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

Canada reaffirms the conclusions of the 2012-2013 and 2014-15 reports of the UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98 and A/70/174). Canada is pleased to have been selected as a member of the 2016-2017 GGE, and looks forward to building on these outcomes in the coming year.

Taking into account the conclusions of the 2012-2013 and 2014-15 UN 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. cyberbullying, 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 believes that a free, open and secure cyberspace is critical to global security, economic prosperity and the promotion of human rights, democracy and inclusion.

Canada also believes that any approach to tackling cyber threats must go hand-in-hand with respect for human rights and fundamental freedoms. In Canada’s view, human rights and cyber security are complementary and mutually reinforcing. Canada is part of the Freedom Online Coalition (FOC), a group of 29 countries working together to promote Internet freedom issues worldwide. As part of our engagement in the FOC, Canada takes part in a Working Group focused on bringing a human rights framing to cyber security issues.

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 Strategy. Some of the results achieved to date include furthering the Canadian government’s engagement with critical infrastructure partners; launching the “Get Cyber Safe” public awareness campaign; and bolstering the capabilities of the Canadian Cyber Incident Response Centre (CCIRC). The Strategy has also fostered collaboration and information sharing, which Canada views as our best defense in a rapidly evolving threat environment. Recently, the Government has committed to undertaking a review of existing measures to protect Canadians and our critical infrastructure from cyber threats.

Canada’s Anti-Spam Legislation (July 2014) is assisting in clarifying legal rights-obligations and respective duties of government agencies, as well as strengthening 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, thereby creating a more secure online environment.

**International level**

In the 2012-2013 report of the UN GGE on Developments in the Field of Information and Telecommunications in the Context of International Security, 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 value in promoting peacetime norms to help sustain an environment in which responsible behaviour guides state actions, sustains partnerships and supports a stable cyberspace. Canada was a member of the 2012-13 UN GGE and looks forward to actively participating as a member of the 2015-16 UN GGE.

Since 2007, Canada has committed $8.25 million to support cyber security capacity building projects in the Americas and Southeast Asia. Canada has provided $3.85 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 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 supports a $2.8 million project with INTERPOL to establish a more secure and robust cyber infrastructure environment in the Americas and to facilitate cooperation and information exchanges on transnational organized crime. Canada is also contributing $500,000 to the 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 believes that practical Confidence-building measures (CBMs) are a proven method to reduce tensions and the risk of armed conflict, while also encouraging national, bilateral and multilateral cooperation and transparency. In December 2013, a first set of CBMs were introduced in the cyber realm with the OSCE’s Ministerial Decision on 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 CBMs 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 welcomes the second set of CBMs that OSCE members agreed to in March 2016, which aim to reduce the risk of tensions arising from cyber activities. These CBMs focus on cooperation between participating states and include measures to effectively mitigate cyber-attacks on critical infrastructure that could affect more than one participating state. Canada looks forward to participating in discussions on a possible third set of CBMs, which should focus on stability measures and responsible state behaviour, as we believe that practical CBMs can play an important role in advancing peace and security in the use of Information and Communication Technologies (ICTs).

Canada supports NATO efforts to strengthen the Alliance’s cyber defence 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 has contributed $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.

Canada works with the US to protect our shared infrastructure. The Canada-US Cybersecurity Action Plan aims to enhance the resiliency of our cyber infrastructure by implementing measures to improve 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 that are critical to enhancing the cyber security preparedness of both nations. Bilaterally, Canada and the US are also partnering on a cybercrime capacity building initiative that aims to strengthen cyber security and combat cybercrime by delivering regional training workshops for partner countries in the Americas. This initiative will strengthen these countries’ participation in the G7’s 24/7 Network, which connects national law enforcement points of contact in the battle against high-tech crime.

In December 2015, the Royal Canadian Mounted Police (RCMP) released its Cybercrime Strategy, which set out an operational framework and an action plan to help Canada's national police service reduce the threat and impact of cybercrime in Canada. One of the action items in the Strategy was a pledge to expand international collaboration with close allies to better understand and combat cybercrimes that are transnational in character. In response to the growing concern around the online exploitation of children, Canada became a member of the Global Alliance against child sexual abuse online in 2013. It should also be noted that the RCMP is combating online child sexual abuse worldwide as a member of the Virtual Global Taskforce (VGT). The VGT is a multi-national law enforcement body that focuses on identifying, locating and rescuing victims. The VGT also aims to divert those who attempt to use the Internet to abuse and exploit children. The National Child Exploitation Coordination Center (NCECC) is Canada’s main portal for all matters related to the sexual exploitation of children on the Internet, including those destined for international agencies and those originating from foreign agencies and destined for Canada. The NCECC validates international requests and prepares and disseminates investigative packages to the proper jurisdiction within Canada.

