United Nations A/72/315

General Assembly

Distr.: General
11 August 2017
English:
Original: Arabic/English/French/
Russian/Spanish

Seventy-second session
Item 95 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/72/150.

17-13876 (E) 280817

I. Introduction

1. On 5 December 2016, the General Assembly adopted resolution 71/28 on developments in the field of information and telecommunications in the context of international security. In paragraph 3 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 2 of the resolution;

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

2. Pursuant to that request, on 16 February 2017 a note verbale was sent to all Member States inviting them to provide information on the subject, followed by a further note verbale dated 12 June 2017. The replies received at the time of reporting are contained in section II. Additional replies received after 31 July 2017 will be posted on the website of the Office for Disarmament Affairs (www.un.org/disarmament/) in the original language.

II. Replies received from Governments

Afghanistan

[Original: English]
[26 May 2017]

The Ministry of Communications and Information Technology of the Islamic Republic of Afghanistan has reported the following in reference to operative paragraph 3 of General Assembly resolution 71/28 on developments in the field of information and telecommunications in the context of international security.

Achievements

To promote the international security of information technology and the authenticity of electronic transactions, the Ministry of Communications and Information Technology has established a public key infrastructure device. The Ministry has also created the NOC system and intends to connect this system with the system of the Member States for identification and verification purposes of the ongoing statistics and data flow on the Internet.

The Ministry has drafted cybercrime laws and has sent them to the Ministry of Justice for consideration. For fundamental solutions, in light of these laws, more secure electronic deals can be made and cybercrime can be prevented.

The Ministry has created a national cyberstrategy to exchange secure information, establish an information technology security framework for the NIXA project that will be implemented by the Ministry, and address and identify cybercrime.

Proposals

The Ministry of Communications and Information Technology requests the developed countries that have cyberpolice to assist and cooperate with the Ministry in the establishment of the cyberpolice.

To address cybercrimes and to fight seriously against this phenomenon a coherent system (conducive for criminal information) should be established at the international level.

One of the important solutions for the security of the Internet is to establish Internet governance. Through Internet governance, a basis can be provided for the exchange of confidential information and data between all departments and offices of the Government for the implementation of the network mentioned above. In this regard, the Ministry requests the cooperation of all Member States.

The Ministry also requests Member States to support the staff of the Ministry to fight cybercrime and improve information security, by providing them with vocational and technical training programmes.

Armenia

[Original: English]
[31 May 2017]

General appreciation of the issues of information security

Given the pace of e-society development in the Republic of Armenia, issues related to information security are acquiring significant relevance, having a huge impact on all aspects of national security.

The trends in information and communications technology (ICT) pose qualitatively new threats and challenges requiring systematic coordination and new approaches to ensure the secure use of ICT. Taking into account the use of "information warfare" techniques in different conflict environments, Armenia attaches vast importance to ensuring information security for the maintenance of international peace and security.

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

Armenia has undertaken activities aimed at safeguarding State and public interests in the field of information security and harmonization of relevant legislation with international standards. A series of normative acts governing the sphere have entered into force, including the national security strategy and the information security concept, as well as laws on the fight against terrorism; State and official secrets; electronic documents and digital signatures; personal data protection; freedom of information; and the mass media.

Pursuant to the relevant decisions of the Government:

(a) A number of practical measures were taken to ensure the protection of publicly accessible information of government bodies on the Internet and provide a secure connection of their information systems to the Internet;

(b) Minimum requirements for official Internet websites of government bodies were adopted.

Armenia has approved and applied a set of ISO standards related to information security. In October 2006, the Council of Europe Convention on Cybercrime was ratified and appropriate amendments to the national legislation followed.

Armenia actively engages in relevant programmes, training courses and cooperative initiatives carried out within different international frameworks, such as the Commonwealth of Independent States, the Collective Security Treaty Organization, the European Union and the North Atlantic Treaty Organization. In particular, in 2016 the two-stage "Cyber-antiterror" joint exercise of member States of the Commonwealth of Independent States was held. A draft "Agreement on cooperation among CSTO member States in the field of ensuring information security" was proposed for domestic interdepartmental approval earlier in 2017.

The content of the concepts mentioned in paragraph 2

The Republic of Armenia information security concept defines the term "information security" as "the protection of national interests in the information sphere, which is linked to the entirety of the balanced interests of individuals, society and the State".

Taking into account the rapid development of information and communications technology, an inter-agency working group has been established to draft a renewed concept on ensuring information security and information policy in the Republic of Armenia in late 2017.

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

Armenia underlines the importance of enhanced and effective international cooperation on information security issues, emphasizing the role of the International Telecommunication Union.

Belarus

[Original: Russian]
[5 June 2017]

General appreciation of the issues of information security

The current state of international information security is unsatisfactory. There are attempts being made to use information technology for political purposes.

Belarus has a number of distinctive information security issues:

(a) Insufficient protection of the national segment from exposure to distributed denial-of-service (DDoS) at the level of backbone providers and domestic providers, and even hosting platforms;

(b) The potential for undeclared capabilities and vulnerabilities to appear in information security products and a lack of capacity for detecting them in a timely fashion, which often undermines the impact of measures to protect information;

(c) The threat of intruders attacking critical infrastructure and information technology infrastructure, such as power supply systems and automated systems for managing production and transport.

