Canada's implementation of the 2015 GGE norms

Canada would like to share some of the best practices it has identified and the lessons it has learned on the implementation of previously recognized voluntary, non-binding norms of responsible State behavior endorsed by the UN General Assembly, in case this is useful to other UN member States as they seek to implement the 11 norms laid out in the 2015 GGE report.

Norm 1 – Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are agreed to be harmful or that may pose threats to international peace and security.

Canada has taken a number of steps to increase stability and security in the use of ICTs and prevent the most harmful ICT practices. These steps include:

A) The drafting and updating of comprehensive national cybersecurity strategies.

The Government of Canada's initial Cyber Security Strategy was released in October 2010 and provided a plan to defend against cyber threats. The 2010 Strategy was built on three pillars: (I) Securing Government of Canada systems; (II) Partnering to secure vital cyber systems outside the federal government; and (III) Helping Canadians to be secure online. The 2010 Strategy, and the nation-wide initiatives it introduced through its accompanying Action Plan, bolstered the Government of Canada's capacity to prevent, detect, respond to, and recover from malicious cyber activities. Some of the results achieved included 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. The Strategy also fostered collaboration and information sharing, which Canada views as our best defense in a rapidly evolving threat environment.

Recognizing the evolving cyber landscape, on June 12, 2018, the government, led by Public Safety Canada, released Canada's new National Cyber Security Strategy (NCSS) to strengthen partnerships to secure vital cyber systems both inside and outside the federal government, protect Canadians as they connect online, as well as enhance the detection of, and ability to respond to, continually evolving cyber threats. The new NCSS is organized according to three high-level goals:

1) *Secure and Resilient Canadian Systems*

Through collaborative action with partners and enhanced cyber security capabilities, we will better protect Canadians from cybercrime, respond to evolving threats, and defend critical government and private sector systems.

2) *An Innovative and Adaptive Cyber Ecosystem*

By supporting advanced research, fostering digital innovation, and developing cyber skills and knowledge, the federal government aims to position Canada as a global leader in cyber security.

3) *Leadership, Governance and Collaboration*

The federal government, in close collaboration with provinces, territories, and the private sector, will take a leadership role to advance cyber security in Canada.

The new NCSS was designed to be flexible and remain relevant as the cyber security environment continues to evolve. Similarly, its accompanying activities are not an end state. They represent an incremental step towards achieving Canada's long-term vision of safety and security in the digital age both at home and internationally.

As part of this strategy, Global Affairs Canada will work with Canada's allies, likeminded countries and the international community to shape the international cyber security environment by promoting a free, open and secure Internet, as well as by promoting respect for international law and agreed norms of State behaviour in cyberspace.

B) The development of our cyber capacities to better defend ourselves and prevent malicious cyber activities, in a fully transparent manner.

In implementing Canada's 2018 National Cyber Security Strategy, Canada created the Canadian Centre for Cyber Security, which consolidated the cyber security operational units of the Government of Canada into one public-facing organization. The Cyber Centre is a single unified source of expert advice, guidance, services and support on cyber security for government, critical infrastructure owners and operations, the private sector and the Canadian public. Specifically, the Cyber Centre enables faster, better-coordinated, and more focused Government responses to cyber threats. It provides quicker, more effective information flow between the Government and private sector partners. The Cyber Centre provides a clear national point of contact for authoritative cyber security advice and assistance. The Cyber Centre also aims to provide enhanced public awareness and education about cyber security, improve cyber security skills sharing and information, and provide more regular cyber threat assessments to better inform decision-making and inform federal policy on cyber security. As an outward-facing organization, the Cyber Centre welcomes collaborative partnerships and projects with the Canadian cyber security sector.

Canada's Defence Policy, released on June 7, 2017, recognized the growing threat posed by malicious actors in cyberspace. To help protect and defend Canada, our Defence Policy stated that the Canadian Armed Forces are developing the capability to conduct active cyber operations focused on external threats to Canada in the context of government-authorized military missions. All our missions are subject to all applicable domestic and international law. The 2017 Defence Policy also announced the creation of the cyber occupation in the military to increase the Canadian Armed Forces capacity in this domain.