For more than 40 years, Canada has supported the use of ICTs as tools for development, including to help community organizations deliver essential services such as emergency assistance in conflicts or natural disasters, or basic education and healthcare to communities in remote regions. Other initiatives have included giving producers and small scale entrepreneurs access to market information, job opportunities, banking services and business and technical skills. ICT-related tools are driving innovation, productivity and efficiency gains across industries, and contributing to overall economic growth and competitiveness. They are connecting people to their governments, strengthening accountability and service delivery and supporting democracy and human rights. In so doing, these tools are 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. Several recent projects include small and medium-sized farm business development in Ukraine that provides tips for sustainable farm management and crop growing practices with ICTs; improving entrepreneurship and business growth for youth in Ethiopia; strengthening the capacity of auditors in Cuba; and strengthening systems for universal birth registration in Kenya.
For almost 30 years, Canada’s International Development Research Centre (IDRC) has also helped to advance social and economic development around the world with ICT for development research and capacity building. IDRC’s capacity building and research efforts around the global South have supported critically important research initiatives facilitated by emerging and now established policy leaders. Many of the organizations in the global South that are responding to cyber policy challenges have received support from IDRC; they include Research ICT Africa (RIA), the Centre for Internet and Society (CIS), Dialogo Regional Sobre Sociedad de la Informacion (DIRSI) and LIRNEasia. Among other projects, IDRC supports global research networks that help policy leaders in developing countries strike a balance between the innovative potential of the Internet on the one hand, and cyber security and digital rights concerns on the other. Projects include the Cyber Stewards network, which convenes Canadian and Southern-based researchers who are generating new ideas for how to ensure an open and secure Internet in the global South. IDRC also supports the network on privacy rights and development that is contributing evidence to policy debates on how to safeguard privacy and protect personal data in a world increasingly dominated by unfettered data collection. One of the many issues emerging from research is that cyber-related issues need broadly informed policy environments that incorporate expertise from overlapping areas – from telecommunications, infrastructure and technology, to economics, law and politics. More than ever, policymakers around the global South need advice grounded in evidence to inform the rules and laws that govern the use of digital technologies. Moreover, researchers in developing countries need sustained resources to support the data gathering and analysis necessary for this critical policy research. To this end, IDRC is supporting cyber policy think tanks in the global South that produce credible and legitimate research that convenes different perspectives on emerging digital issues. Evidence from the recent net neutrality debate in India highlights just how important policy leaders are in the debates confronting the global South. Past IDRC support has resulted in outcomes such as the Memorandum of Montevideo, the reference document in the Latin American region on how to protect youth's privacy and personal data on social networks.

2. International concepts

Canada believes that existing international law is applicable to the use of ICTs by states, and is essential to maintaining peace and stability and to promoting an open, secure, peaceful and accessible ICT environment. Among existing international legal instruments relevant to cyberspace are International Human Rights Law and International Humanitarian Law.

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 on which Canada’s economic prosperity and security rely. Canada is also enhancing collaboration and information sharing with its key partners and within multilateral organizations on cyber security.

The Canadian Cyber Threat Exchange (CCTX) was established in December 2015. It is a private sector led, not-for-profit organization that focuses on sharing actionable information on cyber threats between businesses operating in Canada. This hub will complement existing information sharing hubs in specific sectors by providing a cross-sector venue to share threat information. CCTX is on track to be operational by 2017.

Canada is 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. Since the launch of Canada’s Cyber Security
Strategy, Canada has launched the “Get Cyber Safe” public awareness campaign to raise Canadians’ awareness about cyber threats and provide authoritative advice to Canadians about how to protect themselves online. Canada is also working with the US to align our cyber security public awareness campaign initiatives via the “Stop. Think. Connect.” Coalition.

Many countries have expressed interest in enhancing cyber security and preventing 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 Convention serves as a guideline for developing comprehensive national legislation against cybercrime and as a framework for international cooperation between states. Following the adoption of the Protecting Canadians from Online Crime Act, Canada ratified the Budapest Convention on July 8, 2015 and the Convention entered into force on November 1, 2015. The Convention helps Canada and state parties fight crimes committed against the integrity, availability and confidentiality of computer systems and telecommunications networks. It also helps in the fight against any criminal activity that leaves electronic evidence. Canada fully supports the Budapest Convention as the best tool to fight cybercrime at the international level. Canada encourages countries to bolster their anti-cybercrime efforts by becoming Parties to the Convention, or using it as a model to implement their own cybercrime laws.