United Nations A/71/172

General Assembly

Distr.: General
19 July 2016
English
Original: Arabic/English/French/
Russian/Spanish

Seventy-first session
Item 94 of the provisional agenda*

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

Report of the Secretary-General

Contents

* A/71/150.

I. Introduction

1. On 23 December 2015, the General Assembly adopted resolution 70/237, entitled “Developments in the field of information and telecommunications in the context of international security”. In paragraph 4 of the resolution, the 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/70/174), to continue to inform the Secretary-General of their views and assessments on the following questions:

(a) General appreciation of the issues of information security;

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

(c) The content of the concepts mentioned in paragraph 3 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 15 February 2015, a note verbale was sent to all Member States inviting them to provide information on the subject. The replies received at the time of reporting are contained in section II. Any additional replies received will be issued as addenda to the present report. The full text of all submissions can be found at www.un.org/disarmament/topics/informationsecurity.

II. Replies received from Governments

Albania

[Original: English]
[15 April 2016]

The main priority for Albania in the field of security and protection for classified information is the signing of the agreement between the Government of the Republic of Albania and the European Union — the agreement on the security procedures for the exchange and protection of classified information. The above-mentioned agreement was signed on 3 March 2016 in Tirana, and it is expected to be ratified in due time by the Assembly of the Republic of Albania.

In the context of initiating and implementing the appropriate measures in Albania, in order to strengthen information security and to promote international cooperation in this matter, a revision of the legal statutes was undertaken.

- Council of Ministers decision no. 188, dated 4 March 2015, “On the approval of rules ensuring staff security”
- Council of Ministers decision no. 189, dated 4 March 2015, “On ensuring physical security of classified information marked as ‘state secret’, NATO information”
- Decision of the Council of Ministers no. 190, dated 4 March 2015, “For several alterations and additions on Decision of the Council of Ministers no. 81, ‘On defining the criteria and the procedures to destroy classified information’”

– Council of Ministers decision no. 701, dated 22 October 2014, “On approving the rules for securing classified information in the industrial area”

Albania has a more comprehensive legal regulation, which is concerned with the physical security of classified information. The “areas of security”, are redefined and located, taking into account the different levels of classified information.

Following the adoption of the new decision for staff security, inter-institutional cooperation, supervision and the inspection of state institutions have eventually increased. State agencies started the process of revising the lists of staff duties and issuing relevant security certificates according to the field of responsibility.

With regard to industrial security, Albania has focused on reviewing politics of information security, by reviewing practices of the Council of Ministers by decision no. 701, dated 22 October 2014.

Another important step on which we have put emphasis, is the drafting of a new law for dealing with classified information — an initiative which constitutes an efficient, up-to-date piece of law with high European standards. The review of national legislation in this field is done taking into account the acquis of the European Union and in particular, Council Decision 2013/488/EU on the security rules for protecting EU classified information.

Australia

[Original: English]
[31 May 2016]

Australia welcomes the opportunity, in response to the invitation in General Assembly resolution 70/237, to provide its views on developments in the field of information and telecommunications in the context of international security. This submission builds upon information provided by Australia in response to resolution 68/243 in 2014 and to resolution 65/41 in 2011.

Cybersecurity is as intrinsically linked to innovation as it is to national security. It is the bedrock of innovation, growth and prosperity. Cybersecurity is a global opportunity that Governments, the private sector and the community are all invested in and can all derive benefit from.

The global community needs to get cybersecurity right. Everyone — Governments, businesses and individuals — need to work together to build a trusted online environment. Not only to protect critical information, but to provide the environment for innovation to flourish; to enable the technology industry to thrive; and to capitalize on the growing global need for better cybersecurity solutions, equipment and skilled individuals.

Australia recognizes strong cybersecurity as a fundamental element for growth and prosperity in a global economy. In 2015 Australia reviewed its approach to cybersecurity and launched its new Cyber Security Strategy on 21 April 2016.

Australia believes that a priority task for the international community is the elaboration of how international law applies to States’ behaviour in cyberspace, especially in non-conflict situations. There is a need for further work to develop understandings on how key concepts such as sovereignty and jurisdiction apply in cyberspace, taking into account our common interest in preserving the global nature of the Internet. There is scope for the further development of voluntary norms set out in the 2015 report of the Group of Governmental Experts in relation to the protection of critical infrastructure, computer emergency response teams, the responsibility of States to assist, cooperation on cybercrime and preventing the proliferation of malicious cyber tools and techniques. It is important that work on confidence-building measures moves to the next phase, from the promotion of transparency to the implementation of cooperative measures.

Canada

[Original: English]
[27 May 2016]

On cyber issues, Canada believes that:

- A free, open and secure cyberspace is critical to global security, economic prosperity and the promotion of human rights, democracy and inclusion.
- Any approach to tackling cyberthreats must go hand in hand with respect for human rights and fundamental freedoms.
- Existing international law is applicable to the use of information and communications technologies by States.
- Promoting peacetime norms helps sustain an environment in which responsible behaviour guides state actions, sustains partnerships and supports a stable cyberspace.
- Practical confidence-building measures are a proven method to reduce tensions and the risk of armed conflict.

At the national level, since the Canadian Government released its Cyber Security Strategy in 2010, it has continued efforts to help secure Canada’s cybersystems and protect Canadians online. Since then, Canada has also launched the “Get Cyber Safe” public awareness campaign. Recently, the Government has committed to undertaking a review of existing measures to protect Canadians and our critical infrastructure from cyberthreats.