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

Such efforts include:

(a) Work across the entire system to update requirements as regards technical and cryptographic protection of information, whose dissemination and/or provision is restricted;

(b) The organization and application of technical norms and standards pertaining to the technical and cryptographic protection of information;

(c) The implementation of information exchange agreements with leading information security companies;

(d) Regular cooperation with State bodies and organizations to facilitate prompt responses to specific information security incidents;

(e) Maintenance by countries themselves of their own malware-detection packages;

(f) Collaboration with countries of the Collective Security Treaty Organization through the consultative coordination centre.

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

A key approach of Belarus to international information security is related to the need to prevent the possible misuse of information and communications technology (ICT) so as to undermine national security and stability and international security.

Belarus actively takes part in discussions about international information security in forums of various international organizations, including the United Nations, the Collective Security Treaty Organization and the Organization for Security and Cooperation in Europe.

Belarus supports the initiative to adopt a universal instrument on international information security within the United Nations.

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

At the international level, it is crucial to gradually advance the principle of non-interference in the internal affairs of sovereign States and mutual rejection of aggressive actions in the information sphere. Such steps should principally be achieved through support of the information sovereignty of United Nations Member States for the purpose of:

(a) Upholding citizens' rights to receive, store and disseminate complete, reliable and timely information;

(b) Developing an information society in which United Nations Member States participate in global information relationships on an equal basis;

(c) Ensuring effective information management of an intergovernmental policy to prevent the proliferation of terrorist and extremist ideas;

(d) Ensuring the resilient operation of critical infrastructure.

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

(a) Develop mechanisms for international cooperation, as provided for in current and future instruments of international law;

(b) Build effective cooperation between the international community and multinational corporations that control the overwhelming majority of ICT, in order to identify and block the sources of threats to information security.

Brunei Darussalam

[Original: English]
[29 June 2017]

Brunei Darussalam recognizes that global trends have shifted with increasingly prominent developments in the field of information and telecommunications. At the same time, this has also introduced new threats and challenges in the form of hacking, cybercrimes and cyberterrorism, which endanger vital infrastructures, networks and services worldwide. Its transnational and intangible nature requires collaborative efforts from the global community to build a secure and trusted online environment.

On a national scale, under the auspices of the National Security Committee, the country maintains strong cooperative ties with a host of local security agencies to manage internal cybersecurity threats. The Brunei national computer emergency response team was established in May 2004 and became the nation's one-stop referral agency in dealing with computer- and Internet-related security incidents. Through a global affiliation with other computer emergency response teams, the national team acquires valuable information on security threats to information and communications technology (ICT) and shares findings on security risks detected within the nation's ICT infrastructure.

Brunei Darussalam is committed to working with regional and international partners to constantly maintain a state of readiness in the face of major international cyberthreats. Within the regional architecture of the Association of Southeast Asian Nations (ASEAN), Brunei Darussalam will participate in the ADMM-Plus Expert Working Group on Cyber Security, which brings 18 countries together to promote practical and effective cooperation and to enhance capacity in protecting the region's cyberspace and addressing challenges to cybersecurity.

Threats in all cyberlandscapes, including that of cloud computing and mobile systems, are recognized by the Government and represent a major part of the security and defence priorities of Brunei Darussalam.

Canada

[Original: English]
[17 July 2017]

On cyberissues, Canada believes that:

(a) A free, open and secure cyberspace is critical to promoting security, prosperity and human rights;

(b) Existing international law is applicable to the use of information and communications technology by States;

(c) Promoting peacetime norms helps sustain an environment in which responsible behaviour guides State actions;

(d) Practical confidence-building measures are a proven method to reduce the risk of armed conflict.

At the national level, the Government released its cybersecurity strategy in 2010, which focused on securing the cybersystems of Canada and protecting Canadians online. The Government recently finalized a review of existing cybersecurity measures. On this basis, the country's new approach to cybersecurity is set to be released in late 2017.

The 2017 defence policy includes new investments and policy direction to better leverage cybercapabilities in support of military operations. The Canadian Forces' active cybercapability will be subject to the same rigour as other military tools, including applicable domestic and international law and rules of engagement.

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

(a) It continues to promote the development of peacetime norms for State behaviour in cyberspace, including the outcomes of the 2012-2013 and 2014-2015 Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security;

(b) It ratified the Council of Europe Convention on Cybercrime (Budapest Convention) in July 2015. Canada encourages countries to become parties to the Convention, or to use it as a model as they design their own cybercrime law;

(c) Since 2007, it has committed $11 million to support cybersecurity capacity-building projects;

(d) It is working with the United States of America to implement the Canada-United States cybersecurity action plan, which aims to enhance the resilience of its cyber infrastructure;

(e) It has been working on implementing 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;

(f) It supports efforts of the North Atlantic Treaty Organization to strengthen the cyberdefence of the Organization and that of individual allies.

Cuba

[Original: Spanish]
[5 April 2017]

As stated in General Assembly resolution 71/28, scientific and technological developments can have both civilian and military applications, and these developments must be prevented from affecting international security.