In June 2019, the *Communications Security Establishment Act* (*CSE Act*) received Royal Assent. It gave the Communications Security Establishment, Canada's signals intelligence agency, the authority to undertake active and defensive cyber operations for the first time. These authorities are needed to allow Canada to better defend against foreign cyber threats before they can damage Canadian systems or information holdings. The legislation also included clear requirements for and restrictions on the exercise of this authority.

Other partners and allies have been similarly transparent about their capabilities and the conditions under which they might be used. Like others, we see this transparency as an important step to avoid misperceptions, reduce uncertainties and foster trust in cyberspace.

C) The promotion, at the international level, of the applicability of international law and of norms of responsible behavior applicable to the conduct of different actors in cyberspace.

To counter cyber threats, Canada has supported the recognition of the applicability of international law in cyberspace, the adoption of voluntary norms for responsible State behaviour, and the development of confidence-building measures. The 2013 and 2015 UN GGE reports recognized the applicability of international law and the 2015 GGE report outlined voluntary norms for State behaviour in cyberspace. These norms were subsequently endorsed in a wide range of international forums, including by the UN General Assembly, the G20 and various regional organizations. Canada has endorsed these norms and is actively working to promote their implementation. One way we have done this is by organizing workshops to help countries better understand the norms and what can be done to implement them. We co-hosted a workshop with Mexico and the OAS on May 30, 2019 that targeted OAS countries, and we organized a similar one targeting Francophonie countries on September 6, 2019.

In our annual submissions to the UN, such as our 2016 submission, and elsewhere, Canada has stated that we believe 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. The international law relevant to cyberspace includes the UN Charter, the law on State Responsibility, including countermeasures, International Human Rights Law and International Humanitarian Law, where applicable.

Canada has also participated in the work of the Internet & Jurisdiction (I&J) Policy Network. Founded in 2012, the I&J has brought together international stakeholders from academia, industry (Internet companies, technical operators), governments, international organizations and civil society groups with over 200 key organizations as members from more than 40 countries. The goal of the I&J Network is to look at developing consensus-based approaches to the challenges created by the cross-border nature of the Internet, in three key policy areas: action at the domain level, dealing with offensive content and ensuring appropriate law enforcement access to data. The I&J Network last met in Berlin in June 2019, where discussions were based on operational approaches to all three areas, with norms, criteria and mechanisms. The I&J Network has also undertaken the creation of a Global Status Report on the state of jurisdiction on the Internet, drawing on the expertise of more than 100 members of the I&J Policy Network.

D) Canada's work with regional organizations on disseminating cyber CBMs

Canada believes that cyber Confidence Building Measures (CBMs) are an important tool to promote stability and security in cyberspace and address cyber incidents by preventing miscalculations and conflict. Canada has been working closely with regional organizations such as the ASEAN Regional Forum (ARF), the Organization of American States (OAS), and the Organization for Security and Co-operation in Europe (OSCE) to disseminate and implement cyber CBMs. For example, Canada has contributed to the ARF's efforts to implement cyber-related CBMs in ASEAN countries by jointly organising a workshop with Singapore in June 2019 on National Strategies on Security in the Use of ICTs. Canada has also recently announced that we will lead efforts to implement OSCE cyber CBM 4, "Participating States [to] voluntarily share information on measures that they have taken to ensure an open, interoperable, secure, and reliable Internet." Canada will indicate to other OSCE participating States how we are implementing this CBM, and provide guidance and best practices on its implementation.

E) Cyber capacity building

Canada's Anti-Crime Capacity Building Program (ACCBP) helps support global efforts to combat cybercrime and threats to cyber security. These projects form a critical part of Canada's engagement strategy to influence countries to share our vision of preserving an open, secure and multistakeholder-led Internet. The Program also enhances the capacities of national authorities to deter, respond to, and investigate cyber threats, including criminal exploitation of ICTs. Since 2015, the ACCBP has contributed over $9M to cyber capacity building, primarily in the Americas. Canada currently programs through international organizations such as the UNODC, OAS and INTERPOL. ACCBP cyber programing also assists nations develop their national cyber strategies, which includes developing standards on how to increase security of ICTs, while at the same time ensuring human rights and privacy are protected for all citizens.