At the international level, Canada is active in a number of ways on cyber issues:

- Canada will continue to promote the development of peacetime norms for state behaviour in cyberspace, including the outcomes of the 2012-2013 and 2014-2015 United Nations Group of Governmental Experts. Canada has been selected to participate in the 2015-2016 Group.
- Canada ratified the Budapest Convention in July 2015. Canada encourages countries to become parties to the Convention, or to use it as a model to implement their own cybercrime laws.
- Since 2007, Canada has committed $8.25 million to support cybersecurity capacity-building projects in the Americas and South-East Asia.
- Canada is a founding partner of the Global Forum on Cyber Expertise.

- Canada is working with the United States to align our cybersecurity public awareness campaign initiatives via the “Stop. Think. Connect.” coalition.
- Canada is also working with the United States to implement the Canada-United States Cybersecurity Action Plan, which aims to enhance the resiliency of our cyberinfrastructure.
- Canada has been working to develop confidence-building measures in various forums, including the Organization for Security and Cooperation in Europe and the Regional Forum of the Association of Southeast Asian Nations.
- Canada supports North Atlantic Treaty Organization (NATO) efforts to strengthen the Alliance’s cyberdefence and that of individual allies. Canada has contributed $1 million to the NATO Cooperative Cyber Defence Centre of Excellence.
- Canada has supported the use of information and communications technologies (ICTs) as tools for development, including to help community organizations deliver essential services such as emergency assistance in conflicts.
- Canada’s International Development Research Centre has helped to advance development around the world with ICT for development research and capacity-building.

Colombia

[Original: Spanish]
[13 June 2016]

Through its “Vive Digital” (“Live Digital”) Plan (2010-2014) and the new Plan “Vive Digital — para la gente” (“Live Digital — for the people”) (2014-2018), Colombia has achieved a digital revolution, increasing its total Internet connections from 2.2 million to over 12.2 million in just five years. Colombia will be the first Latin American country to have high-speed Internet connection in all of its municipalities. Over the same period, educational entities have been provided with more than 2 million terminals; 74 per cent of micro, small and medium-sized enterprises are now connected to the Internet (compared with 7 per cent in 2010); we have achieved 90 per cent growth in household connections; and we have taken the Internet to the most isolated rural areas through 7,621 Vive Digital kiosks (located in rural centres with over 100 inhabitants). Among many other achievements, we also have the largest community of digital entrepreneurs in Latin America, with more than 100,000 members.

The national Government recognizes that it is not possible to maximize the benefits and use of information and communications technologies if citizens or companies cannot trust them, in other words, if there is a perceived lack of security in the digital environment. The increasing number of digital security incidents is having a growing impact on such perceptions.

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

Colombia has just launched a new national digital security policy, contained in document CONPES 3854 of 2016, which seeks to ensure that the Government, public and private organizations, law enforcement personnel, academics and individuals in general in Colombia are able to depend on a reliable and secure digital environment that maximizes economic and social benefits, boosting competitiveness and productivity in all sectors of the economy. The policy is the result of a process that engaged multiple stakeholders and it is one of the first national policies in the world — and the first in the region — to incorporate the digital security risk management recommendations issued in September 2015 by the Organization for Economic Cooperation and Development.

The policy provides, first of all, for the establishment of a clear institutional framework for digital security. To that end, coordination and advisory bodies for digital security will be established at the highest level of government and cross-sectoral liaison units will be set up in all agencies of the national executive branch. Secondly, the right conditions will be created to enable multiple stakeholders to manage digital security risk in their socioeconomic activities, and to generate confidence in the use of the digital environment, by establishing mechanisms for active ongoing participation, ensuring an appropriate legal and regulatory framework and providing training in responsible behaviour in the digital environment. Thirdly, national defence and security in the digital environment will be strengthened at the national and transnational levels, adopting a risk management approach. Lastly, but no less importantly, standing mechanisms will be established, with a strategic focus, to promote cooperation, collaboration and assistance in the area of digital security at the national and international levels.

(b) The content of the concepts mentioned in paragraph 3 of resolution 70/237:

Colombia, as a member of the most recently established Group of Governmental Experts (2014-2015), fully agrees that there is a need for further examination of the concepts relating to the security of information and global telecommunications systems and matters related to the application of international law in cyberspace.

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

In line with the above, we fully endorse the important recommendations issued by consensus by the experts who were members of the Group of Governmental Experts, including in relation to the voluntary adoption of measures and good practices, as well as capacity-building and cooperation by States to promote the peaceful use of information and communications technologies, so that they continue to serve as economic and social development tools for countries, especially those that are less technologically advanced.

Cuba

[Original: Spanish]
[6 May 2016]

Cuba shares the concern expressed in resolution 70/237 that information technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields.

Resolution 70/237 also appropriately stresses the need to prevent the use of information resources or technologies for criminal or terrorist purposes.

In this regard, Cuba reiterates its great concern over the covert and illegal use, by individuals, organizations and States, of the computer systems of other nations for the purpose of attacking third countries, because of its potential for triggering international conflicts.

Joint cooperation between all States is the only way to prevent and confront these threats and to avoid cyberspace from turning into a theatre of military operations.

The use of telecommunications with the declared or hidden intent of undermining the legal and political order of States is a violation of internationally recognized norms in this area and can give rise to tensions and situations that might be detrimental to international peace and security.