Measures are needed to promote, at multilateral levels, the consideration of existing and potential threats in the field of information security, as well as possible strategies to prevent and address them.

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

Cuba supports the work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, established pursuant to resolution 58/32, in which a Cuban expert participates.

We consider it necessary to establish a legally binding international regulatory framework which is complementary to existing international law but applies to information and communications technologies.

Information and telecommunications systems can be turned into weapons when they are designed or used to inflict damage on the infrastructure of a State. All States must respect existing international standards in this field. Access to the information or telecommunications systems of another State should be in line with the international cooperation agreements concluded and should be based on the principle of consent of the State concerned. The nature and scope of exchanges must respect the laws of the State which is granting access.

The hostile use of telecommunications with the overt or covert intention of undermining the legal and political system of States is a violation of internationally recognized norms in this field and constitutes an illegal and irresponsible use of those means. Such use can give rise to tensions and situations that are not conducive to international peace and security and can adversely affect the integrity of State infrastructure to the detriment of its security in both the civilian and military fields.

Cuba reiterates its concern at 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.

Through illegal radio and television broadcasts, the United States has been constantly attacking Cuban airwaves, disseminating programming specifically designed to incite the overthrow of the constitutional order established by the Cuban people. In 2016, illegal broadcasts averaging 1,875 hours per week were transmitted against Cuba, using 25 frequencies, from United States territory. The constant radio and television broadcasts transmitted by the United States against Cuba contravene the purposes and principles of the Charter of the United Nations, international law and the regulations of the International Telecommunication Union.

Once again, Cuba calls for an immediate end to these aggressive policies which violate the sovereignty of Cuba and which are, furthermore, incompatible with the development of ties based on mutual respect and cooperation between States.

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.

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 in their levels of development, to practice tolerance and to live together in peace with one another as good neighbours.

At the fifth Summit of CELAC, held in Punta Cana, Dominican Republic, 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.

Cuba reiterates that international cooperation is essential to tackle the dangers associated with the misuse of information and communications technologies. Cuba

also emphasizes that the International Telecommunication Union has an important role to play in the intergovernmental debate on cybersecurity issues.

Ecuador

[Original: Spanish]
[28 July 2017]

Ecuador considers that security in international relations must be based on trust and respect among States. The continuing revelations about massive and indiscriminate systems of espionage that are being used to monitor the communications of all citizens all over the world, as well as the use of information and communications technologies in a manner that violates international law, infringe the principles of respect for sovereignty and non-interference in the internal affairs of States. Moreover, those actions inject a serious element of instability into the relations between States and therefore affect international security. These systems of espionage also violate various fundamental human rights.

For that reason, Ecuador supports the efforts made to continue studying existing and potential threats in the field of information security and possible cooperative measures to address them, as well as the way in which international law should be applied to the use of information and communications technologies by States, and also the norms, rules and principles of responsible State behaviour in this area.

El Salvador

[Original: Spanish]
[24 May 2017]

In compliance with its obligations to the United Nations, El Salvador has the honour to report, in connection with General Assembly resolution 71/28 on developments in the field of information and telecommunications in the context of international security, that, in 2016, the El Salvador Armed Forces acquired a system for encrypting institutional documentation in order to strengthen information security. The system is in the process of being implemented.

Estonia

[Original: English]
[31 May 2017]

Estonia recognizes that security in the cyberworld has become a very important issue in the context of wider international security. The role and involvement of the United Nations is therefore becoming increasingly relevant.

Security on the Internet has been one of the high priorities of the Estonian Government. The main guiding document on this issue is the national cybersecurity strategy (2014-2017). The Cyber Security Council of the Security Committee of the Government supports strategic-level inter-agency cooperation and oversees the implementation of the objectives of the cybersecurity strategy. The Cooperative Cyber Defence Centre of Excellence of the North Atlantic Treaty Organization was established in Tallinn and as of May 30th 2017, it has 20 contributing Member States.

Estonia is convinced that the broad use of digital services demands a high level of cybersecurity. For Estonia, the socioeconomic and politico-military aspects

of cyber security are intertwined. Estonia considers it elementary that countries abstain from attacking national critical infrastructure. Estonia also call for responsible behaviour towards the global communications infrastructure to promote access to information and trust towards information and communications technology (ICT). It considers it a responsibility of every country to draft and enforce national laws that help control malicious uses of ICT by non-State actors and to seek ways to better formulate, disseminate and promote responsible and active cyberpolicies, narratives and argumentation.

Estonia is a member of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security for the fourth consecutive time. The Group has served as a very productive forum. In the future, it could be a useful instrument with regard not only to studying cyberthreats and possible remedies but to understanding how different countries implement existing international law and norms, rules and principles. In the view of Estonia, the Group should continue its work on advancing dialogue among Member States, which facilitates the exchange of information and best practices. In addition, it should discuss practical cooperation measures and mechanisms to advance the capacity-building of Member States, with the ultimate goal of equipping Member States with the competence and capacity to tackle all aspects of Internet challenges.

It is important to advance the progress achieved at the 2014-2015 meetings of the Group of Governmental Experts by further promoting norms of State behaviour that support openness, accountability and other democratic values in cyberspace. Estonia hopes to see yet another consensus report from the Group in June 2017.