Norm 2 – In case of ICT incidents, States should consider all relevant information, including, inter alia, the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences.

A) Canada's 2018 National Cyber Security Strategy created a streamlined response process to ICT incidents: Until recently, the government of Canada's cyber security operational capabilities were distributed across different departments and agencies. Though measures were in place to ensure good communication and coordination, ambiguity concerning roles and responsibilities and the inherent difficulty in coordinating multiple decision makers was a barrier to the quick, effective, clear, and trusted technical guidance that Canadians have come to expect from their government. To address this gap, the Government of Canada established the new Canadian Centre for Cyber Security within the CSE in October 2018. The Cyber Centre leads Canada's response to cyber security events as the country's National Computer Emergency Response Team (CERT) and the Government of Canada's Computer Incident Response Team (CIRT). The Cyber Centre provides a single point of contact for critical infrastructure owners and operators for advice and guidance in the event of a cyber incident.

The 2018 National Cyber Security Strategy also included funding for the new National Cybercrime Coordination Unit (NC3). While managed by the Royal Canadian Mounted Police (RCMP), the NC3 will serve all Canadian police agencies and will work with public and private sector partners. The NC3 will coordinate and de-conflict cybercrime investigations targeting multiple jurisdictions in Canada and internationally, and will implement a new public reporting system to make it easier for Canadian victims to report cybercrime incidents to law enforcement. The NC3 will work closely with the Cyber Centre to address cyber threats. The NC3 will have initial operating capability by April 2020, and the new public reporting system is planned for 2022.

B) Canada has participated in public attributions of activities that it deems to be unacceptable State behaviour. In undertaking its attribution process, Canada considers the larger context of the event, the challenges of attribution in the ICT environment, relevant international law and voluntary norms, and the nature and extent of the consequences of the incident.

C) Through international cyber capacity building Canada has assisted countries implement or improve their Computer Security Incident Response Teams (CSIRTs), which allow for real time information sharing between nations on cyber incidents, including the misuse of ICTs. Canada also works with police forces and judiciary systems of foreign nations to increase their capacity of cyber forensics and investigation, attribution, and prosecution of those who use ICTs for criminal or exploitative purposes.

Norm 3 – States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

Canada considers that States have a responsibility to ensure that their territory is not used in a way that harms the rights of other States. If Canada is contacted about incidents on our territory, we will take appropriate action to contain the harmful behaviour. Furthermore, in order to ensure that our territory is not used to commit internationally wrongful acts, Canada has:

A) Developed legislation to prosecute cyber criminals: Canada's *Criminal Code* includes a number of offences that can apply to the actions of cyber criminals, as well as investigative tools that may be relevant to investigate these activities. This includes production orders, and preservation demands and orders, which are used to ensure evidence is not deleted prior to obtaining authority for access by investigators. A key offence in this regard is found in section 342.1, the offence of unauthorized use of a computer, which provides:

"Everyone is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction who, fraudulently and without colour of right,

(a) obtains, directly or indirectly, any computer service;
(b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system;
(c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or under section 430 in relation to computer data or a computer system; or
(d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)."

Possession of a device to obtain unauthorized use of a computer system or commit mischief is also criminalized, under section 342.2.

Another relevant offence in this context is section 430(1.1), mischief in relation to computer data, which provides:

"Everyone commits mischief who wilfully

(a) destroys or alters computer data;
(b) renders computer data meaningless, useless or ineffective;
(c) obstructs, interrupts or interferes with the lawful use of computer data; or
(d) obstructs, interrupts or interferes with a person in the lawful use of computer data or denies access to computer data to a person who is entitled to access to it."

The punishment for this offence is found at section 430(5) and (5.1), which state:

"(5) Everyone who commits mischief in relation to computer data

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
(b) is guilty of an offence punishable on summary conviction.

(5.1) Everyone who wilfully does an act or wilfully omits to do an act that it is their duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or computer data,

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or

(b) is guilty of an offence punishable on summary conviction."