The Heads of State and Government of Latin America and the Caribbean, at the second Summit of the Community of Latin American and Caribbean States (CELAC), held in Havana in January 2014, proclaimed the Latin American and Caribbean region to be a zone of peace, in order to, among other objectives, foster cooperation and friendly relations among themselves and with other nations, irrespective of differences in their political, economic, and social systems or development levels, to practice tolerance and to live together in peace with one another as good neighbours.

At the fourth Summit of CELAC, held in Quito in January 2016, the importance of information and communications technologies, including the Internet, as tools to foster peace, human well-being, development, knowledge, social inclusion and economic growth was again highlighted. The peaceful use of information and communication technologies in a manner compatible with the purposes and principles of the Charter of the United Nations and international law was also reaffirmed, and it was stressed that such technologies should never be used with the objective of subverting societies or creating situations with the potential of fostering conflict amongst States.

Nevertheless, those efforts continue to be threatened by the constant radio and television broadcasts transmitted by the Government of the United States against Cuba, in contravention of the purposes and principles of the Charter of the United Nations and various regulations of the International Telecommunication Union, and in violation of the sovereignty of Cuba.

Through illegal radio and television broadcasts, it has been constantly attacking Cuban airwaves, disseminating programming specifically designed to incite the overthrow of the constitutional order established by the Cuban people To illustrate, illegal broadcasts averaging 1,880 hours per week were transmitted against Cuba, using 23 frequencies, in the first quarter of 2016 alone.

Cuba hopes for an immediate end to these aggressive policies, which are, furthermore, incompatible with the development of ties based on mutual respect and cooperation between Cuba and the United States, as agreed by the two Governments when they restored diplomatic relations.

It also hopes that the economic, commercial and financial embargo, which has caused serious damage to the Cuban people, will be lifted. The embargo has had a harmful impact in the area of information and communications, among other aspects of the daily life of the Cuban people

International cooperation is essential for confronting the dangers associated with the misuse of information and communication technologies. The International Telecommunication Union has an important role to play in the intergovernmental debate on cybersecurity issues.

Cuba supported resolution 70/237 and will continue to contribute to the peaceful global development of information and telecommunications technologies and their use for the good of all humanity.

El Salvador

[Original: Spanish]
[26 April 2016]

The El Salvador Armed Forces have upgraded the perimeter security computer equipment and implemented security policies governing access to the computer network's resources (regular changes to user passwords, restriction of access to USB ports and DVD and CD readers, and blocking of access to equipment unit C).

Finland

[Original: English]
[31 May 2016]

Finland welcomes the opportunity to provide information on General Assembly resolution 70/237. The following efforts have been take at the national level:

(a) The National Cyber Security Strategy of Finland (2013) and its Implementation Programme (2014) define key guidelines and actions in strengthening cybersecurity and resilience. The Implementation Programme is being updated through a consultative multi-stakeholder process with the aim of finalizing it in 2016.

(b) Since the adoption of the national Cyber Security Strategy, Finland has established the National Cyber Security Centre and the Cybercrime Prevention Centre, and an Ambassador for Cyber Affairs has been appointed. The National Information Security Strategy was adopted in February 2016.

(c) As part of Finnish development cooperation, Finland supports various information and communications technologies (ICTs) for development and cyber capacity-building projects. Finland is a founding partner of the Global Forum on Cyber Expertise. Finland has joined the United States-led Global Connect Initiative, which seeks to bring 1.5 billion people online by 2020. Finland aims to join the new World Bank Digital Development Partnership Trust Fund. Finland supports internet governance based on a multi-stakeholder model.

(d) Finland actively engages in international dialogue on cyber issues in multilateral and regional forums, and in bilateral contacts. Within the Organization for Security and Cooperation in Europe (OSCE), Finland works towards strengthening trust, security and stability in cyberspace and implements the agreed cyber confidence- and security-building measures.

(e) Finland has endorsed the 2015 report of the United Nations Group of Governmental Experts in the Field of Information and Communications Technology in the Context of International Security. Finland has participated actively in the discussions on international law in cyberspace, e.g. in consultations on Tallinn Manual 2.0, and in United Nations Institute for Disarmament Research workshops. Finland joined the Freedom Online Coalition in 2012 and contributes to the Digital Defenders Partnership.

(f) Finland has been a party to the Budapest Convention since 2007. The new Strategic Police Plan, targeting resources at computerized crime prevention and developing cybersecurity know-how, was launched in 2015. There is also a Comprehensive Cybercrime Prevention Plan.

Priority areas for further work by the international community:

(a) Finland attaches a lot of importance to the work of the new Group of Governmental Experts and is prepared to contribute to its success, including to further the identification of norms of responsible state behaviour in cyberspace with a special emphasis on peacetime activities;

(b) Further developing and implementing regional confidence-building measures in the framework of the OSCE;

(c) Continuing support to cyber capacity-building with a view to strengthening resilience and security in cyberspace;

(d) Finland will continue to support and encourage multi-stakeholder dialogue. Strengthening public-private partnerships nationally and internationally is a priority.

India

[Original: English]
[9 June 2016]

While information technology facilitates economic growth and social connectivity, there are serious challenges which need to be addressed. Growth in the information and communications technology (ICT) sector is also accompanied by increasing cyberthreats which range from cyberattacks, cybercrime, cyberterrorism, espionage and money-laundering. Evidence shows that terrorists groups (e.g. ISIS) use internet and social media platforms for their nefarious activities, including recruitment, fund raising, propaganda and radicalization. Misuse of social media is a major concern. While it brings about tremendous connectivity, it can also be misused for accentuating ethnic and social discord.

