United Nations A/69/112

General Assembly

Distr.: General
30 June 2014

Original: English/Spanish

Sixty-ninth session
Item 92 of the preliminary list*
Developments in the field of information and telecommunications in the context of international security

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

Report of the Secretary-General

Contents

		Page
I.	Introduction	2
II.	Replies received from Governments	2
	Australia	2
	Austria	3
	Colombia	4
	Cuba	7
	El Salvador	9
	Georgia	9
	Germany	10
	Portugal	12
	Serbia	13
	Switzerland	15
	United Kingdom of Great Britain and Northern Ireland	17

* A/69/50.

14-56479 (E) 110714 110714

Please recycle

I. Introduction

1. On 27 December 2013, the General Assembly adopted resolution 68/243 entitled "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/68/98), 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 19 February 2014, a note verbale was sent to Member States inviting them to provide information on the subject. The replies received are contained in section II below. Any additional replies received will be issued as addenda to the present report.

II. Replies received from Governments

Australia

[Original: English]
[30 May 2014]

In Australia's view, existing international law provides the framework for State behaviour in cyberspace and for appropriate responses to unlawful online activity pursued by States. This includes, where applicable, international humanitarian law, law regarding the use of force, international human rights law and international law regarding State responsibility. Any new or additional norms for State behaviour in cyberspace must be developed consistent with international law.

The consensus report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98) made a significant contribution to the guidance of States by affirming that international law, and in particular the Charter of the United Nations, is applicable to States' use of cyberspace and essential to maintaining peace and stability. Australia considers this finding to be of fundamental significance. Australia believes that States should, individually and collectively, reiterate publicly their understanding that international law applies to States' behaviour in cyberspace and their commitment to act in cyberspace in accordance with their understanding of international law.

The report recognized the need for further discussion and articulation of how international law applies to States' use of cyberspace and recommended further

study in this area. It noted that additional norms could be developed over time. Australia believes that elaborating how international law applies to States' behaviour in cyberspace in both conflict and non-conflict situations, while acknowledging the complexities involved, is a priority task for the international community.

The report also made groundbreaking recommendations on cyber confidence-building measures. Australia recognizes that the elaboration of how international law applies to States' use of cyberspace is a long-term task. In the short term, there is a need for practical measures to address and prevent problems between States in cyberspace that may result from misperception and that could lead, through miscalculation and escalation, to conflict. Regional security organizations are particularly well-placed to consider, develop and implement cyber confidence-building measures. Australia is leading work within the Association of Southeast Asian Nations (ASEAN) Regional Forum to advance this important agenda, which, in view of varying capacities among members, should include capacity-building objectives.

Austria

[Original: English]
[19 May 2014]

The Austrian Cybersecurity Strategy, adopted in March 2013, provides a comprehensive and proactive concept for protecting cyberspace and people in virtual space while guaranteeing human rights. It enhances the security and resilience of Austrian infrastructures and services in cyberspace. Most importantly, it serves to build the awareness and confidence of Austrian society.

Global networking and international cooperation are essential to the Austrian Cybersecurity Strategy. Security in cyberspace is pursued through a coordinated policy mix at the national and international levels. Austria will engage in an active "cyber foreign policy" in the framework of European Union, United Nations, Organization for Security and Cooperation in Europe (OSCE), Council of Europe, Organization for Economic Cooperation and Development (OECD) and North Atlantic Treaty Organization (NATO) partnerships based on a coordinated and targeted approach.

Austria will contribute substantially to the implementation of the European Union Cybersecurity Strategy, participating fully in the strategic and operational work of the European Union. The competent ministries will take the necessary measures to implement and take full advantage of the Convention on Cybercrime of the Council of Europe. Austria advocates a free Internet at the international level. The free exercise of all human rights must be guaranteed in virtual space; particularly, the right to freedom of expression and information must not be restricted unduly in the Internet.

Austria will continue its bilateral cooperation in the framework of its NATO partnership and actively support the preparation of a list of concrete confidence- and security-building measures in OSCE. Austria participates actively in planning and implementing transnational cyberexercises. The experience gained will feed directly into planning and further developing operational cooperation. The Ministry for

Foreign Affairs coordinates the foreign policy measures relevant for cybersecurity. Where appropriate, the conclusion of bilateral or international agreements will be taken into consideration.