B) Prosecuted cyber criminals: The RCMP has successfully investigated and prosecuted several cyber criminals. For example, an RCMP investigation into leakedsource.com recently resulted in a guilty plea by a 27-year-old Ontario man who sold large numbers of stolen passwords online through the now-defunct service Leakedsource.com.

In another example dating back to 2018, Karim Baratov was arrested in Canada in connection with a security breach at Yahoo. The RCMP and FBI investigated this individual and he was prosecuted in the U.S., resulting in a 5 year prison sentence and a $250,000 US fine. Several other cases involving cyber criminals are currently before Canadian courts.

C) Promoted the patching of vulnerabilities: The Cyber Centre regularly issues alerts and advisories on potential, imminent, or actual cyber threats, vulnerabilities, or incidents affecting Canada's critical infrastructure.

D) Capacity building: Canada works through international organizations such as UNODC, INTERPOL, the Council of Europe and the OAS to assist countries in developing their legal framework around cybercrime and the capacity of their law enforcement institutions in order to prevent and combat cybercrime, as well as to address the effects and impacts of new information technologies on the abuse and exploitation of citizens. This also greatly improves the capability of nations to effectively investigate and prosecute cybercriminals in a manner that aligns with international norms and human rights.

Norm 4 – States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs, and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

Canada has developed an array of measures to increase its cooperation with its partners to prevent terrorist and criminal use of ICTs, such as:

A) Adopting and promoting the Budapest Convention:
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 for Canada 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. Now that Canada is a party to the Budapest Convention, the RCMP responds to a significant number of requests from other States pursuant to the Convention. 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.

Canada is actively participating in the works of the Council of Europe to develop an additional protocol to the Budapest Convention in order to further develop the cooperation among law enforcement and judicial authorities at the international level, including in the field of access to electronic evidence. In addition, at Canada's suggestion, the Quintet of Attorneys General (which brings together Attorneys General from Canada, the US, Australia, New Zealand and the UK) issued a public statement at their July 31, 2019 meeting, expressing their support for the Budapest Convention as an effective global framework to support the fight against cybercrime, and for the work currently being done by the United Nations Open-Ended Intergovernmental Expert Group on Cybercrime (UNIEG).

B) Promoting the adoption of a draft resolution on cybercrime: At the 28th Session of the United Nations Commission on Crime Prevention and Criminal Justice (CCPCJ) in May 2019, Canada tabled, with Austria's support, a draft resolution on cybercrime, stressing the importance of technical assistance in this context. The resolution was adopted by consensus and referred to the United Nations' General Assembly.

C) Capacity building: Since 2015, Canada has disbursed over $9.1M to cyber security capacity building, primarily in the Americas. Programming of this nature falls under the mandate of Global Affairs' ACCBP. Canada's current international cyber security programming is provided through several international partners, including the OAS, INTERPOL, and the United Nations Office on Drugs and Crime (UNODC).

By partnering with the OAS on cyber capacity building projects, Canada seeks to encourage States to ratify the Budapest Convention by helping them develop their own national cyber strategies in order to meet the convention's standards for ratification. These projects also help to establish or improve CSIRTs throughout the Americas. With Canadian funding, the OAS has been able to launch the CSIRTAmericas.org website, which functions as a centralized platform for all CSIRTs to share information and develop coordinated responses to cybercrime and threats to cyber security.

D) At the June 2018 Charlevoix Summit, G7 Leaders announced the creation of the **Rapid Response Mechanism (RRM)**. The RRM is mandated to coordinate G7 efforts to identify and respond to diverse and evolving threats to our democracies, including through information sharing and analysis, and identifying opportunities for coordinated responses. The RRM is meant to address a broad spectrum of threats to democracy. The illustrative examples identified by Ministers during their April 2018 Toronto meeting were grouped under three headings: 1) Institutions and Processes; 2) Disinformation and Media; and 3) Fundamental Freedoms and Human Rights. The RRM consists of Focal Points from G7 members, together with the EU, responsible for delivering on the Charlevoix commitment. Each Focal Point is positioned to leverage its own national or institutional structures and processes. Canada coordinates the RRM on an ongoing basis. To operationalise the RRM and ensure its smooth functioning, the RRM Coordination Unit was stood-up at Global Affairs Canada. While the RRM is a G7 entity, the RRM also engages with other likeminded countries and interlocutors who share our interest and expertise in protecting democracy from foreign threats. Recently, Australia, Lithuania, the Netherlands and New Zealand were included in the RRM information sharing network. This network also includes over 100 experts representing think tanks, academic institutions and multilateral organizations.