It is important for the international community to develop a common understanding on the state behaviour in cyberspace and to adopt the confidence-building and capacity-building measures as recommended by the 2015 report of the United Nations Group of Governmental Experts. The issue of Internet governance should not be allowed to get bogged down in the divisive discussions of semantics. While various stakeholders have a role in their respective domains, the

Governments have a primary role to play in the cybersecurity issues relating to national security. There is a need to develop suitable mechanisms for sharing of information relating to cyberthreats, cybercrime and cyberterrorism. There is also a need for real-time cooperation between government agencies to deal with cybercrime. Further, the issue of cyberwarfare, cyberdoctrines and their impact on international security should be discussed at all international forums. While rules of responsible State behaviour in cyberspace are still be agreed to, a common understanding on the confidence-building measures as enumerated in the 2015 report of the United Nations Group of Governmental Experts could be used for taking appropriate measures for capacity-building in the area of cybersecurity. In this regard, the framework developed by the Global Forum on Cyber Expertise provides useful guidance.

India is an important stakeholder in the use of ICT. It supports the multi-stakeholderism in Internet governance and is proactive in various international forums, including the Group of Governmental Experts, the Open Consultation Process on Overall Review of the Implementation of the World Summit on the Information Society Outcomes and the Internet Corporation for Assigned Names and Numbers. India, in consultation with all stakeholders, has adopted an integrated approach with a series of policy, legal, technical and administrative steps for addressing cybersecurity concerns and to promote international cooperation on the subject. Its legal framework is aligned with other legal frameworks in the world. National Cyber Security Policy (2013) has been put in place with a vision to build secure and resilient cyberspace for citizens, businesses and Government. It emphasizes capacity-building, skill development and public-private partnerships on cybersecurity.

Japan

[Original: English]
[27 May 2016]

General appreciation of the issues of information security

Japan believes that cyberspace should be a space where freedom is assured without unnecessary restrictions, and where all actors who wish to access it are neither denied nor excluded without legitimate reason. Our efforts comply with the following five principles; free flow of information, rule of law, openness, self-governance and multi-stakeholder approach.

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

1. Efforts taken at the national level to strengthen information security

Based on the Cybersecurity Strategy established in September 2015, Japan makes efforts to strengthen information security.

2. Efforts taken at the national level to promote international cooperation

Japanese efforts consist of the following three pillars: promoting (1) the rule of law in cyberspace; (2) confidence-building measures; and (3) capacity-building. With regard to the promotion of the rule of law, Japan proactively contributes to international discussion to promote a common understanding that existing international law is applicable in cyberspace as well as to develop non-binding and voluntary norms of responsible state behaviour. As for confidence-building measures, Japan is engaged in the promotion of confidence-building through bilateral dialogue and multilateral frameworks such as the Regional Forum of the Association of Southeast Asian Nations (ASEAN). With regard to capacity-building, Japan is actively engaged in human resource development assistance and technical cooperation focusing on the ASEAN region.

The content of the concepts mentioned in paragraph 3 of the resolution

The confirmation of the applicability of international law and development of non-binding and voluntary norms of responsible state behaviour in cyberspace are the basis for ensuring stability and predictability of the international community.

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

With regard to the promotion of the rule of law, Japan urges the need for further elaboration of the deliberation about peacetime rules of international law, the law concerning the right of self-defence and international humanitarian law as well as the development of voluntary norms in the next Group of Governmental Experts. As for confidence-building measures and capacity-building, it is critical to promote the implementation of the recommendations contained in the Group's reports by each State and region. Study on ways to lead tangible cooperation is necessary.

Jordan

[Original: Arabic]
[2 May 2016]

Information and communications technology has become essential to our daily lives. It promotes the social, cultural and economic growth and development of local communities in various ways, and has numerous implications for the interaction of individuals with their local communities and with the wider world.

The extremely rapid progress of information and communications technology makes it vulnerable to risks and challenges. Those risks must be addressed through both technological and legal means with a view to finding effective and practical solutions that reduce risks and avert potentially catastrophic consequences.

The Jordanian Army has played an active and influential role in promoting security and peace at the national, regional and global levels through the development of technology that it employs to secure information and both wired and wireless communication, including the following:

(a) It has updated its communications and information systems by installing protected networks that use encrypted IP technology all over the Kingdom, including at the borders, which it uses to strengthen national and regional security;

(b) It engages in security cooperation with the international community using communications systems that are compatible with those used by the North Atlantic Treaty Organization and the United States Army, and that meet type 1 international encryption standards;

(c) It has improved its technical capacities by acquiring an infrastructure-independent communications system for use in maintaining national security in conflict zones, refugee camps and remote areas. The Jordanian Army also uses that technology in support of peacekeeping operations in conflict zones around the world;

(d) It trains and certifies all communications systems users and maintenance and support personnel without relying on the supplier company, in order to ensure optimum reliability and dependability at all times;

(e) The highest command-and-control standards are applied to all systems used by the military in order to raise the level of national and regional security coordination and cooperation;

(f) It takes active part in international conferences and keeps abreast of their outcomes in order to increase complementarity between friendly armies, avoid interference between communications systems used by neighbouring States in the region, and ensure coordinated control and surveillance at international borders.

