the related communiqué that takes this by-law as a basis. The relevant studies aim to promote the level of national cyber security directly in the activities of operators and to contribute international cyber security implicitly.

On the other hand, there are also Authority regulations on electronic signature and registered electronic mail within the context of the Electronic Signature Law (No. 5070) and the Turkish Trade Law (No. 6112). These regulations contribute to the efforts for promoting security and reliability of document and electronic mail exchange processes.

2. Cyber security exercises

The Information and Communication Technologies Authority organizes cyber security exercises to further develop the technical and administrative capacity, to raise awareness and to establish opportunities for international cooperation.

2.1. National Cyber Security Exercise 2011

National Cyber Security Exercise 2011 was held from 25 to 28 January 2011, with the participation of 41 public, private and non-governmental organizations involving representatives of the finance, information and communications technology, education, defence and health sectors, as well as the judicial and law enforcement units and various ministries. Six of the aforementioned organizations participated in the exercise on the observer status.

2.2. Cyber Shield Exercise 2012

This exercise was held in May 2012 under the coordination of the Information and Communication Technologies Authority and with the participation of 12 Internet access providers operating in the electronic communications sector. The participants were the ones with the largest market share in the sector, along with the third generation (3G) mobile Internet service providers. In the exercise, mainly Distributed Denial of Service attacks were applied to the participants and the adequacy of the security measures taken against the attacks was assessed.

2.3. National Cyber Security Exercise 2013

National Cyber Security Exercise 2013, which was co-organized by the Information and Communication Technologies Authority and the Scientific and Technological Research Council of Turkey, under the auspices of the Ministry of Transport, Maritime Affairs and Communications, was carried out from 24 December 2012 to 11 January 2013, with the participation of 61 public, private and non-governmental organizations. Notwithstanding that most of the participants were public organizations, private and non-governmental organizations also participated in the exercise. In addition, the Chairman of the International Telecommunication Union (ITU)-International Multilateral Partnership against Cyber Threats (IMPACT) and one of the board members of Forum for Incident Response and Security Teams (FIRST), which are international cooperation platforms on cyber security, attended the closing event of the exercise as speakers.

3. Project on the prevention of cyber threats

The project on the prevention of cyber threats (Siber Tehditleri Önleme Projesi-STOP) involves the development of necessary mechanisms for the establishment of a honey pot system to detect cyber threats, the instalment and improvement of a cyber attack report system and the production of metadata regarding cyber threats. The activities required by the project are being fulfilled according to the deadlines anticipated by the short-term national cyber security action plan. Within the context of the international cooperation dimension of the project, the Information and Communication Technologies Authority became a member of ITU-IMPACT, which works under ITU.

4. Project on the prevention of spam e-mails

This project was conducted in 2009, under the coordination of the Information and Communication Technologies Authority and with the efforts of Internet service providers and hosting service providers. The purpose of the project was to prevent spam e-mails that pose a threat against network security and keep the network resources busy. At the end of the project, the number of Internet providers propagating spam was reduced by 99 per cent; this improvement was reflected in the reports prepared by global cyber security firms.

5. Establishment of a domestic Internet Exchange Point

The Internet service providers' routing practice of unnecessarily circulating the Internet traffic between two end points from a remote point causes a decrease in service quality owing to unnecessary transmission delays and an increase in the security concerns.

Within this context, by the establishment of an effective Internet Exchange Point and the operators' ability to exchange their traffic under more attractive circumstances, those undesired routing practices and the security concerns caused by them can be highly reduced. Therefore, the Information and Communication Technologies Authority conducts various activities together with the related parties (domestic Internet service providers and international content providers) focused on the formation of an effective domestic Internet Exchange Point.

Measures for strengthening information security globally

Establishment of a national computer emergency response team

Today it is necessary to form a cyber incident response organization that will work effectively at the national level for detecting the newly emerging cyber threats, taking measures necessary to reduce or suppress the effects of potential cyber incidents and sharing information. To this end, in February 2013, the Ministry of Transport, Maritime Affairs and Communications delegated the mission of establishing and operating Turkey's national computer emergency response team to the Communications Presidency, and various activities were initiated to establish the national computer emergency response team that will work 24 hours a day, 7 days a week against cyber threats. USOM, the computer emergency response team, which began operation in May 2013, will work in close cooperation with the other countries' computer emergency response teams and of international organizations.

As a result of the rapid development and proliferation of information and communications technologies, threats against information security go beyond national borders. Hence, it is critical for international organizations and Governments to promote cooperation on information security-related issues and execute that cooperation as soon as possible.