E) Canada's *Criminal Code* contains a number of offences and investigative tools that are relevant to the criminal misuse of the Internet, including for terrorist purposes.

The *Criminal Code* contains a number of terrorism offences, which are largely designed to prevent the carrying out of a terrorist activity. For example, the *Criminal Code* includes an offence of knowingly participating in or contributing to any activity of a terrorist group for the purpose of enhancing the ability of any terrorist group to facilitate or carry out a terrorist activity (s 83.18 of the *Criminal Code*).

Sections 22 and 464 of the *Criminal Code* are general counselling offences that can be applied to the counselling of terrorism offences as well as other criminal offences. Counselling is defined to include soliciting, procuring or inciting (subsection 22(3) of the *Criminal Code*). As well, there is the specific terrorism offence in section 83.221 of the *Criminal Code* of counselling another person to commit a terrorism offence without identifying a specific terrorism offence. The offence may be committed whether or not a terrorism offence is committed by the person who is counselled. The definitions of "terrorist activity" and "terrorism offence" in the *Criminal Code* expressly include counselling.

In addition, section 320.1 of the *Criminal Code* allows a judge to order to deletion of hate propaganda that is stored on and made available to the public though a computer system that is within the jurisdiction of the court. Also, section 83.223 of the *Criminal Code* allows a judge to order to deletion of terrorist propaganda that is stored on and made available to the public though a computer system that is within the jurisdiction of the court. Both "hate propaganda" and "terrorist propaganda" are defined terms in the *Criminal Code* (subsections 320(8) and 83.222(8)). Similar authorities for the removal of offensive content from the Internet are available in the *Criminal Code* in relation to child pornography and other prohibited sexual content such as voyeuristic recordings in section.164.1 and in relation to hate propaganda in section 320.1, as noted above.

Canada is also able to cooperate with other States, and has a statutory framework specifically in relation to this cooperation (*Mutual Legal Assistance in Criminal Matters Act*).

F) Establishing strong partnerships at the technical level:

The Cyber Centre has strong partnerships with other organizations in the Government of Canada, the private sector and internationally. Within the Government of Canada, the Cyber Centre provides cyber security expertise to support lead agencies in the delivery of their core functions, including collaborating with the RCMP to address cybercrime. The Cyber Centre has also established partnerships at the technical level with Canada's critical infrastructure owners and operators in order to share enhanced cyber threat information, as well as to promote the integration of cyber defence technology. Finally, the Cyber Centre works closely with foreign counterparts and other national Computer Incident Response Teams (CIRTs) and Computer Emergency Response Teams (CERTs).

G) Canada's work with regional organizations on cyber CBMs also helps build partnerships at the technical level. For example, Canada has participated in several OSCE exercises that used the "points of contact" CBM to share information among participating States' points of contact (at both the technical and policy level) during simulated cyber crises. These contacts could be used to defuse real crises by allowing CERTS, Interior and Foreign Ministries and relevant technical points of contact to communicate rapidly during a real cyber incident.

Norm 5 – States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions A/HRC/RES/20/8 and A/HRC/RES/26/13 (The promotion, protection and enjoyment of human rights on the Internet), as well as General Assembly resolutions A/RES/68/167 and A/RES 69/166 (The right to privacy in the digital age), to guarantee full respect for human rights, including the right to freedom of expression;

A) Canada's position on human rights and privacy online: Canada believes that addressing the security of ICTs 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 and privacy rights. All States must respect their international human rights obligations in cyberspace. They should also apply the human rights commitments they made at the Human Rights Council and the General Assembly.