Focus should always be placed on citizen awareness of pervasive cyberthreats and how cybersecurity measures when using electronic systems can minimize and counteract those threats. Heightened security awareness while handling any kind of information should not interfere with the benefits of technology.

The following measures have been taken to protect vital national information networks:

(a) Encryption is used for all voice, data and video communications systems;

(b) Closed networks (intranets) are used;

(c) Links with other security agencies are established through stand-alone peripheral devices;

(d) Information and communications security measures and the “need to know” principle are applied. Access permissions and user identities are checked continually;

(e) Virtual networks are used whereby the user interacts with a screen linked to the network on the basis of access permissions for access to information. Access or connection many not be done via other devices, such as flash drives;

(f) Jordan has enacted the following cybersecurity legislation:

(1) A law on cybercrimes has been enacted;

(2) A law on electronic transactions has been enacted;

(3) A national cybersecurity and protection strategy has been drafted;

(4) National cybersecurity and protection policies have been drafted;

(5) A national cybersecurity and protection strategy was approved by the Cabinet in 2012.

We propose the following global measures:

(a) Communications networks and information should be classified by importance;

(b) Cybersecurity and protection measures should be implemented;

(c) The need-to-know principle should be applied;

(d) Technical measures such as encryption and frequency-hopping should be employed;

(e) Users and network access permissions should be verified and categorized;

(f) Networks should be linked by stand-alone peripheral devices;

(g) Within certain networks, closed intranets should be used, and the World Wide Web should be avoided where possible;

(h) The United Nations intranet should be enhanced and kept separate from public networks. It should be protected through technical and security measures such as encryption, safeguards and verification of access permissions;

(i) Cooperation should be promoted among computer emergency response teams to follow-up breaches, install safeguards and address gaps;

(j) Security measures and procedures for addressing breaches should be circulated.

We stress the potential of information and communications technology to advance sustainable development, especially in poorer and more remote areas, in the following ways:

(a) It can accelerate poverty eradication, for example, through mobile banking, which has brought direct and tangible benefits to millions of people around the world who have no banking experience.

(b) Modern technology and new communications media can mitigate the impact of famines by providing crucial information to farmers about which crops to cultivate.

Recommendations:

(a) International response and recovery teams should be formed to address cybersecurity incidents, crises and disasters;

(b) A Jordanian representative should be included in the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security scheduled to be formed in 2016;

(c) Scientific and research cooperation and training exchanges among the members of the Security Council should be increased.

Lebanon

[Original: Arabic]
[24 May 2016]

In the modern age, cybersecurity affects a range of economic, social, political, military and humanitarian issues. Cyberterrorism will be one of the most serious future threats to superpowers and developing States alike.

The cyberwar is being fought on a number of fronts, including the following: recruitment and mobilization websites; psychological warfare; information exchange and dissemination via the Internet; electronic hacking of websites, data and information systems; and cyberterrorism.

The threat of cyberterrorism is on the rise in all States. Lebanon has been the victim of a number of cyberattacks aimed primarily at the banking sector (the Gauss virus) and the communications sector. Most e-services are regularly subject to attack.

National efforts to promote cybersecurity and international cooperation include the following:

- In 1999, Law No. 140 on the confidentiality of telecommunications and Law No. 75 on intellectual property were enacted. Both address software piracy to some degree.
- In 2006, the criminal investigations division of the Directorate-General of the Internal Security Forces created an office to combat cybercrime and protect intellectual property.
- In 2007, a Communications Regulatory Authority was established, and it has become an active member of the International Multilateral Partnership against Cyber Threats (IMPACT).
- In 2009, the Army Command established an electronic forensics division within the Intelligence Directorate.
- The Ministry of National Defence is working to establish a Lebanese computer incident response team (LEBCIRT) in collaboration with national and global bodies. It has been taking part in all the relevant initiatives and holding conferences and training courses.
- In 2012, the Cabinet issued a decision to establish a national security committee to host Government websites. The committee includes a representative from the Ministry of National Defence.
- In 2013, the Cabinet formed a committee to study the threat posed by Israeli enemy communications towers facing Lebanese territory. That committee was chaired by the Ministry of National Defence and included the other relevant ministries.
- In 2015, the Lebanese Army created a dedicated cybersecurity division.
- Parliament is currently considering a draft law on electronic transactions.

Measures that could be taken by the international community to strengthen cybersecurity at the global level include the following:

- Resolutions adopted by the United Nations and the World Summit on the Information Society aimed at disseminating a culture of information should be complied with, and a cooperation framework should be established with the relevant international bodies to ensure sharing of information and best practices.
- National laws and regulations on combating information crimes should be harmonized with global rules, with a view to preventing digital havens.

- A global system should be established to manage information crises. Robust international legislation should be adopted to reinforce the capacity of national laws to address the global and international nature of cybercrime.

Poland

[Original: English]
[18 July 2016]

1. General opinion

Cybersecurity is vital for maintaining economic growth and the functioning of civil society. Cyberattacks can affect not only the private sector and public administration, but also industrial automation systems in critical infrastructure facilities.

Ensuring a coherent system of information and telecommunication security is necessary in light of the nature of the threats and the growing dependence of businesses, administration and society on information technology. All stakeholders, including the State, business and non-governmental organizations must be involved and contribute to cybersecurity.

Respect for international law and norms are a necessary condition for maintaining peace and security between States in cyberspace.

Enhancing national capabilities is the key element in strengthening international security in cyberspace.

Expanding confidence in cyberspace will have a positive impact on relations between States in other areas.