Nationally, a steering group is developing an implementation plan to carry out the horizontal measures laid down in the Austrian Cybersecurity Strategy. The competent bodies are responsible for implementing these measures within their respective mandates, with coordination by the steering group. Based on the Austrian Cybersecurity Strategy, they will develop substrategies for their sphere of responsibilities. The ministries represented in the steering group are tasked to submit an implementation plan to the Federal Government biannually. The preparation of the plan will be accompanied by a review of the Austrian Cybersecurity Strategy, to be revised and updated if necessary.

Colombia

[Original: Spanish]
[23 May 2014]

General appreciation of the issues of information security

In recent years, significant progress has been achieved in developing and applying information and communication technology, and this has led to major changes and benefits that have made a considerable contribution to the development of many countries, while promoting increased international cooperation for the dissemination of information.

Nevertheless, these technological advances have also highlighted deep concerns about the possibility that those advances could be used to undermine international stability and security, and adversely affect the integrity of States' infrastructure, with a resulting reduction in their civil and military security.

In this context, the use of new technologies to generate computer threats, and the existing threat of crime in cyberspace, are matters of great concern and of the utmost national importance for Colombia.

It is therefore imperative for Colombia to define policies and strategies to prevent information technology from being used for terrorist or criminal purposes.

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

Legislative and institutional responses

In 2005 Colombia applied the ISO 27001 standard, conceived as a management system that set quality standards for information security in national entities, and advocated safeguarding the confidentiality, integrity and availability[1] of information.

[1] Confidentiality: preventing information from being used by unauthorized individuals or processes. Integrity: safeguarding the accuracy and completeness of anything of value to an organization. Availability: ensuring that information is accessible and usable on demand by authorized entities.

Four years later, the Congress of the Republic of Colombia enacted Act No. 1273 of 2009, which amended the Criminal Code by creating a new legally protected interest, namely "information and data protection". The amendment enabled the establishment of a national legal framework for the relevant authorities to prosecute and try information technology-related offences.

Within this framework, Colombia criminalized, inter alia, illegal access; illegal interception; attacks on data integrity; attacks on system integrity; device abuse; computer counterfeiting; computer fraud; child pornography; and crimes against intellectual property and related rights.

In 2011, through the CONPES 3701 document, Colombia launched its national cyberdefence and cybersecurity policy based on three fundamental pillars:

(a) Adopting an appropriate inter-institutional framework for prevention, coordination and monitoring and the formulation of recommendations to address any threats and risks that arise;

(b) Developing specialized training programmes on information security;

(c) Strengthening legislation on those matters and international cooperation, and, within that framework, accelerating Colombia's accession to the various international instruments, namely, the Budapest Convention.

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

1. The Intersectoral Commission, responsible for formulating the strategic vision of information management and setting policy guidelines for the management of public information technology infrastructure, cybersecurity and cyberdefence;

2. The Colombian Computer Emergency Response Team (colCERT), the national coordinating agency on matters of cybersecurity and cyberdefence;

3. The Armed Forces Joint Cyber Command (CCOC), which is tasked with preventing and countering any cyber threat or attack that affects national values and interests;

4. The Cyber Police Centre, which is responsible for Colombia's cybersecurity, offering information, support and protection from cybercrime.

Similarly, Colombia has a legal framework for the protection of personal data, established by means of Act No. 1581 of 2012 and Decree No. 1377 of 2013, which partially regulates the Act. Furthermore, a Department for Personal Data Protection was established in the Superintendence for Industry and Trade.

The Ministry of Information Technology and Communications also set up and implemented a Government Online strategy incorporating the requirements for entities to adopt information security management systems. Similarly, since 2008, the Ministry has trained around 6,300 civil servants on information technology management-related processes.

It should also be noted that, in the area of capacities, progress is being made with the identification of critical infrastructure (the infrastructure which, if damaged, could potentially lead to a loss of human life, economic damage or reduced governability of the country) with a view to safeguarding cybersecurity at those locations.