Finland

[Original: English]
[21 July 2017]

Finland welcomes the opportunity to report on the implementation of General Assembly resolution 71/28.

Efforts made at the national level include the following:

(a) The national cybersecurity strategy (2013) and its updated implementation programme (2017) define key guidelines and actions in strengthening cybersecurity and resilience;

(b) Finland has established a National Cyber Security Centre and a Cybercrime Prevention Centre and appointed an Ambassador for Cyber Affairs in the Ministry of Foreign Affairs. The national information security strategy was adopted in 2016;

(c) Finland actively contributes to cooperation on cyberspace within the European Union;

(d) Finland supports various forms of information and communications technology for development and cyber-related capacity-building projects. It is a founding partner of the Global Forum on Cyber Expertise. In 2016, it joined the World Bank Digital Development Partnership trust fund. Finland supports Internet governance based on the multi-stakeholder model. It has been actively engaged in the World Summit on the Information Society and its follow-up process, including participating in the work of the Internet Governance Forum and financing it. The eighth Finnish Internet Forum took place in Helsinki in April 2017;

(e) Finland actively engages in dialogue on cyberissues in multilateral and regional forums and bilaterally. Within the Organization for Security and

Cooperation in Europe (OSCE), it works towards strengthening trust, security and stability in cyberspace and implements the agreed cyber confidence-building measures;

(f) Finland has endorsed the 2015 report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and participates actively in the work of the present Group. It has participated actively in the discussions on international law in cyberspace, for example, consultations on Tallinn Manual 2.0 and workshops organized by the United Nations Institute for Disarmament Research;

(g) Finland joined the Freedom Online Coalition in 2012 and contributes to the Digital Defenders Partnership. It organized the 2016 World Press Freedom Day conference, which was held in Helsinki;

(h) Finland is a party to the Council of Europe Convention on Cybercrime. A new strategic police plan (2015) targets resources at computerized crime prevention and the development pf cybersecurity know-how. There is also a comprehensive cybercrime prevention plan.

Priority areas for further work by the international community include:

(a) The work of the present Group of Governmental Experts, to which Finland attaches a lot of importance and to the success of which it is prepared to contribute, including further 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 within OSCE;

(c) Continuing support to cyber capacity-building to strengthen resilience and security in cyberspace;

(d) The multi-stakeholder dialogue, which Finland will continue to support and encourage, and the strengthening of public-private partnerships nationally and internationally.

Germany

[Original: English]
[30 May 2017]

The evolution of information and communication technology (ICT) offers numerous economic, social and scientific opportunities. Ensuring access to cyberspace and maintaining the integrity, authenticity and confidentiality of data in cyberspace have become vital issues of the twenty-first century.

In an increasingly interconnected world, States, critical infrastructures, businesses and individuals depend on the reliable functioning of ICT. The consequences of a misuse of ICT may not be limited to cyberspace. They can cause social, economic, political and other damage. For instance, attacks targeting State institutions or democratic and political processes can affect public order and safety.

Germany is addressing these challenges by promoting international law-abiding, norm-adhering and confidence-building State use of ICT at three levels:

(a) Globally, Germany is supporting efforts at agreeing how international law applies to State use of ICT and at developing voluntary non-binding norms, rules or principles of responsible State behaviour that aim at an open, secure, stable, accessible and peaceful ICT environment. Of particular importance in this context is the work of successive Groups of Governmental Experts on Developments in the

Field of Information and Telecommunications in the Context of International Security. German experts have actively participated in those Groups and Germany is committed to promoting their recommendations. Now is the time to widen the debate and involve the wider United Nations membership, with a view to universalizing the work on ICT in the context of international security. Germany supports a lead role for the United Nations and a strengthening of United Nations capacities in this field. Issues to be explored further include international information-sharing and cooperation on attributing cyberattacks. Clear and universally respected rules should address the malicious use of cybercapabilities as well as online espionage for economic purposes;

(b) At the regional level, confidence-building measures help to address the risk that ICT incidents may escalate into political or even military crises. At the Organization for Security and Cooperation in Europe (OSCE), Germany has for years been active in defining and implementing confidence-building measures aimed at security in and of State use of ICT. During the German chairmanship-in-office of OSCE in 2016, participating States agreed additional such measures. The 2016 OSCE Ministerial Council in Hamburg approved them and gave directions not only for their implementation, but also for further work to be undertaken. That needs to expand beyond politico-military aspects to multiple dimensions of security. Outside OSCE, Germany also supports similar efforts in regional organizations on other continents;

(c) Bilaterally, Germany maintains cyberdialogues and conducts regular cyberconsultations with multiple partners. Building on established partnership relations, Germany also supports the cybersecurity capacity-building efforts of other nations. When updating its cybersecurity strategy in November 2016, the German Government decided to work towards establishing a German institute for international cybersecurity, with a view to systematizing and increasing those efforts.

The efforts of Germany concerning information and telecommunications in the context of international security are part of intense work to promote ICT security overall. Recent national regulatory measures, such as the 2015 Information Technology Security Act and the 2016 overhaul of the national cybersecurity strategy are aimed at improving overall ICT security in Germany.