Human rights and fundamental freedoms should be equally protected in cyberspace and in the real world. Respect for fundamental freedoms on the Internet is essential for democratic society, sustainable growth and prosperity.

2. National initiatives to strengthen cybersecurity and international cooperation

The Polish system of cybersecurity is based on a network of institutions. It is based on the cooperation of entities, both in the civil and military dimensions and in the sphere related to cybercrime.

The Polish Government is advancing its efforts to develop a national cybersecurity strategy and national cybersecurity law. The key elements of the Polish cybersecurity system will include procedures, people and technology.

Last year, Poland hosted several major international events that contributed to the promotion of international cooperation: the SECURE 2015 Conference, the European Cybersecurity Forum (cybersecforum.eu) and the International Conference on Cyber Security on safety and security beyond borders.

3. Possible measures that could be taken to strengthen cybersecurity at the global level

It is necessary to further develop confidence-building measures in the field of cyberspace implemented globally, regionally and nationally.

The international community should encourage to build national capabilities in the area of cybersecurity.

It is important to deepen bilateral and regional cooperation. A good example of regional efforts is the Central European Cyber Security Platform, comprised of Poland, the Czech Republic, Slovakia, Hungary and Austria.

International exercises in the field of cybersecurity allow for better understanding of the nature of threats and means of responding to them. The Cyber Europe or North Atlantic Treaty Organization's Locked Shields exercises are a case in point.

One should not underestimate the value of involvement in the international dialogue of stakeholders representing non-governmental organizations, business and academia.

Portugal

[Original: English]
[31 May 2016]

General Assembly resolution 70/237 on "Developments in the field of information and telecommunications in the context of international security" recalls the importance of science and technology in this context, recognizing that the developments in those areas can have civil and military applications. If the progress in the fields of information and telecommunications means the increasing of opportunities to the development of knowledge, the cooperation among States, the promotion of human creativity and the circulation of information in the community as a whole, on the other hand we find that those technologies and means can potentially be used in ways contrary to international stability and security, and may negatively affect the national integrity of States.

Resolution 70/237 requires the contribution of the Member States in what concerns four areas, recalling the report of the 2015 Group of Governmental Experts:

(a) General appreciation of the issues of information security;

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

(c) The content of the concepts aimed at strengthening the security of global information and telecommunications systems;

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

The report contained in document A/68/98 presents some recommendations regarding the following areas: recommendations on norms, rules, and principles of responsible behaviour by States; recommendations on confidence-building measures and the exchange of information; recommendations on capacity-building measures.

Following those recommendations, Portugal presents the following comments.

I. Norms, rules and principles that characterize the responsible behaviour of States

1. Portugal considers that the security in the network information is important and has been growing.

2. We must highlight the progress in the efforts to implement legislation on networks' security and integrity, by adopting risk assessment methods, which demand the adoption of adequate cooperative security measures, at technical and organizational levels, and the requirement of reporting security violations or integrity loss, which have a significant impact on the functioning of services.

3. At the level of concepts it is important to reinforce the idea that regulation should primarily stem from international rules.

4. At the international level it is important to reinforce information-sharing and the realization of training field exercises in border areas.

II. Measures of confidence reinforcement and information-sharing

1. It is crucial to promote information-sharing between all the stakeholders (both public and private), taking into account the wider context of globalization.

2. At the national level, our efforts have been focused on the accomplishment of joint exercises in which public and private entities took part, in the promotion of technical standardization and in the organization of conferences and seminars, some of them with the participation of international speakers.

III. Measures of capacity-building

1. It is important to develop measures on capacity-building. Nevertheless, there are difficulties related to the training and maintenance of human resources connected to these activities.

2. There is a need to facilitate the access of knowledge and to promote collective training regarding several aspects, including security, between all the major stakeholders.

Serbia

[Original: English]
[31 May 2016]

Understanding the great importance of assuring and developing information security, this area is recognized in the Republic of Serbia as one of the strategic priorities in the information society field.

The National Assembly of the Republic of Serbia adopted the Law on Information Security in January 2016. The Law established the competent authority for information security, with tasks to prepare regulations in accordance with national and international standards, cooperate with competent authorities of other countries, and conduct inspection on law enforcement. The Law defined the information and communications technology (ICT) systems of special importance in Serbia, for which operators will have to undertake adequate technical and organizational measures in order to ensure information security. These systems are: (a) ICT systems of public bodies; (b) ICT systems where sensitive personal data are handled; (c) ICT systems in the areas of public interest (energy, transport, gas, banking, health care and other).

The competent authority conducts international cooperation and especially provides alerts on risks and incidents which have one of these characteristics: (a) are growing rapidly or have a tendency to become high risks; (b) exceed national capacities; (c) may have an impact on more than one country.

The Law established National CERT within the Regulatory Agency for Electronic Communications and Postal Services, which will, among other duties, cooperate with similar organizations in other countries.

The Law also regulates cryptosecurity and protection against the compromising electromagnetic emanation.

In order to strengthen the security of global information and telecommunications systems, States should cooperate, especially by maintaining effective and responsive mechanisms for information exchange, alerts and announcements on cybersecurity incidents. For that purpose, States should appoint focal points and make contact information easy available. Special focus should be on the protection of critical infrastructure, especially if the incidents affect the territory of more than one State. The States should also cooperate on exchange of knowledge and education in this area.