International cooperation

In 2013, Colombia formally applied for membership of the European Convention on Cybercrime, which establishes the principles of the international agreement on cybersecurity and penalties for the corresponding offences, and of which the main aim is to protect society from cybercrime by putting in place appropriate legislation and international cooperation.

In addition, in 2012, Colombia joined a multilateral agreement with the World Economic Forum, known as the "Partnership for Cyber-Resilience", geared to identifying and addressing global systematic risks stemming from the ever greater connectivity between persons, processes and objects.

Meanwhile, the Secretariat of the Inter-American Committee against Terrorism (CICTE) of the Organization of American States has established a comprehensive approach to capacity-building in the area of cybersecurity among member States. The Secretariat's main achievement has been the setting up of national "alert, watch, and warning" groups, also known as Computer Security Incident Response Teams", which have a mandate and the capacity to respond to crises, incidents and threats to cybersecurity.

Within this framework, and in cooperation with CICTE, Colombia has set up "alert, watch, and warning" groups that contribute to the development of national cybersecurity strategies. It has also taken part in workshops, courses and conventions on the handling of incidents involving cybersecurity, information security and cybercrime.

It should also be noted that Colombia has reached agreements with international enterprises and organizations operating in the information and communication industry, notably an agreement with Microsoft to enable access to institutions such as the "Cybercrime Center" and other cybersecurity programmes; and an agreement with the "Antipishing Working Group" for the purpose of joining the global coalition of legal authorities, industry enterprises and Government entities that are working to set up more efficient cyberincident alert and response mechanisms.

International measures taken to strengthen information security

Cybersecurity is not exclusively a Government problem, nor can it be solved by the Government alone: the support of other actors, namely, academia, industry and civil society, will be needed to address effectively the risks arising from the ever more intensive use of information and communications technology in all sectors.

Colombia considers that, for international information security to be strengthened at the global level, it is important for the international community to:

- Seek mechanisms to raise awareness in society, among elected officials and in the entities of each State of the need to create an information security culture and of the importance of international cooperation against cybercrime.
- Promote States' obligation to develop strategies geared to strengthening national capacities in the area of cybersecurity and cyberdefence.
- Urge States to identify critical infrastructure and set up a programme specifically intended to enhance its security and resilience.

- Provide incentives for bringing domestic legal frameworks into line with existing international instruments in the area of cybersecurity. Greater harmonization between different countries makes it easier to set up channels of cooperation for the prevention, investigation and prosecution of cybercrime by States.

Such harmonization should contribute to defining technology-related offences and set clear rules on jurisdiction and entitlement to prosecute.

- Promote the establishment of obligations requiring States and public and private national entities to save computer records for subsequent use in investigations and trials.
- Compile a glossary of cybercrime-related computer terminology that is generally unknown to officials in the criminal justice system, to ensure the confidentiality and integrity of systems, networks and computer data.
- Promote exchanges of experiences and best practices in the area of cyberdefence and cybersecurity, as well as set up specialized training networks.
- Urge States to join cyberincident alert networks.

Cuba

[Original: Spanish]
[27 May 2014]

Cuba fully shares the concern expressed in resolution 68/243 regarding the use of information technologies and means of telecommunication that may affect international stability and security and the integrity of States to the detriment of their security in civil and military fields. The resolution also places due emphasis on the need to prevent the use of information resources or technologies for criminal or terrorist purposes.

In this regard, Cuba expresses 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. Some Governments have even said that it would be possible to respond to such attacks with conventional weapons. The only way to prevent and tackle these novel threats, and to avoid cyberspace turning into a theatre of military operations, is joint cooperation between all States.

The hostile use of telecommunications with the declared or hidden intent of undermining the legal and political order of States is a violation of the internationally recognized norms in this area and can give rise to tensions and situations that are not conducive to international peace and security.

In this regard, Cuba reiterates its condemnation of the radio and television war waged by the Government of the United States of America against Cuba, which violates the current international rules governing the radio-electric spectrum. This aggression is being perpetrated without regard for the damage that could be caused to international peace and security by creating dangerous situations.

