United Nations A/69/112/Add.1

General Assembly

Distr.: General
18 September 2014
English
Original: English/French/Spanish

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

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

Report of the Secretary-General

Addendum**

Contents

* A/69/150.
** The information in the present report was received after the issuance of the main report.

14-61130 (E) 230914

II. Replies received from Governments

Canada

[Original: English]
[12 June 2014]

Canada would like to share the following views with the Secretary-General, taking into account the 2013 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). As an engine of economic growth, innovation and social development, cyberspace has enhanced social interaction and transformed industries and governments. It has also introduced new threats and challenges to society (for example, cyberbullying, cybercrime and the use of the Internet for terrorist purposes).

Canada was pleased to see, in the 2013 report of the Group of Governmental Experts, a clear affirmation by States of the applicability of international law in cyberspace as the cornerstone for norms and principles for responsible State behaviour.

Canada has a strong interest in maintaining an open and free Internet, not only for its economic prosperity, but also to support its values and interests and protect the security of its citizens.

Efforts by Canada at the national level include the implementation of its Cybersecurity Strategy and Action Plan, which help to secure the country's cybersystems and protect Canadians online through active engagement with major critical infrastructure sectors (for example, finance, transportation and energy).

Canada has developed the Cyberincident Management Framework in order to provide a consolidated national approach to the management and coordination of potential or occurring cyberthreats or cyberincidents.

Canada is working closely with multilateral and private sector partners to strengthen the information security of the networks upon which its economic prosperity and security rely.

Internationally, Canada has committed over $3.6 million through the Organization of American States (OAS) (2007-2016) to build cybersecurity capacity in OAS countries, including by establishing computer security incident response teams.

Within the Organization for Security and Cooperation (OSCE), Canada participated in drafting a set of confidence- and security-building measures to reduce the risks of conflict stemming from the use of information and communication technologies in cyberspace.

Canada is working within the Regional Forum of the Association of Southeast Asian Nations (ASEAN) to build capacity on the importance of confidence-building and transparency measures for stability in cyberspace.

Through the Canada-United States Cybersecurity Action Plan, Canada is partnering with the United States to enhance the resiliency of Canada's cyberinfrastructure and improve engagement, collaboration and information-sharing at the operational and strategic levels.

Within the Group of Seven, the United Nations Office on Drugs and Crime (UNODC) and OAS, Canada is also participating in initiatives to combat cybercrime. It is a member of the Global Alliance against Child Sexual Abuse Online and participated in the 2012-2013 Group of Governmental Experts.

Canada recommends that all Member States wishing to enhance cybersecurity and prevent cybercrime refer to the Convention on Cybercrime of the Council of Europe.

Canada believes that addressing the security of information and communication technologies must go hand in hand with respect for human rights and fundamental freedoms. The same rights that people have offline must also be protected online, including freedom of expression, association and assembly and respect for privacy.

The full text of the submission by Canada can be found at http://www.un.org/disarmament/topics/informationsecurity/.

France

[Original: French]
[15 September 2014]

France wishes first to reiterate that it does not use the term “information security”, preferring the terms “information systems security” or “cybersecurity”. As an active proponent of freedom of expression online (see Human Rights Council resolution 20/8, adopted in 2012), France does not consider information as such to be a potential source of vulnerability requiring protection, except under conditions strictly established by law, in a proportionate and transparent way, in accordance with article 19 of the International Covenant on Civil and Political Rights.

The functioning of our society is increasingly dependent upon information systems and networks, including the Internet. A successful attack on a critical information system could therefore have serious consequences, both human and economic. For this reason, in 2011 France drew up an information systems defence and security strategy, thereby making cybersecurity a genuine national priority. The 2013 Defence and National Security White Paper has sharpened the national perception of the threat by identifying two significant dangers to the nation: cyberespionage and cybersabotage of critical infrastructure.

Established in 2009 to address these challenges, the French Network and Information Security Agency has seen its resources and powers continuously strengthened since then. It is now responsible, on behalf of the Prime Minister, for all prevention and response functions relating to the cybersecurity of France’s critical infrastructure, including government infrastructure. The Ministry of Defence, which is responsible for its own network security, has also gained momentum in this area, as indicated by the release in February 2014 of an ambitious strategy paper, the Cyber-Defence Pact.

At the same time, France has been actively engaged in strengthening international cybersecurity cooperation, the absence of which would limit national efforts. France has had a special interest, since the 2011 Group of Eight meeting in Deauville, in strengthening the international regulation of cyberspace. To that end, the country now participates actively in the work of the United Nations Group of

Governmental Experts and the Organization for Security and Cooperation in Europe (OSCE) to establish an international normative framework based on current international law, as well as confidence-building measures and specific standards of conduct in cyberspace. Finally, France is making great efforts to implement the objective of international cybersecurity capacity-building through specific programmes, both bilateral and multilateral (through the European Union and the North Atlantic Treaty Organization (NATO)).

The full text of the submission by France can be found at http://www.un.org/disarmament/topics/informationsecurity.

Republic of Korea

[Original: English]
[30 June 2014]

Cyberspace offers infinite opportunities for economic and social development and greater global prosperity. An open and secure cyberspace is essential to increase human accomplishments and promote democratic participation. However, it also poses new challenges, such as cybercrime, cyberterrorism and cyberwarfare.

To address such challenges, in July 2013, the Government of the Republic of Korea announced the National Cybersecurity Comprehensive Countermeasures, which set out the its response to cyberattacks and efforts to strengthen security measures for designated critical information infrastructures.

