Developments in the Field of Information and Telecommunications

in the Context of International Security

Canada appreciated the opportunity to have participated in the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security that resulted in a report based on consensus. Canada would also like to congratulate its GGE colleagues for having achieved that positive outcome, and in particular the Chairperson for her outstanding efforts in reaching consensus on the report. We also want to express our deep and sincere appreciation to Ewen Buchanan of the United Nations Office for Disarmament Affairs for his support.

The 2013 GGE report recognizes important norms for responsible state behaviour, in particular the applicability of international law in cyberspace; the relevance of state sovereignty; the responsibility of states for addressing unlawful acts carried out on their territory; and that the security of information and communications technologies by states must not obstruct the free flow of information and ideas online.

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

1. Information security

   The explosive growth, complexity and dynamism of cyberspace that has enhanced social interaction and transformed industries and governments, has also introduced new threats and challenges to our society (e.g. cyber-bullying, cyber-crime, use of the Internet for terrorist purposes).

   Enabling creative new forms of communication and commerce, the Internet has become one of the greatest engines of economic growth, innovation and social development. 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.

   Canada's freedom and prosperity increasingly depend on a robust and innovative Internet, which will continue to flourish as private sector innovation and civil society drive its growth.

   National level

   Since the Canadian Government released its Cyber Security Strategy and Action Plan for Critical Infrastructure in 2010, it has continued efforts to help secure Canada's cyber systems and protect Canadians online. As outlined in the Action Plan 2010-2015 for Canada's Cyber Security Strategy, the Government is actively engaged with major critical infrastructure sectors (e.g. finance, transportation, energy), and has improved the collaboration between departments and agencies that are actively working to improve cyber security.

   International level

   Since 2007, Canada has been supporting the Organisation of American States (OAS) in the delivery of training to enhance the capacities of national authorities in Latin America and the Caribbean to deter,

respond to, and investigate criminal exploitation of critical information infrastructures, information systems and networks. This contribution helps the countries involved to develop and implement national cyber security strategies and how to run Computer Security Incident Response Teams (CSIRTs). From 2007 - 2016, Canada is committing over $3.6 million for building cyber security capacity in Latin America and the Caribbean. As a direct result of previous Canadian funding, the number of CSIRTs has increased from 6 to 17 over the last five years.

In 2012, the OSCE Permanent Council established an informal working group, chaired by the US, to draft an initial set of Confidence and Security Building Measures (CSBMs) to reduce the risks of conflict stemming from the use of information and communication technologies. These CSBMs were agreed to at the December 2013 OSCE Ministerial Council in Kyiv. Canada, a member-state of the Organization for Security and Cooperation Europe (OSCE), has actively participated in drafting an initial set of CSBMs to reduce the risks of conflict stemming from the use of information and communication technologies in cyberspace. These Measures include voluntary measures such as information-sharing on national organizations, programmes, and strategies relevant to cyber security; tri-annual meetings of cyber security experts; communication amongst national computer emergency response teams; and common cyber security terminology.

As a member of the ASEAN Regional Forum (ARF), Canada has worked with partners there to increase engagement on cyber security issues, mainly through regional cyber-related workshops. The most recent was the ARF Workshop on Cyber Confidence Building Measures, held in Kuala Lumpur, Malaysia on March 25-26, 2014, aimed at developing ARF participants' knowledge and understanding of the role and importance of confidence building and transparency measures in promoting stability in cyberspace. Another goal of this workshop was to foster the development of a senior-level regional network of policy advisers who would resolve issues in relation to regional cyber incidents.

Canada, which shares critical infrastructure with the United States, partners with the US to protect our shared infrastructure. The Canada-US Cybersecurity Action Plan, which aims to enhance the resiliency of our cyber infrastructure, improves engagement, collaboration, and information sharing at the operational and strategic levels, with the private sector, and in public awareness activities. The Action Plan establishes lines of communication and areas for collaborative work critical to enhancing the cybersecurity preparedness of both nations.

Canada is also actively participating in international initiatives to combat cybercrime in a number of fora, including the G7, the UNODC and the OAS. On the growing concern around the online exploitation of children, in 2013 Canada became a member of the Global Alliance against child sexual abuse online. Canada also participated in the last UN Group of Governmental Experts on Developments (UN-GGE) in the Field of Information and Telecommunications in the Context of International Security (2012-13).

For the past 25 years, Canada has supported the use of ICTs as a tool for development such as helping community organizations deliver essential services such as emergency assistance to affected populations, or basic education and health care to communities in remote regions; giving producers and small entrepreneurs access to market information, job opportunities, business and technical skills and banking services; driving innovation, productivity and efficiency gains across industries, contributing to overall economic growth and competitiveness; connecting people to their governments, strengthening accountability and service delivery and supporting democracy and human rights; and linking development agencies, field workers, local organizations and communities on a global basis, enabling them to share knowledge and to find common solutions to some of the world's most pressing challenges.

The most recent projects include a strategic framework for the development and use of geomatics in Senegal; an on-line 'one-stop service' in many countries all around the world giving women access to the latest and most-up-to-date information, technical resources, and best practices, on business and economic opportunities.

For the past 15 years, Canada's International Development Research Centre has also helped to advance the social and economic prospects within developing countries, and contributed greatly to building the field of applied ICT research. Its most recent research projects include how digital technologies are enhancing potentially curtailing citizen, creator, and consumer capabilities and freedoms in the global South.

2. International concepts

Existing international law is applicable to the use of Information and Communication Technologies (ICTs) by States, and is essential to maintaining peace and stability, and promoting an open, secure, peaceful and accessible ICT environment. Among existing international law relevant to cyberspace are the Charter of the United Nations, International Human Rights Law, and International Humanitarian Law. In the latest report of the UN-GGE, Canada was pleased to see a clear affirmation by States of the applicability of international law in cyberspace as the cornerstone for norms and principles for responsible State behaviour.

Canada also believes that addressing the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms, including the right to hold opinions without interference, as well as the rights to freedom of expression, association and assembly, and respect for privacy. The same rights that people have offline must also be protected online, including freedom of expression, which is applicable regardless of frontiers and through any media of one's choice in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.

3. Possible measures to strengthen information security globally

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

Canada has developed the Cyber Incident Management Framework to provide a consolidated national approach to the management and coordination of potential or occurring cyber threats or incidents. The Framework, which sets out the roles and responsibilities of all levels of government, critical infrastructure owners and operators, and other public and private sector partners, is intended to enable each organisation to fully and effectively participate in a coordinated national cyber incident response.

There is widespread interest by other countries to enhance cybersecurity and prevent cybercrime. The key international instrument that deals specifically with cybercrime is the Council of Europe *Convention on Cybercrime* that Canada signed in 2001. Also known as the *Budapest Convention*, this document serves as a guideline for developing comprehensive national legislation against cybercrime and as a framework for international cooperation between States.