The illegal radio and television broadcasts against Cuba are intended to promote illegal immigration and encourage and incite to violence, contempt for constitutional order and the perpetration of terrorist acts. The use of information for the purpose of subverting the internal order of other States, violating their sovereignty and meddling and interfering in their internal affairs is illegal.

These broadcasts against Cuba constitute violations of the international norms in force in the constitution of the International Telecommunication Union, of which the preamble acknowledges the growing importance of telecommunications for the preservation of peace and the economic and social development of all States, with the object of facilitating peaceful relations, international cooperation among peoples and economic and social development by means of efficient telecommunications services.

The Government of the United States of America is continuing to transmit audio broadcasts on the medium-wave commercial band 24 hours a day every day. This frequency band is not reserved for services to other countries. Other commercial radio stations provide services to anti-Cuban organizations to transmit broadcasts intended to subvert internal order and misinform the Cuban people.

Such broadcasts are transmitted on the short-wave band by various of these organizations, with the full knowledge of the Government of the United States.

Between April 2013 and April 2014, the average number of hours per week of broadcasts of subversive content to Cuba ranged from 1909 to 2070, using 27 frequencies. In September and October 2013, two North American stations broadcasting in southern Florida and whose signals are picked up in the western and central parts of Cuba began to broadcast programming of a counter-revolutionary nature.

Anti-Cuban broadcasts by the Martí radio and television station via international and domestic satellite systems of the United States also continued.

Furthermore, the "ZunZuneo" case, a complex plot supported by millions of dollars from the United States Government and intended to promote subversion in Cuba using a messaging service on social networks, was exposed this year.

This illegal programme, which was active until 2012, was used to collect the private data of Cuban users, without their consent, and to process their profiles by gender, age, tastes and affiliations of various kinds, for use for political purposes.

ZunZuneo, like other subversive operations, violates Cuban law and United States legislation, such as the Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (Public Law 108-187), adopted by the United States Congress in December 2003, which prohibits the sending of commercial or other types of messages without the express consent of the addressee.

This was yet another violation of the constitution of the International Telecommunication Union since such uses of new technologies, and social networks in particular, are clearly not conducive to peaceful relations and international cooperation by means of efficient telecommunications services.

The harmful practice of sending unsolicited mail (spam) has been the subject of over 10 recommendations of the Telecommunication Standardization Bureau and

constitutes a violation of point No. 37 of the Declaration of Principles of the World Summit on the Information Society held in Geneva in 2003.

The Government of the United States should respect international law and the purposes and principles of the Charter of the United Nations; it should therefore cease its illegal and covert actions against Cuba, which are condemned by the Cuban people and international public opinion.

In this regard, the Community of Latin American and Caribbean States (CELAC) adopted a communiqué on 29 April, in which it stressed that the illegal use of new information and communication technologies had a negative impact on nations and their citizens.

In that communiqué, CELAC strongly expressed its rejection of the use of ICTs in a manner contrary to international law, and all actions of that nature. It underlined the importance of guaranteeing that the use of such technologies should be fully consistent with the purposes and principles of the Charter of the United Nations, international law, in particular sovereignty, non-interference in internal affairs and internationally recognized standards of coexistence between States. It reiterated its commitment to intensifying international efforts to safeguard cyberspace and promote its use for exclusively peaceful purposes and as a medium contributing to economic and social development.

Cuba supported resolution 68/243 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 May 2014]

The Armed Forces of El Salvador, within the framework of information security and telecommunications, has put in place a voice, video and data telecommunications network that is separate from the public network and intended to protect all information from any external agent that might attempt to infiltrate it, as well as from cyberattacks.

Georgia

[Original: English]
[30 May 2014]

Executive summary

Cyberwar, conducted against Georgia in 2008, put the protection of critical infrastructure high on the agenda of the Government of Georgia. The rapidly growing dependence of the critical infrastructure and Government services on information technology (IT) increases vulnerability to cybercrime-related incidents. Accordingly, adequate protection of critical infrastructure from cyberthreats is one of the priorities of the Government of Georgia.