Taking into account increased risks and characteristics of cyberattacks in the interconnected world, the international community should encourage the States to cooperate and make dialogues, to promote the building of mutual cybersecurity capacities and give support to international organizations who are designed for cooperation in the field of information security. Joint and effective cooperation will contribute to making the global ICT environment safer and protected, where the States and citizens are secured from various risks in the cyberworld.

Spain

[Original: Spanish]
[26 May 2016]

Spain considers that information and communications technologies (ICT) provide immense opportunities and continue to grow in importance for the international community. However, there are disturbing trends representing risks for international peace and security. States should therefore cooperate effectively in order to prevent harmful practices in cyberspace, and not knowingly allow their territory to be used to commit internationally wrongful acts using such technologies.

In July 2015, the National Cybersecurity Council approved nine plans stemming from the National Cybersecurity Plan to implement the measures set forth in the 2013 National Cybersecurity Strategy.

Spain participates actively in all strategic initiatives related to cybersecurity in the European Union, the Organization for Security and Cooperation in Europe, the North Atlantic Treaty Organization, the Council of Europe and the Organization for Economic Cooperation and Development.

In 2015, Spain joined the Freedom Online Coalition and the Global Forum on Cyber Expertise.

Spain supports the outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society, adopted in December 2015.

Increased connectivity, innovation and access to ICT have been instrumental in facilitating progress on the Millennium Development Goals. Spain considers that the process of the World Summit on the Information Society should be closely aligned with the 2030 Agenda for Sustainable Development, since access to ICT has also become a development indicator and an aspiration in and of itself.

Spain supports the process that aims to achieve an international consensus on cybersecurity, and considers that States should continue reflecting on how the principles and norms of international law, especially those relating to the threat or use of force, humanitarian law and protection of the fundamental rights and freedoms of individuals, should be interpreted and applied in cyberspace.

Spain supports the aspirations of the international community as to the peaceful use of ICT for the common good of humankind; it considers that the Charter applies in its entirety and that States have an inherent right to adopt measures consistent with international law to be able to respond in a timely, legitimate and proportionate manner to threats or attacks that may affect their national security.

Switzerland

[Original: English]
[7 June 2016]

1. General appreciation of the issues of information security

Information and communication technologies (ICTs) have become an indispensable driver of social, economic and political activities. Switzerland is committed to seizing the opportunities that are generated by the use of ICT. However, the use of ICT has exposed information and communication infrastructure to criminal, intelligence, politico-military or terrorist abuse of functional impairment. Disturbances, manipulation and specific attacks carried out via electronic networks are the risks that an information society entails.

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

In 2012, the Swiss Federal Government adopted the national strategy for the protection of Switzerland against cyberrisks (NCS), laying thereby the foundation for a comprehensive approach. The NCS seeks to improve the early detection of cyberrisks and emerging threats, make Swiss infrastructure as a whole more resilient to cyberattacks and generally reduce cyberrisks. The NCS also reflects the need for a culture of (cyber) security, shared responsibility of all participants and the need for a risk-based approach. It also advocates coordination at a governmental level, national (i.e. private-public partnership) and international cooperation. The strategy comprises 16 measures. The Swiss Federal Government has adopted a detailed plan for the implementation of the NCS in 2013.

3. The content of the concepts mentioned in paragraph 3 (of the resolution)

Cyberrisks have to be encountered by means of enhanced international cooperation (sphere of action 5 defined by the strategy). The Swiss foreign policy in the field of cybersecurity focuses on the development of norms of responsible State behaviour, confidence-building measures and capacity-building. With this in mind, Switzerland participates in different international processes. The Organization for Security and Cooperation in Europe (OSCE) has adopted confidence-building measures in the realm of cybersecurity. Switzerland considers this process as paramount. In addition, the London process constitutes a further important process within which Switzerland participates. Switzerland supports a range of projects designed to develop capacity-building.

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

All measures taken by the international community have to balance security considerations and human rights deliberations. The same rights people have offline must be guaranteed online as well. Measures designed to build trust and confidence need to be further developed. The set of confidence-building measures adopted by the OSCE is of paramount importance in order to strengthen security. Building transparency by exchanging information and enhancing cooperation through practical and joint activities will contribute to the overall stability of the cyberdomain.

Togo

[Original: French]
[2 June 2016]

Although the progress of information and telecommunications is an enormous asset for countries' development, it also represents a threat to national and international security. It is a virtual space that is often used for criminal or terrorist purposes.

Togo is not immune to this threat and is already experiencing crime related to information and communications technologies (ICT), ranging from scams and other types of fraud to child pornography and offences against the freedom and integrity of individuals.

In an age characterized by terrorism, the web and social media are used for propaganda and recruitment by terrorist organizations. Most countries are also migrating to electronic administration, representing a major challenge for our Governments, which face the prospect of cyberattacks that could undermine the functioning of administrations and civilian and military security.

It is therefore important to adopt measures at the national and international levels to regulate the ICT sector and ensure that it is not used for criminal purposes.

In Togo, several measures have been taken in this connection, including:

- Issuance of Decree No. 2011-120/PR of 6 July 2011 on the systematic and mandatory identification of subscribers to telecommunications services;

- Adoption of Act No. 2012-018 on electronic communications and Act No. 2013-003 to amend Act No. 2012-018;
- Preparation of draft legislation on cybercrime, cryptography, cybersecurity, protection of personal data, and electronic transactions.

The purpose of these instruments is to ensure the traceability of all ICT activities and to establish a security mechanism to protect ICT networks against fraudulent intrusion.