B) The protection of human rights in Canada is founded on a system of representative and responsible government, constitutional guarantees, statute law, including specialised human rights legislation, the common law and an independent judiciary. The legislative, executive, and judicial branches of government, at all levels of government in Canada, share responsibility for the protection of human rights. Relevant legislation is enacted by Parliament and the provincial and territorial legislatures. Numerous departments and agencies work within the executive branch to formulate policies and programs and take into account Canada's human rights obligations in their work.

Canada has adhered to UN human rights treaties and Optional Protocols including the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR).

The Constitution of Canada includes the *Canadian Charter of Rights and Freedoms*, which guarantees the fundamental freedoms of conscience and religion, of thought, belief, opinion, and expression (including freedom of the press and other media), of peaceful assembly, and of association; democratic rights; mobility rights; the right to life, liberty, and security of the person, and the right not be deprived thereof except in accordance with the principles of fundamental justice; various rights relating to the legal process, including the right to be secure against unreasonable search and seizure; the right to equality before and under the law and the right to the equal benefit and protection of the law without discrimination; recognition of French and English as the two official languages of Canada; and minority-language educational rights.

All governments in Canada have adopted legislation prohibiting discrimination on various grounds, by government and by private sector actors, regarding employment matters, the provision of goods, services, and facilities customarily available to the public, and accommodation. Statutes on freedom of information and privacy exist at both the provincial/territorial and federal level to help protect individuals' right to privacy (vis-à-vis both public via the Privacy Act - and private-sector entities - via the Personal Information Protection and

Electronic Documents Act) and provide a right of access to information that is in the custody or control of government.

C) Through Canadian funded cyber capacity building projects, human rights considerations are always integrated in various forms, including: by encouraging beneficiary governments to include civil society human rights groups in processes leading to the development of cybersecurity strategies; by inviting the Inter-American Commission on Human Rights (IACHR) and its Special Rapporteur on Freedom of Expression to provide expertise in relevant project activities; by inviting human rights civil society organizations to participate in regional events sponsored through projects and; by promoting discussions on human rights and cybersecurity through awareness-raising activities.

Norm 6 – A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

Canada has made it clear that any government of Canada cyber operations will be conducted in full compliance with international law. For example, Canada's 2017 Defence Strategy indicated that "cyber operations will be subject to all applicable domestic law, international law, and proven checks and balances such as rules of engagement, targeting and collateral damage assessments."

Norm 7 – States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account, inter alia, General Assembly resolution 58/199 (2003) "Creation of a global culture of cybersecurity and the protection of critical information infrastructure", and other relevant resolutions;

A) As specified in the Action Plan 2010-2015 for Canada's Cyber Security Strategy, the following actions have been taken since 2001 to protect Canada's critical infrastructure from ICT threats:

Action	**Timeline**	**Deliverable**	**Status**
Develop a new process to coordinate a national response to major cyber incidents.	Start: 2012	Develop a Cyber Incident Management Framework.	
Engage owners and operators of Canada's critical infrastructure, using the mechanisms established under the National Strategy and Action Plan for Critical Infrastructure.	Start: 2010	Provide cyber security briefings to all sector networks.	Ongoing
	Start: 2013	Develop and implement a strategy to engage CEOs on cyber security.	
Engage provinces and territories on cyber security, to seek their active engagement in improving the cyber security of their systems and vital systems under their jurisdiction.	Start: 2011	Establish the Federal Provincial and Territorial Assistant Deputy Minister Committee on cyber security.	Completed
		Obtain security clearances for, and provide classified briefs to the National Chief Information Officer Sub Committee on Information Protection which includes provinces and municipal representatives.	Completed

		Develop and implement information sharing arrangements and protocols.	Ongoing
	Start: 2001	Operate a Federal/Provincial/Territorial Coordinating Committee of Senior Officials Cyber Crime Working Group.	Ongoing
Develop a Cyber Security Partnership Program for vital systems outside the government to provide tangible support to their owners and operators.	Start: 2010	Organize workshops across the country to improve awareness and understanding of the threats to industrial control systems.	Ongoing
		Establish an Industrial Control System laboratory program and testing environment – the National Energy Infrastructure Test Center.	Completed
		Operate the Industrial Control System laboratory program and testing environment.	Ongoing
		Develop and implement a grant and contribution program.	
		Design and implement other program elements, in consultation with owners and operators of vital systems	Ongoing