The first targets of cyberattacks in 2008 were Government and news media websites. Later, the attacks were expanded to include many more Government websites, Georgian financial institutions, business associations, educational institutions, more news media websites and a Georgian hacking forum. These cyberattacks were intended to interrupt normal business operations. Apart from the two big banks, the business-related targets were primarily organizations that could have been used to communicate and coordinate responses among different businesses.

The above-described experience demonstrates that cyberattacks on the critical infrastructure of Georgia by State and private actors can cause serious physical damage as well as significant financial damage to the public and private sectors. Therefore, the Government of Georgia considers cybersecurity to be part of the general security policy of the country, especially in the view of its increased reliance on IT as a vehicle for the delivery of Government services.

Voicing these concerns, the National Security Council and a special working group comprised of different Government agencies developed the national Cybersecurity Strategy of Georgia throughout 2011, as a part of the National Security Review. The Cybersecurity Strategy and the action plan for its implementation were presented to the public for discussion in March 2012 and finally adopted in January 2013.

A further step was the establishment of the Data Exchange Agency of the Ministry of Justice of Georgia in 2010 as a central Government entity responsible for the development and implementation of e-governance policies and solutions. An important part of the Agency's mandate is information security for the public sector and private entities as follows:

- Adoption and implementation of information security policies and standards in public sector and critical infrastructure
- Providing consultancy services in the field of information security and performing information security audits
- Awareness-raising activities about information security issues in the public as well as the civil sector
- Cybersecurity mandate through the national computer emergency response team.

The full text of Georgia's submission can be found at http://www.un.org/disarmament/topics/informationsecurity/.

Germany

[Original: English]
[30 May 2014]

Executive summary

Information and communication technologies (ICTs) offer unprecedented opportunities for industrialized and developing countries alike. At the same time, vulnerabilities and systemic weaknesses exist.

There is a trend towards hard-to-detect, sophisticated and malicious activities, targeting high-value objectives. Severe consequences may result. A cyberattack against key infrastructures could cause more disruption than an isolated physical attack, sometimes with unpredictable consequences for other networked entities.

Despite such risks, an all-out "cyberwar" seems unrealistic for the time being. A more likely scenario may be the limited use of cybercapabilities as part of a larger war-fighting effort. Finally, there is the danger that cyberincidents may escalate into "real-life" conflict.

In this situation, increasing cyberresilience, agreeing on laws and rules that apply to the use of ICTs and engaging in confidence-building measures become ever more important.

There has been welcome progress in 2013: The last report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security made clear that international law is applicable to cyberspace. The Group also found that State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to its jurisdiction over ICT infrastructure within its territory. Germany is looking forward to seeing how the new Group of Governmental Experts will take this further.

Concerning confidence-building measures, OSCE made important progress with the adoption of a first set of steps to increase inter-State cooperation, transparency, predictability and stability, with a view to reducing the risks of misperception, escalation and conflict that may stem from the use of information and communication technologies. This OSCE agreement might be useful as a model for other regional organizations.

Germany's Cybersecurity Strategy (2011) proceeds from the assertion that the availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace have become of vital importance. Ensuring cybersecurity has turned into a central challenge for the State, business and society. All need to act together, both at the national level and in cooperation with international partners. Germany's Cybersecurity Strategy sets out the following objectives and measures:

- Protecting critical information infrastructures
- Securing IT systems
- Strengthening IT security in public administration
- Running a national cyberresponse centre
- Establishing a national Cybersecurity Council
- Effective crime control in cyberspace
- Effective coordinated action to ensure cybersecurity in Europe and worldwide
- Using reliable and trustworthy information technology
- Personnel development among federal authorities
- Tools to respond to cyberattacks.

Following the German general election in September 2013 and according to the Coalition Agreement, cybersecurity is high on the Government agenda. Data privacy standards will be on the rise. Lead topics for the next four years include better consumer protection; amendments to the criminal laws to better protect individuals; the passing of an IT security law with mandatory minimum IT security standards for critical infrastructure; and an obligation in respect of all federal authorities to invest 10 per cent of their IT budget to improve the security of their systems.