Togo has also found it necessary to establish an institutional oversight framework. In this connection, it has established a computer emergency response team responsible for cybersecurity at the national level, to complement the Post and Telecommunications Regulatory Authority.

Human capacity is also being enhanced to enable law enforcement agencies and public and private entities involved in cybersecurity to take effective action against any kind of threat.

Lastly, international cooperation, including through the International Telecommunications Union and the United Nations, will help to bolster information and telecommunications security.

Turkmenistan

[Original: Russian]
[28 March 2016]

Neutrality is the foundation of Turkmenistan's domestic and foreign policy, based on the close relationship between national interests, global security and shared progress. A key element for Turkmenistan, arising from its neutral status and international obligations, is the peace-loving nature of its foreign policy. Accordingly, all matters are addressed exclusively through political and diplomatic channels, primarily the United Nations and other international organizations. Turkmenistan fully supports international efforts to combat the proliferation of weapons of mass destruction, their means of delivery and related technologies, and it advocates disarmament as a prerequisite for global security. In its legislation, Turkmenistan proclaims its refusal to possess, manufacture, store or transport nuclear, chemical, bacteriological and other types of weapons of mass destruction, including new types of such weapons or technologies for their production.

Turkmenistan has acceded to a number of international disarmament instruments whose main purpose is to encourage States parties to maintain global peace, harmony and security.

Attaching particular importance to strengthening international peace and security, Turkmenistan calls for a reduction in the number of arms in the belief that the fewer weapons there are in the world, the steadier and calmer its development will be and the greater the trust and understanding among countries and peoples. Turkmenistan's foreign policy framework document for 2013 to 2017 emphasizes that Turkmenistan will continue to actively promote disarmament processes and the reduction of weapons arsenals, primarily weapons of mass destruction.

In his speech at the meeting of the Cabinet of Ministers on 5 June 2015, the President of Turkmenistan drew special attention to our country's international obligations to the global community. He emphasized that neutrality means non-adherence to political, economic or military unions and blocs; having our own army with sufficient troop strength to protect the nation's peace and freedom; rejecting weapons of mass destruction and prohibiting such weapons from entering our national territory and air space; committing to universal human values and democratic principles, and safeguarding civic harmony and peace within the country; and conducting domestic and foreign policy in close cooperation with the United Nations and humanitarian international organizations.

At the sixty-ninth session of the General Assembly on 3 June 2015, resolution 69/285 on the permanent neutrality of Turkmenistan was unanimously adopted by 193 States. This clearly illustrates the universal recognition of our country's effective policy to safeguard regional and international peace, security and sustainable development. The resolution underscores the important contribution of permanent neutrality in Turkmenistan to the strengthening of peace and security in the region, and to the development of friendly and mutually beneficial relations with the countries of the world.

As the host country of the United Nations Regional Centre for Preventive Diplomacy for Central Asia, Turkmenistan calls for that body to be more engaged in various aspects of regional issues with the support of States Members of the United Nations and other organizations (including the Organization for Security and Cooperation in Europe, the European Union and the Commonwealth of Independent States).

An international forum on safeguarding peace, stability and security in the Central Asian region was successfully held in Ashgabat in 2015. As a party to international treaties, United Nations conventions and multilateral instruments in the field of disarmament, Turkmenistan intends to continue to do its utmost to facilitate these processes, first and foremost at the regional level, and aims for Turkmenistan to hold regular regional meetings on disarmament issues in Central Asia.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[31 May 2016]

The United Kingdom welcomes the opportunity to respond to General Assembly resolution 70/237, entitled "Developments in the field of information and telecommunications in the context of international security", which builds on its response to resolution 69/28 in 2015. The United Kingdom uses its preferred terminology of "cybersecurity" and related concepts throughout its response, to avoid confusion given the different interpretations of the term "information security" in this context.

The United Kingdom recognizes that cyberspace is a fundamental element of critical national and international infrastructure and an essential foundation for economic and social activity online. The United Kingdom makes reference to the 2015 National Security Risk Assessment that confirmed cyber continues to be a Tier I threat to national security. The United Kingdom's allocated funding of £860 million during the life of the previous National Cyber Security Strategy (2011-2016) will be supported by an additional allocation of £1.9 billion over the next five years. A new

National Cyber Security Strategy will be published in 2016, including the establishment of a new National Cyber Security Centre.

The United Kingdom recognizes that international collaboration is central to successful cybersecurity. We continue to promote a free, open, peaceful and secure cyberspace so its economic and social benefits are protected and available for all. The United Kingdom takes a lead on cross-border cybersecurity challenges through initiatives such as the WePROTECT Global Alliance to End Online Child Sexual Exploitation. We are also committed to sharing best practices internationally and to ensuring that the global community has access to assistance in developing their cybersecurity capabilities.

The United Kingdom continues to participate actively and constructively in the international debate on cybersecurity. We have provided experts for all four United Nations Groups of Governmental Experts and consider that the consensus report of the last Group made valuable progress in reaffirming that international law is applicable in cyberspace and that States' adherence to international law, in particular their United Nations Charter obligations, is an essential framework for their actions in their use of information and communications technologies.

The United Kingdom also welcomes continued discussion of potential future confidence-building measures in cyberspace at the Organization for Security and Cooperation in Europe and similar work in other regional organizations.

The United Kingdom is pleased to be actively engaged on these important issues and looks forward to further participation in strengthening capability and international cooperation on cybersecurity.