Greece

[Original: English]
[26 May 2017]

Within the framework of the Council of Europe, Greece has ratified by virtue of Law 4411/2016 (Government Gazette A΄ 142, 3 August 2016) the Council of Europe Convention on Cybercrime (Budapest, 23.11.2001) and the Additional Protocol to the Convention on Cybercrime concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (Strasbourg, 28 January 2003).

It should be noted that a process for integrating the European Union directive on security of network and information systems into national law is already in place. This directive is of paramount importance for enhancing resilience in the face of cyberattacks at the national level and sets a number of obligations for all European Union member States that are pertinent to this end and also includes the adoption of a national strategy on the security of network and information systems.

According to information provided by the Hellenic Ministry of Defence, the cybersecurity vision of Greece is to develop the full range of capabilities to defend

its national infrastructure and networks against the latest cyberthreats and cybercriminals. This includes addressing cyberdefence at the highest strategic level within the country's defence-related organizations, further integrating cyberdefence into operations and extending coverage to deployable networks. The following efforts have been undertaken at the national level to strengthen information security and promote international cooperation:

(a) A national cyberdefence strategy framework is currently under development, while the national cybersecurity strategy that regulates the general cybersecurity framework and defines the necessary actions for maintenance of the minimum requirements of cybersecurity is becoming a law;

(b) Cyberdefence is already part of the national defence operation plans, while the national emergency alert system has been incorporated into most policy documents referring to information systems and has been integrated into all major national exercises. Cybersecurity has been included in the operation plans for crisis periods in all public organizations;

(c) Greece has developed and continuously improves incident/emergency response capabilities under the Military Computer Incident Response Centre. Rapid reaction teams can deploy at short notice to help respond to and recover from cyberincidents in the military or public networks. Recovering instructions from faults or cyberattacks, have been integrated into computer information security policy documents;

(d) A cybersecurity operation centre for all national military defence network systems is under construction, while at national level there are four computer emergency response teams responsible for the public and private sectors.

Measures that could be taken by the international community, in order to achieve a higher level of information security are as follows:

(a) Increased incident response capabilities, network monitoring capabilities and actionable defence against cyberthreats through fully operational national cybersecurity operation centres;

(b) Full integration of cyberdefence into operations;

(c) Development of national cybersecurity/cyberdefence strategies;

(d) Enhanced cyberawareness of the personnel employed in cyberdefence and improvement of existing technical capabilities;

(e) Continuous training of the personnel employed in cyberdefence organizations;

(f) Harmonization of the national laws with the global cybersecurity laws and directives.

According to information provided by the Hellenic Police, the mission of the Cybercrime Division of the Hellenic Police, according to article 30 of presidential decree 178/2014, includes the prevention, investigation and prosecution of crimes committed through the Internet or other electronic communications media. The Cybercrime Division is an autonomous central service and is directly assigned to the chief of the Hellenic Police headquarters.

One of the units of the Division is responsible for the security of electronic and telephone communications and software and copyright protection. More specifically, the unit investigates cases of illegal penetration of computer systems and the theft, destruction or trafficking of software, digital data and audiovisual works throughout the country.

The Cybercrime Division of the Hellenic Police works in close cooperation with the National Authority against Electronic Attacks, which is part of the National Intelligence Service. The mission of the National Authority is to attend to the prevention of and to passively and actively counter electronic attacks against communication networks, data storage facilities and information and communications technology systems. In addition, the Authority is responsible for processing data and notifying the competent authorities.

Japan

[Original: English]
[27 July 2017]

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. Japan's efforts comply with the following five principles; free flow of information, rule of law, openness, self-governance and a multi-stakeholder approach.

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

Japanese efforts consist of the following three pillars; promoting the rule of law in cyberspace, confidence-building measures and capacity-building.

With regard to the promotion of the rule of law, Japan proactively contributes to international discussion to promote common understanding that the existing international law is applicable in cyberspace, as well as development of voluntary, non-binding norms. They are the basis for ensuring the stability and predictability of the international community. Given the unique characteristics of information and communications technology, further clarification is needed on how individual rules and principles would be applied.

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 their disposal. 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. Study of the ways to lead tangible cooperation is necessary.

With regard to capacity-building, Japan has been promoting the development of laws, statutes and policy frameworks for cybersecurity, and has been engaging in the assurance of cybersecurity of governmental bodies, CII operators; measures against cybercrime; human resources development to foster cybersecurity experts; and research and development of cybersecurity technologies. Based on these experiences and accumulated knowledge, Japan will further proactively cooperate on capacity-building.

Jordan

[Original: Arabic]
[23 March 2017]

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 country, including at the borders. It uses those networks 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 — the Arab 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 improve 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.

There should be a constant focus on citizen awareness of pervasive cyberthreats and how cybersecurity measures can minimize and counteract such threats to the use of electronic systems. When any kind of information is handled, it is essential to heighten security awareness, provided that such action does not prevent the technology from being put to good use.

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 should like to stress that information and communications technology has the potential 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 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security formed in 2003.