As a consequence of concerns about unlawful or arbitrary surveillance and/or interception of communications, as well as unlawful or arbitrary collection of personal data by third parties, the Government of Germany strongly encourages IT service providers to encrypt telecommunication and not to forward telecommunication data to foreign intelligence services.

The full text of Germany's submission can be found at http://www.un.org/disarmament/topics/informationsecurity/.

Portugal

[Original: English]
[20 May 2014]

General Assembly resolution 68/243 on the above-mentioned theme recalls the important role of science and technology in the context of international security, recognizing that the developments in those areas can have civil and military applications and also recognizing that progress should be maintained and encouraged. Progress in the field of information and telecommunications means increasing opportunities for the development of civilization; cooperation among States; the promotion of human creativity; and the circulation of information in the community as a whole.

However, those technologies and means can potentially be used for purposes that are inconsistent with international stability and security and may negatively affect the national integrity of States, in the civil and military fields.

General Assembly resolution 68/243 requires the contribution of Member States in four areas, recalling the report of the Group of Governmental Experts A/68/98:

1. General appreciation of the issues of information security;

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

3. The content of the concepts aimed at strengthening the security of global information and telecommunications systems;

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

The report presented 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, we can describe our national context:

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

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

2. We must highlight the development of efforts in the implementation of legislation on network security and integrity by adopting methods in respect of risk, which demand the adoption of adequate security measures, at the technical and organizational levels, and the requirement of reporting security violations or integrity loss which have a significant impact on the functioning of services. Also important are the auditing procedures in the field of security, carried out by the national Notification Centre for Security Violations or Integrity Loss;

3. Concerning protection of personal data and privacy, it is important to highlight the changes that have occurred, for instance in the mandatory reporting of personal data violations;

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

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

(II) Measures for the reinforcement of confidence and information-sharing

1. It is crucial to promote information-sharing, taking into account wider globalization;

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

(III) Measures for 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 access to knowledge;

3. Top-level hierarchy is not sufficiently aware of its own responsibility in these matters.

Serbia

[Original: English]
[28 May 2014]

Taking into account the great importance given to information security on the global and national levels, the Republic of Serbia has undertaken a number of activities in order to provide efficient national policies and effective security mechanisms. In the Strategy for the Development of the Information Society in the

Republic of Serbia until 2020, adopted by the Government of the Republic of Serbia in 2010, information security is declared to be one of six priority areas. Serbia does not have a national strategy solely dedicated to information security, but this topic is dealt with in a number of other documents. In October 2013, a special working group was formed and tasked to draft a law on information security. The law is harmonized with the relevant international and European Union legal frameworks and determines the following: information security institutional framework; measures needed to provide enhanced security of ICT systems in the Republic of Serbia, including ICT systems of public bodies and enterprises; norms for prevention coordination in respect of security risks in ICT systems; establishment of the national computer emergency response team; specific security measures and preconditions to be applied in information systems of State bodies; security of classified data in ICT systems; crypto-security and protection from compromising electromagnetic emanations.

The ICT Department of the Administration for Joint Services of the Republic Bodies performs the activities related to the protection of information security, data protection and the implementation of prescribed security standards for information systems of State bodies. In the Administration's annual report, it was stated that within its mandate of protection of State ICT systems, the Department provides protection from cyberattacks on a daily basis, as the network is attacked every day.

The Academic Network of the Republic of Serbia performs the computer security incident response activities for the educational and scientific research institutions in the Republic of Serbia. In the Academic Network's 2013 annual report, it was declared that there has been an increasing number of incidents compared with 2012. The report identified old equipment as one of the reasons for the increasing number of attacks.

Only a well-established national information security culture embraced at every level of society can be effective to locally strengthen the security of national information and telecommunications systems. Similarly, only such well-established national information security systems can be a part of the application of the international information security concepts to strengthen the security of global information and telecommunications systems.