B) Canada's 2018 National Cyber Security Strategy aims to further protect Canada's critical infrastructure from ICT threats. Budget 2018 earmarked $507.7 million over five years, and $108.8 million per year thereafter, for the implementation of the Strategy – representing the single largest investment in cyber security made by the Canadian government thus far. This funding is supporting 14 ongoing initiatives led by eight different federal government departments. These initiatives are detailed in a new National Cyber Security Action Plan, released in August 2019. The Action Plan provides a blueprint for the implementation of the Strategy, and includes specific milestones and timelines, respective to each initiative (see tables below).

INITIATIVE	DEPARTMENT	ACTION/MILESTONE	TARGET END DATE	STATUS
Goal 1: Secure and Resilient Systems				
Supporting Canadian Critical Infrastructure Owners and Operators	Public Safety Canada (PS)	Acquire/develop a technical cyber assessment tool	2019	Planned
		Establish an Industrial Control System (ICS) Advisory Committee	2019	Completed
		Increase the number of cyber security exercises delivered to critical infrastructure stakeholders	2020	Planned
		Develop technical ICS security training and awareness solution	2020	Planned

Improved Integrated Threat Assessments	Communications Security Establishment (CSE)	Increase capacity to enable CSE to better meet increasing demands for cyber threat assessments	2024	In Progress
		Increase capacity to enable CSE to assess a wider array of cyber threats reflecting the Cyber Centre's growing client base	2024	In Progress
Preparing Government of Canada Communications for Advances in Quantum	Communications Security Establishment (CSE)	Protect Government of Canada's classified information against anticipated advancements in quantum computing	2024	In Progress
Expanding Advice and Guidance to the Finance and Energy Sectors	Communications Security Establishment (CSE)	Finance and energy sectors work cooperatively with the Cyber Centre and within their sectors to improve their cyber security postures	2024	In Progress
		Improve cyber security posture of the finance and energy sectors	2024	In Progress
Cyber Intelligence Collection and Cyber Threat Assessments	Canadian Security Intelligence Service (CSIS)	Augment CSIS collection of national security cyber intelligence and cyber threat assessments	2023	Planned
National Cybercrime Coordination Unit (NC3 Unit)	Royal Canadian Mounted Police (RCMP)	Reach initial operating capability	2020	In Progress
		Establish NC3 Unit Advisory Group	2021	In Progress
		Launch the National Cybercrime and Fraud Public Reporting System	2022	In Progress
		Reach full operating capability	2023	In Progress
Federal Policing Cybercrime Enforcement Capacity	Royal Canadian Mounted Police (RCMP)	Deploy cyber specialists abroad	2020	In Progress
		Establish/support cybercrime investigative teams	2021	In Progress
		Recruit/train cyber capability specialists	2021	In Progress

INITIATIVE	DEPARTMENT	ACTION/MILESTONE	TARGET END DATE	STATUS
Goal 2: An Innovative and Adaptive Cyber Ecosystem				
Cyber Security Student Work Placement Program	Employment and Social Development Canada (ESDC)	Launch student work-integrated learning program	2018	Completed
		Complete student work-integrated learning program and conduct evaluation	2021	Planned
Cyber Security Assessment and Certification for Small and Medium-Sized Enterprises (SMEs)	Innovation, Science, and Economic Development (ISED), with CSE and SCC	Develop security controls in collaboration with CSE	2019	Completed
		Launch cyber education and awareness tool	2019	In Progress
		Launch cyber certification program	2019	In Progress
		Launch national standard for cyber security	2020	Planned