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

Madagascar

[Original: French]
[20 June 2017]

The recommendations of the United Nations are based on international security and envisage:

– Studies aimed at strengthening the security of global information and telecommunications systems;

– Evaluation of all existing and potential threats in the field of information security and the adoption of appropriate strategies to address this scourge;

– The engagement of State officials to strengthen information security, with a view to building a common understanding of security at the global level;

Resolution 71/28 specifically addresses information and telecommunications, which is a rapidly expanding field in Madagascar. Our response to this resolution requires input from experts in this field.

Netherlands

[Original: English]
[31 May 2017]

The Netherlands warmly welcomes the opportunity to offer its response to General Assembly resolution 71/28.

Cyberspace and especially the Internet are a critical resource for economic and societal growth. The increased importance of cyberspace has presented the global community with new challenges. Societies are highly interconnected and dependent on the Internet and information and communications technology and have become more vulnerable to the misuse of these technologies. Geopolitical tensions manifest themselves in cyberspace and States and other actors are increasingly using cyberoperations to pursue their strategic interests. However, those cyberoperations have the potential to cause instability in international relations and could present risks for international peace and security.

The need for international cooperation to reduce these risks is clear. In the light of the above, the Netherlands is stepping up its engagement in cyberdiplomacy to maintain peace and stability in cyberspace, promote the international legal order and foster a culture of collaborative security as stated in its international cyberstrategy, “Building digital bridges”.

The international community is taking steps to address these risks. The reports produced by the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security are of great importance in this regard. The Netherlands is also grateful for being in a position to contribute to the 2017 Group of Governmental Experts.

The Netherlands continues to promote an inclusive dialogue on responsible State behaviour in cyberspace, defends human rights online and fosters capacity building through various activities. Various efforts have been undertaken by the Netherlands, of which most notably:

(a) In the best tradition of support for the development of the international legal order, the Netherlands organized consultations between State legal advisers on the Tallinn Manual 2.0 on the International Law Applicable to Cyberoperations;

(b) The Netherlands supported the United Nations Institute for Disarmament Research in the organization of a series of three workshops on cybernorms, international law and countering the spread of malicious tools and techniques, successfully bringing together diplomats and the technical community;

(c) Last, the Netherlands launched numerous initiatives to foster guiding norms, including the Global Commission on the Stability of Cyberspace, which will develop proposals for norms and policies to enhance international security and stability.

All these efforts aim to make digitized international relations and cyberspace itself more stable and secure. The Netherlands believes that this is essential in order to reduce the risks of conflict and to maintain an open, free and secure cyberspace.

Norway

[Original: English]
[27 July 2017]

Norway is among the world's most digitalized countries and is increasingly dependent upon a well-functioning and secure cyberspace. It is firmly committed to a free, open, peaceful and secure cyberspace, so that its economic and social benefits are protected and available for all. Cyberspace knows no national boundaries and security in cyberspace can only be ensured on an international scale with close cooperation between States and the private sector.

Efforts taken to strengthen information security

National approaches

The Government has issued a white paper entitled "ICT security: a joint responsibility" (2016-2017) which includes plans for a national framework for improved coordination between the relevant actors at the national level and the establishment of a technical platform for improved sharing of information between public and private entities.

On 31 March 2017, the Combined Cyber Coordination Centre for the security and intelligence services was established.

International approaches

The Government has issued a white paper on global security challenges in its foreign policy (2014-2015), in which cyberthreats play a substantial part.

Norway is about to launch an international strategy for cyberspace for the country.

Norway takes part in several regional cooperation initiatives relevant to cyberissues, such as:

(a) Work within Organization for Security and Cooperation in Europe (OSCE) related to the development of norms and confidence-building measures to reduce the risk of conflict stemming from the use of information and communications technology (ICT);

(b) Close cooperation with the Cooperative Cyber Defence Centre of Excellence of the North Atlantic Treaty Organization in Tallinn, including the application of international law in the cyber domain and doctrine development;

(c) The Council of Europe Convention on Cybercrime.

Norway is supportive of the work of the Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Norway takes part in bilateral and regional dialogues on cyberissues, especially within the framework of the Nordic States.

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

Norway considers international law to be applicable in cyberspace and that State adherence to international law, in particular to obligations under the Charter of the United Nations, is an essential framework for their actions in their use of ICT. The international community needs to explore further the application of international law in the cyberdomain, as well as norms of responsible behaviour in cyberspace.

A sustainable global Internet depends on the right balance between openness, security, robustness and liberty. This can only be ensured through international cooperation and dialogue, globally and regionally. The ongoing work on this in forums such as the United Nations, the European Union, the Organization for Economic Cooperation and Development and OSCE should be continued.

Universal human rights also apply in the cyberdomain. The same rights that individuals have offline must also be protected online, in particular freedom of expression, including the freedom to seek, receive and impart information and the right to privacy.

Paraguay

[Original: Spanish]
[31 July 2017]

Paraguay agrees that information security is an area of growing importance at the global level as Governments increasingly rely on information and communications technologies and cyberspace. The response to the rise in cyberattacks must be concerted, robust and proportionate. Without a strategic response at the global level, a country's efforts in the area of cybersecurity will be unsustainable, sporadic, duplicative and inefficient.