The Office of the National Security Council and Classified Information Protection (hereinafter, the National Security Council Office) is the Serbian Government service responsible for coordination of the implementation of national and European Union security policies at the national level (National Security Authority). A specific segment of its activities is reflected in the adoption of information assurance measures and the coordination of the implementation of those measures in Government bodies and other institutions for the purpose of the protection of classified information. In this context, the Decree on special measures for the protection of classified information in information telecommunications systems was passed in 2011 (Official Gazette RS, No. 53/2011). At the international level, since 2011, the National Security Council Office has been an active participant in the Forum of the directors of the South-East European National Security Authorities. One of the Forum's primary aims is to enhance information assurance and classified information protection in the regional countries, in line with international standards. The National Security Council Office acts as a chief coordinator for developing a regional cyberdefence concept within the framework of the South-East European National Security Authorities.

The National Security Council Office has prepared and sent other thematic working group members a number of related proposals for their examination, harmonization and approval. Such proposals are structured by means of the following working documents: (l) Cyberdefence programme objectives; and (2) — South-East European National Security Authorities cyberdefence questionnaire.

The Ministry of Defence of the Republic of Serbia is participating in the implementation of General Assembly resolution 68/243. Departments within the Ministry of Defence are active in the working group tasked to draft the law on information security.

Also, the Ministry of Defence is in the process of forming different departments that will operate in the area of information security and cyberdefence.

Switzerland

[Original: English]
[29 May 2014]

A. 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 seize the opportunities that are generated by the use of ICTs. Switzerland takes account of the new developments and challenges in relation to ICTs and actively engages in shaping the information society by means of the Strategy of the Federal Council for an Information Society in Switzerland.

However, the use of ICTs has exposed information and communication infrastructure to criminal, intelligence, politico-military or terrorist abuse or functional impairment. Disturbances, manipulation and specific attacks carried out via electronic networks are the risks that an information society entails. Against this background, States have become increasingly engaged in a series of regional and international policy discussions and debates over cybersecurity. This engagement is generated from a growing sense of insecurity regarding vulnerabilities in computer systems and related technologies and how they can be exploited for malicious purposes.

Even though vulnerabilities and threats in this environment have been recorded since the 1980s, it was not until the past seven years that threats and vulnerabilities stemming from the use of ICTs were put on the national security agenda. As a result, the Swiss Federal Government set up an expert group in 2010 in order to scrutinize the risks and increase the national capacity to respond to these threats and vulnerabilities.

Switzerland's functioning as a holistic system depends on a growing number of mutually networked information and communication facilities (computers and networks). This infrastructure is vulnerable. Country-wide or long-lasting disruptions and attacks could have severe adverse effects for Switzerland's technical, economic and administrative performance. Such attacks can be launched by a variety of perpetrators and have various motives: individual perpetrators, political activists, criminal organizations intent on fraud or blackmail, and terrorists or State spies who want to disrupt and destabilize the State and society. ICTs are particularly attractive as targets not only because they offer many possibilities for abuse, manipulation and

damage, but also because they can be used anonymously and with little effort. Protecting information and communication infrastructure from such disturbances and attacks is in Switzerland's national interest. In this sense, we welcome the conclusion of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security that international law is applicable to ICTs.

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

On 27 June 2012, the Swiss Federal Government adopted the National strategy for the protection of Switzerland against cyberrisks, thereby laying the foundation for a comprehensive, integrated and holistic approach to tackling cyberrisks. The strategy seeks to improve the early detection of cyberrisks and emerging threats, make Swiss infrastructure more resilient to cyberattacks and generally reduce cyberrisks. The main focus lies on cybercrime, espionage and sabotage. The underlying rational of the strategy is the need for a cybersecurity culture, shared responsibility and the need for a risk-based approach. It advocates stronger coordination at the Government level and fosters private-public partnership and enhanced cooperation in the international arena.

The strategy comprises a set of 16 measures, which should be put in place by 2017. In order to guarantee the effective and timely implementation of these measures, the Government of Switzerland adopted a detailed plan for the implementation of the strategy on 15 May 2013. It also established a steering committee, in which the leading agency for the implementation of a specific measure is represented. The steering committee is mandated to secure the coordinated, purposeful implementation of this strategy. Its roles and responsibilities range from ensuring coordination among the relevant Swiss Federal departments[2] and relevant agencies at the local level. At an operational level, the Government has set up a coordination unit which is supposed to support the work of the steering committee.