The Republic of Korea is of the view that agreeing on a set of international norms and confidence-building measures, building the cybercapacity of developing countries and promoting cooperation among computer emergency response teams are key areas for international cooperation.

In this respect, the Government of Korea is holding regular bilateral consultations with a range of countries and is actively participating in regional and international discussions on cyber issues, including in the Regional Forum of the Association of Southeast Asian Nations, the Nuclear Security Summit and the United Nations. More recently, the Republic of Korea hosted the Seoul Conference on Cyberspace on 17 and 18 October 2013, following those held in London (2011) and Budapest (2012). The conference raised awareness on the need to reinforce international cooperation to address growing threats, while finding common ground on major cyber issues. The participating countries agreed on the Seoul Framework for and Commitment to Open and Secure Cyberspace, as part of the Chair's summary.

The full text of the submission by the Republic of Korea can be found at http://www.un.org/disarmament/topics/informationsecurity/.

Spain

[Original: Spanish]
[30 June 2014]

Spain considers that Governments should support and maintain an open, accessible and secure cyberspace while safeguarding fundamental values such as democracy, human rights and the rule of law.

Cybersecurity is a strategic priority for Spain. Consequently, and in line with the Cybersecurity Strategy of its European Union partners, Spain has adopted a National Cybersecurity Strategy (5 December 2013) which reflects a comprehensive approach to cybersecurity and establishes an interministerial coordination system, the National Cybersecurity Council, to respond to crisis situations.

The Strategy also provides for international cooperation measures and the involvement of agencies and businesses, especially strategic ones. Among its key components are educational and awareness-raising activities geared towards increasing civil society's knowledge of cybersecurity issues.

Spain considers that the United Nations has a very important role to play in building international consensus in this area and supports the holding of institutional dialogue within the framework of the United Nations in order to guarantee peaceful and secure use of information technologies. Spain similarly supports the recommendations of the 2013 report of the United Nations Group of Governmental Experts.

In the light of this objective, Spain organized a meeting on cybersecurity, at the permanent representative level, in Madrid on 21 March 2014. Spain also participates in the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, and is actively involved in various international cybersecurity initiatives in forums such as the Organization for Security and Cooperation in Europe, the North Atlantic Treaty Organization, the United Nations Office on Drugs and Crime, the United Nations Human Rights Council and the Meridian Conferences on Critical Information Infrastructure Protection. Furthermore, Spain is a State party to the Budapest Convention on Cybercrime.

Spain considers that the international community should adopt measures in four areas of activity in order to strengthen global information security:

(1) Confidence-building measures: including transparency, exchanges of information and best practices;

(2) International law: the international community and especially the United Nations should continue to consider how the principles and norms of international law should be interpreted and applied in cyberspace;

(3) International cooperation: improved communication channels in the event of incidents, and enhanced and more flexible mechanisms for police and judicial cooperation;

(4) Capacity-building: in countries where capacity-building is needed, it should be provided both bilaterally and within the framework of international organizations.

The full text of the submission by Spain can be found at http://www.un.org/disarmament/topics/informationsecurity/.

Sweden

[Original: English]
[12 September 2014]

While the development of cyberspace generates almost limitless opportunities, security concerns relating to the use of information technologies and telecommunications need to be properly addressed through international cooperation.

In Sweden, the work on the national information technology security strategy has evolved over time and the Government is currently working on a national strategy on cybersecurity. The Swedish Defence Commission has recently made assessments relating to cybersecurity and cyberdefence, stressing the need for an increase in Sweden's overall cybersecurity capabilities.

Sweden participates and contributes actively in various international cyberspace forums, while also seeking bilateral and regional dialogues on cyber issues, including in the Nordic-Baltic region. Sweden has focused in particular on promoting human rights in cyberspace and the multi-stakeholder model for Internet governance, as well as the need for fundamental principles to guide international surveillance activities.

Sweden advocates a consistent European Union cyber policy based on the European Union's fundamental values and interests. A key development was the adoption in 2013 of the comprehensive European Union Cybersecurity Strategy. Sweden was one of the initiators of the Freedom Online Coalition, a group committed to advancing Internet freedom worldwide. For three consecutive years, Sweden has hosted the Stockholm Internet Forum, a multi-stakeholder conference aimed at deepening discussions on Internet freedom and global development. Sweden was among a core group of States that initiated Human Rights Council resolution 20/8 (2012), in which the Council affirmed that the same rights that individuals have offline must be protected online. In three consecutive years, Sweden introduced joint statements in the First Committee of the General Assembly, pointing out, inter alia, the need to maintain a human rights and multi-stakeholder perspective when addressing information and communication technologies and international security. Sweden also contributed actively to the adoption of the initial set of OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies and to increase transparency, stressing in particular the respect for and promotion of human rights.

Global efforts should be made to formulate core principles to guide the use of information and communication technologies and international relations in cyberspace; some tentative concepts are suggested below. The international community, including all stakeholders, should engage in practical collaboration efforts to strengthen cybersecurity, which could include the establishment of a voluntary set of rules of behaviour or standards of international conduct in cyberspace. Global actors should work towards developing confidence-building measures to increase transparency and predictability, thus reducing the risk of misperceptions or conflict in cyberspace.

The full text of the submission by Sweden can be found at http://www.un.org/disarmament/topics/informationsecurity/.