Developments in the Field of Information and Telecommunications in the Context of International Security

Canada reafirms the conclusions of the 2012-2013 Group of Governmental Experts (GGE) report on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98), which recognizes that 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. Canada is hopeful that the next UN GGE report will build on these developments.

Canada also supports the development of work around peacetime norms in cyberspace and views it as a valuable contribution to sustaining a peaceful environment through the promotion of responsible state behaviour.

Taking into account the outcome of the 2012-2013 GGE, and the ongoing work of the 2014-2015 GGE, Canada would like to share with the Secretary-General its views and assessments on the following issues.

1. Cyber 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, cybercrime, use of the Internet for terrorist purposes). As new technologies become increasingly prevalent (e.g. artificial intelligence, cloud computing, Internet of Things), the need to address these challenges will only grow.

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 a free, open and secure Internet.

Canada also believes that addressing the security of Information and Communication Technologies (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.

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 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 engaged in developing new ways to keep strengthening the three pillars of Canada’s Cyber Security Strategy. Current focus on the second pillar of the Strategy includes a stronger engagement between the Government of Canada and the private sector with the common objective to better protect Canada’s major critical infrastructure. Further, the Strategy has allowed for a closer collaboration between departments and agencies that are actively working to improve cyber security.

Canada’s Anti-Spam Legislation (July 2014) is assisting in clarifying legal rights-obligations and respective duties of government agencies, as well as strengthen legislative provisions for enforcement and international collaboration. This legislation generally requires companies to gain a consumer's consent in order to send commercial electronic messages; and helps protect consumers and businesses alike by deterring the most damaging and deceptive forms of spam from occurring in Canada, creating a more secure online environment.
International level

Since 2007, Canada has committed $8 million to support cyber security capacity building projects, primarily in the Americas and more recently in Southeast Asia. Canada has provided $3.6 million since 2007 to the Organisation of American States (OAS) for 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). Canada is also contributing $1.1 million to an INTERPOL-led initiative to enhance cyber security through forensic investigation tools and skills in Southeast Asia. This project is equipping and training ASEAN countries with highly technical forensic tools and skills to investigate cyber-attacks and related crimes. Canada also announced an additional $3.3 million in April 2015 to two initiatives that will combat cybercrime in the Americas. Canada will contribute approximately $2.8 million to INTERPOL, in support of its efforts to establish a more secure and robust cyber infrastructure environment in Central America, and facilitate cooperation and information exchanges on transnational organized crime and terrorism. Canada will also contribute $500 thousand to UNODC’s Global Program in Cybercrime – Internet Crimes Against Children, to enhance the capacity of law-enforcement agencies in Central America to prevent and respond to Internet crimes against children by improving local law-enforcement capacity and making the investigation and prosecution of cybercrime against children a priority. Canada also became a founding partner of the Global Forum on Cyber Expertise (GFCE), a capacity building mechanism focusing on cyber security, cybercrime, data protection and e-governance launched by the Netherlands at the 2015 Global Conference on Cyberspace.

Confidence-building measures (CBMs) are a proven method by which to reduce tensions and the risk of armed conflict, simultaneously encouraging national, bilateral and multilateral cooperation and transparency. In December 2013, CBMs were introduced into the cyber realm with the OSCE’s Confidence-Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies, which provides for communication and information sharing through the OSCE at both the government and expert levels, with the aim of increasing inter-state cooperation and stability. 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; and communication amongst national computer emergency response teams.

Canada supports NATO efforts to strengthen the Alliance’s cyber security and that of individual allies. Canada supported the development of NATO’s enhanced cyber policy, which notably reiterates the commitment of allies to enhance the security of their national networks. Canada also contributes to the development of members’ capabilities and to information-sharing on cyber defence within NATO. Canada is contributing $1 million to the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia to better address regional security challenges related to cyber defence. Canada is providing 1 million to NATO trust funds related to developing Command, Control, Communication, and Computer (C4) capabilities. Canada has also been participating in discussions on the military aspects of cyber security at the annual Seoul Defence Dialogue.

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 and capacity building.

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 cyber security 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, the OAS, and ASEAN. 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 was also a member of 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 more than 40 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 engaging the private sector for small and medium-sized farm business development in Ukraine by providing enterprises with sustainable farm management and crop growing practices using modern information and communication technologies; Strengthening the Capacity of Auditors in Cuba; improving Entrepreneurship and Business Growth for Youth in Ethiopia; and strengthening systems for universal birth registration in Kenya.

For the past 15 years, Canada’s International Development Research Centre (IDRC) has also helped to advance the social and economic prospects within developing countries through supporting ICT for development research and capacity. IDRC supports global networks that seek to help developing countries strike an appropriate balance between the innovative nature of the internet, security, and privacy. There projects include the Cyber Stewards project, a network of Canadian and Southern researchers seeking to better understand how to ensure the future of an open and secure Internet in the global South, and the Protecting Privacy in an Increasingly Digital Developing World project which seeks to add to the evidence-based policy discourse about balancing data collection with data protection and privacy safeguards. Past IDRC support has resulted in outcomes such as the Memorandum of Montevideo, the reference document in Latin American region on how to protect youth’s privacy and personal data on social networks.

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 2012-2013 report of the 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. As work continues, Canada sees the value in promoting peacetime norms to help sustain an environment in which responsible behaviour guides state actions, sustains partnerships, and supports a stable cyberspace.

3. Possible measures to strengthen cyber 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 cyber security 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.