To strengthen information security at the national level, in April 2017, the Government of Paraguay approved a national cybersecurity plan, which was prepared with the direct involvement of representatives of all sectors that have a role and interests in cyberspace. The plan serves as the basis for Government and national policies in this field and establishes the actions to be taken by Paraguay to strengthen the security of its critical assets and to achieve a secure, reliable and resilient cyberspace. Cybercrime is defined under Paraguayan criminal legislation. For the last five years, Paraguay has hosted the Ibero-American Information Security Conference and Fair, a forum to share experiences, learn about developments and assess solutions to the challenges generated by the growth in the use of information and communications technologies.

At the subregional level, the Southern Common Market (MERCOSUR) has a permanent body, the MERCOSUR Meeting of Authorities on Information Security and Privacy and Technological Infrastructure, which proposes common policies and initiatives relating to cybersecurity. Moreover, the Americas region has a comprehensive inter-American cybersecurity strategy, which recognizes the need for all participants in information systems and networks to be aware of their roles

and responsibilities with regard to security, in order to create a culture of cybersecurity.

The establishment of an effective framework for the protection of information networks and systems on a global scale, including the Internet, and for incident response and recovery is dependent on the international community taking the following measures:

– Provide information to users to enable them to protect their information systems against threats and vulnerabilities

– Foster public and private partnerships to promote education and awareness-raising

– Identify and assess technical standards and best practices to ensure the security of the information transmitted by communications networks and promote their adoption

– Promote the adoption of policies and legislation on cybercrime to protect users and to prevent and discourage the inappropriate and illicit use of computer equipment, while respecting the privacy rights of users.

Portugal

[Original: English]
[27 July 2017]

In General Assembly resolution 71/28 on developments in the field of information and telecommunications in the context of international security, the Assembly recalled the importance of science and technology in this context, recognizing that developments in those areas can have civil and military applications. Progress in the fields of information and telecommunications means increasing opportunities for the development of knowledge, cooperation among States, the promotion of human creativity and the circulation of information in the community as a whole; on the other hand Portugal finds 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.

In resolution 71/28 Member States were requested to provide information in four areas:

(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 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.

In its 2013 report (A/68/98), the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security presents some recommendations regarding the following areas: norms, rules and principles of responsible behaviour by States; confidence-building measures and the exchange of information; and capacity-building measures.

Following those recommendations, Portugal presents the following comments.

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

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

It is important to highlight progress in the efforts to implement legislation on network security and integrity by adopting risk assessment methods, which demand the adoption of adequate cooperative security measures at technical and organizational levels and include the requirement of reporting security violations or loss of integrity that have a significant impact on the functioning of services.

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

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

Measures of confidence reinforcement and information-sharing

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

At the national level, Portugal's 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.

Measures of capacity-building

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

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

Qatar

[Original: English]
[4 May 2017]

The State of Qatar recognized some time ago that information security or cybersecurity is not just a technology issue but also a matter of national policy. To this end, the Qatar computer emergency response team (see www.Qcert.org) was formed in 2005 to catalyse change, and more specifically to accelerate the widespread adoption of effective cybersecurity practices and policies, and now has a national mandate to safeguard the digital assets of the State of Qatar.

In 2013, the Prime Minister formed a national Cybersecurity Committee. The committee has developed a national cybersecurity strategy in order to improve the security posture of Qatar and ensure the continued success and growth of the nation through five pillars that determine where action will be taken:

- Safeguard the national critical information infrastructure
- Respond to, resolve and recover from cyberincidents and attacks through timely information sharing, collaboration and action
- Establish a legal and regulatory framework to enable a safe and vibrant cyberspace

- Foster a culture of cybersecurity that promotes safe and appropriate use of cyberspace
- Develop and cultivate national cybersecurity capabilities.

The computer emergency response team has been successfully delivering different information security services to meet the needs of the country's constituents, businesses and organizations, especially in the areas of incident response, intelligence, resiliency, training and awareness, crisis management, key public infrastructure licensing and identity, and the creation of the national information security compliance framework.

Qatar believes there is currently a gap in the ability of States to gain and share sufficient cyber situational awareness at regional and international levels to enable effective decision-making. More work is needed on collaborative prevention to ensure stronger cybersecurity across cyberinfrastructure and services to ensure resilience, especially in regard to the normal operation of daily life for Governments, services, businesses, consumers and citizens.

Cybersecurity has never been more efficient than when information exchange is taking place. Working on information-sharing agreements would be a great asset for States through collaboration frameworks that describe verification and compliance methodologies.

Attacks will happen and nations, Governments, organizations and industry must be prepared, together.

Singapore

[Original: English]
[31 July 2017]

As a small and highly connected State, Singapore supports a secure and resilient cyberspace underpinned by international law, well-defined norms of responsible State behaviour and coordinated capacity-building efforts to meet these norms. Robust international cooperation is necessary to address the emerging challenges posed by cyberthreats and Singapore will play its part.

Singapore established its Cyber Security Agency in 2015 to provide centralized oversight of national cybersecurity functions. Singapore's cybersecurity strategy was launched in October 2016 and outlines its holistic approach to protecting essential services from cyberthreats and creating a secure cyberspace. Four pillars underpin the strategy: building a resilient infrastructure; creating a safer cyberspace; developing a vibrant cybersecurity ecosystem; and strengthening international partnerships.