The set of measures ranges from risk and vulnerability analysis, analysis of the threat landscape, continuity and crisis management and competence-building measures to international cooperation and initiatives.

The 16 measures can be broken down into four main areas:

– Prevention (i.e. risk and vulnerability analysis and threat landscape);

– Reaction (i.e. incident handling, active measures and law enforcement);

– Continuity (i.e. continuity and crisis management);

– Supporting processes (i.e. international cooperation, education and research, legal foundations, etc.).

C. Content of the concepts mentioned in paragraph 2 of General Assembly resolution 68/243

International cooperation is one of the action fields that needs to be strengthened by means of the Swiss national cyberstrategy. Thus, Switzerland is determined to cooperate at the international security policy level so as to encounter the threat in cyberspace together with other countries and international

[2] Equivalent to a Ministry.

organizations. Switzerland is committed to monitor and shape respective developments at the diplomatic level and promote political exchanges within the framework of international conferences and other diplomatic initiatives.

Against this background, Switzerland participates in different international processes aimed at developing global mechanisms. OSCE has adopted confidence-building measures in the realm of cybersecurity. Switzerland considers this process as paramount. Thus, by pursuing a "dual track", Switzerland will focus on the implementation of the first set of confidence-building measures as well as on the development of further measures. In addition, the London Agenda constitutes a further important process within which Switzerland participates. Lastly, as a non-member of the Group of Governmental Experts, Switzerland is interested in the reports issued by this Group. In this regard, we support, in particular, the request to continue to study, among others, how international law, including the Charter of the United Nations and human rights and international humanitarian law, applies to the use of ICTs.

Bilaterally, Switzerland holds regular political consultations with countries on cyber-related issues.

Switzerland is a signatory country to the Council of Europe Convention on Cybercrime, which entered into force on 1 January 2012.

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

Initiatives and measures designed to increase trust and build better understanding and confidence among States are to be focused on. At a bilateral level, track 1, 1.5 and 2 dialogues between States and other relevant stakeholders on cybersecurity issues have proved to be fruitful. Dialogues on cybersecurity need to be further developed and enhanced.

Information security could be strengthened at the global level by means of establishing joint mechanisms to avoid escalation to armed conflict. Thus, direct communication lines at both the technical and policy levels could be established. By maintaining regular contacts at the highest level, security in cyberspace can be improved.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[29 May 2014]

Executive summary

The United Kingdom of Great Britain and Northern Ireland welcomes the opportunity to respond to General Assembly resolution 68/243 entitled "Developments in the field of information and telecommunications in the context of international security", which builds on its response to resolution 67/27 in 2013. 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. Actual and potential threats posed by activities in cyberspace are of great concern. Our response details national and international approaches that have been and will be taken in order to strengthen security and promote cooperation in this field. These approaches have been underpinned by the United Kingdom's National Cybersecurity Strategy, published in November 2011.

The United Kingdom has participated actively and constructively in the international debate on cybersecurity. We have provided experts for all three Groups of Governmental Experts and welcome the consensus report of the last Group, making valuable progress in reaching common understandings on norms of State behaviour in cyberspace and affirming the applicability of international law in cyberspace. The United Kingdom also welcomes the adoption of the first set of regional confidence-building measures on cyberspace that were successfully negotiated at OSCE. The response outlines the United Kingdom's work on sharing best practice worldwide, both by working with international partners to tackle cybercrime and major incidents and by its commitment to building cybercapacity and cybercapability.

The United Kingdom looks forward to seeing further progress in all of these areas. This includes the forthcoming Group of Governmental Experts, the implementation of confidence-building measures in OSCE and the development of further confidence-building measures there and in other regional groups, the establishment of computer emergency response teams and increased cooperation among them, strengthening law enforcement cooperation on cybercrime, and promoting the multi-stakeholder approach.

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.

The full text of the United Kingdom's submission can be found at http://www.un.org/disarmament/topics/informationsecurity/.