At the regional level, Singapore is working to build and deepen capacities among its neighbours. It has launched a S$10 million cybercapacity programme in association with Association of Southeast Asian Nations (ASEAN) to complement regional capacity-building efforts. Under this programme, Singapore held an ASEAN cybernorms workshop in May 2017 and will hold an ASEAN cybersecurity capacity-building workshop in August 2017. It also hosts the annual Singapore International Cyber Week, which comprises the ASEAN Ministerial Conference on Cybersecurity and the International Cyber Leaders' Symposium for global leaders across government, industry and academia to engage the region and discuss emerging and cross-cutting issues.

In terms of multilateral cooperation, Singapore supports the work of the Group of Governmental Experts on Developments in the Field of Information and

Telecommunications in the Context of International Security, including the 11 norms set out in its 2015 report. It is important to define and implement those norms that enjoy broad agreement, especially operational norms. They include not supporting online activity that intentionally damages critical infrastructure; not supporting activity that prevents computer security incident response teams from responding to cyberincidents; and not using those response teams to engage in malicious international activity.

Turkey

[Original: English]
[31 July 2017]

Information and communication technologies (ICTs) have become essential parts of today's society and economic life. They contribute to social wealth and development as well as to the daily life of individuals. They are used in a broad spectrum that includes the public and private sectors, critical infrastructure sectors and individuals, and have become widespread in the country and the world despite cybersecurity risks.

In this context, Turkey has taken part in many initiatives by contributing cooperation efforts on cybersecurity issues. The goal is ensuring cybersecurity. In this context, through the coordination of the Ministry of Transport, Maritime Affairs and Communications, national cybersecurity exercises were held; the first International Cyber Shield Exercise was completed in Istanbul, while Turkey has also regularly and annually participated in and contributed to international exercises related to cybersecurity, namely the Cyber Coalition of the North Atlantic Treaty Organization (NATO), NATO Locked Shields and the NATO Crisis Management Exercise.

Dialogue and cooperation with the United Nations, NATO, the European Union, the Organization for Security and Cooperation in Europe and other international and non-governmental organizations, academia and opinion leaders has been enhanced. This approach is being strengthened by conferences, courses, seminars, meetings, graduate-level education and other supportive programmes. Turkey is leading regional cybersecurity efforts by concluding bilateral agreements with various States.

The memorandum of understanding that describes the cooperation between NATO and its allies was approved by the NATO Cyber Defence Committee and related work for signature is ongoing. Turkey is a sponsoring nation of the NATO Cooperative Cyber Defence Centre of Excellence. The work of the NATO Civil Emergency Planning Committee and meetings of the Regional Arms Control Verification and Implementation Assistance Centre — Centre for Security Cooperation are followed and cooperation on various issues has been developing. Turkey is a founder of the Global Forum on Cyber Expertise and has become a party to the framework document and the Hague Declaration on the Global Forum.

A decision on cybersecurity, emphasizing the work of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, was taken at the Group of 20 Summit held in Turkey on 15 and 16 November 2015.

The Council of Europe Convention on Cybercrime was signed by Turkey in Strasbourg in 2010 and approved through Law No. 6533 in 2014 and its adaptation to national legislation was finalized subsequently.

As the result of the collection, review and assessment of information generated within the scope of meetings and common-sense platforms, a national cybersecurity strategy and action plan for the period 2016-2019 was prepared.

Strengthening information security at the global level and thereby developing a security culture within the international community is a crucial matter for everyone. At the same time every State has the right to take measures to protect itself from the malicious use of ICTs by terrorists, extremists, organized criminal groups and freelance hackers for the preservation of national security. In that context, strengthening international legislation and enhancing bilateral international agreements is also of great importance.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[31 July 2017]

The United Kingdom welcomes the opportunity to respond to General Assembly resolution 71/28 on developments in the field of information and telecommunications in the context of international security, which builds upon its response to resolution 70/237 in 2016. 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 cyberspace as a fundamental element of securing critical national and international infrastructure and an essential foundation for economic and social activity online. Actual and potential threats posed by activities in cyberspace continue to be of great concern. The new national cybersecurity strategy, published in October 2016, will shape the country's efforts over the next five years to defend its assets, deter its adversaries and develop its cybersecurity sector.

The United Kingdom continues to take a leading role in the international debate on cybersecurity. It provided experts at all five Groups of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Despite the lack of consensus in the 2017 group, the country is committed to promoting an international stability framework for cyberspace based on the application of existing international law, agreed voluntary norms of responsible State behaviour and confidence-building measures, supported by coordinated capacity-building programmes. The United Kingdom also welcomes efforts of the Organization for Security and Cooperation in Europe and other regional forums to provide proposals for implementing confidence-building measures and will look to continue to lead by example in adopting such measures.

This response outlines the work of the United Kingdom on supporting and improving cybersecurity and sharing best practice domestically and worldwide, including with international partners to tackle cybercrime, major incidents and building capacity. The United Kingdom looks forward to seeing further progress and is pleased to be actively engaged on these issues. It will continue to participate fully in strengthening capability and international cooperation on cybersecurity.