INITIATVE	DEPARTMENT	ACTION/MILESTONE	TARGET END DATE	STATUS
Goal 3: Effective Leadership, Governance, and Collaboration				
Strategic Policy Capacity in Cyber Security and Cybercrime	Public Safety Canada (PS)	Recruit strategic policy team	2022	In Progress
		Undertake annual progress review	2021-2024	Planned
		Undertake governance review	2021	Planned
Cyber Security Cooperation Program (CSCP)	Public Safety Canada (PS)	Launch the renewed CSCP	2019	Planned
		Conduct program marketing	2019	Planned
		Initiate Call for Proposals	2019	Planned
		Disburse project funding	2019	Planned
Canadian Centre for Cyber Security	Communications Security Establishment (CSE)	Virtual launch of the Canadian Centre for Cyber Security (the Cyber Centre)	2018	Completed
		Achieve basic operating capability	2022	In Progress
		Achieve full operating capability	2023	In Progress
International Strategic Framework for Cyberspace	Global Affairs Canada (GAC)	Launch International Cyber Engagement Working Group	2018	Completed
		Create cyber unit at Global Affairs Canada	2019	Completed
		Develop International Cyber Strategy	2019	In Progress
		Undertake cyber-related capacity building	2019	In Progress
		Develop attribution policy	2019	Completed
		Staff Washington Mission position	2020	Completed
		Host relevant cyber security meetings	2024	In Progress
		Support international participants in cyber negotiations	2024	In Progress
		Promote Canadian interests and values on cyber issues in international forums	2024	In Progress
Bilateral Collaboration on Cyber Security and Energy	Natural Resources Canada (NRCan)	Recruit and hire core staff for the Bilateral Collaboration Team	2019	In Progress
		Launch initial call for expressions of interest and proposals for projects	2019	Completed
		Sign contribution agreements and disburse funding for first round projects	2019	In Progress
		Launch second call for expressions of interest and proposals for projects (if required)	2020	Planned
		Sign contribution agreements and disburse funding for second round projects (if required)	2020	Planned
		Participate in key information sharing activities, workshops, and briefing sessions with the U.S. government	2023	In Progress
		Advance joint initiatives with U.S. partners on cyber security and energy (e.g. tabletop exercises, R&D, information sharing)	2023	In Progress

C) In addition to those initiatives funded under the Strategy, **Budget 2019 also earmarked $144.9M to strengthen the cyber security of Canada's critical infrastructure**, with the specific intent to protect critical cyber systems (CCS) in the finance, telecommunications, energy, and transport sectors. An additional $80M was also allocated to support research, expand private sector partnerships, and grow the pipeline of cyber security talent through the creation of university-affiliated cyber security networks.

D) Canada continues to offer cyber vulnerability assessments to owners and operators of critical infrastructure (CI) in Canada through Public Safety Canada's Regional Resilience Assessment Program (RRAP). RRAP cyber assessments are based on the NIST Cyber Security Framework and evaluate an organization's cyber posture relative to 10 domains such as configuration management, vulnerability management, and situational awareness. Participants get scores that allow industry comparison, and reports that identify gaps in capabilities for remediation. Since 2013, the assessments have helped Canada raise CI operator awareness of cyber resilience and have enabled operators to take action to improve their cyber security postures in over 80 cases.

Through the Industrial Control Systems Security (ICS) Symposium and the hands-on ICS Technical Workshops, Canada continues to bring together ICS experts from across the 10 CI sectors to provide training and to share tools and information to better protect ICS from cyber disruptions and assist CI owners and operators to better protect their most critical ICS and IT systems. In 2018, the ICS Security Symposium Advisory Committee was established as a mechanism to broaden engagement with the ICS community in Canada and to help guide the strategic planning of the ICS Security Symposium.

Canada is also expanding the current cyber-based exercise offering to the CI community. This will include more frequent and recurring CI interdependency exercises and the development of exercises for CI owners and operators to exercise their cyber capabilities. These exercises aim to increase the resilience of the CI community by helping them identify and mitigating cyber vulnerabilities.

E) Cyber Capacity building helps countries enhance the skills of policy-makers and the knowledge of governments and critical infrastructure operators to detect cyber threats, prevent, respond to, and recover from cyber incidents. This is done through activities such as organizing technical trainings at the national, sub-regional or regional level for information security technicians, critical infrastructure operators and law enforcement officers. Training topics have included critical infrastructure and industrial control systems protection, basic and advanced incident response techniques, digital investigative techniques and combatting the use of the Internet for criminal and terrorist purposes.

Norm 8 - States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at another State's critical infrastructure emanating from their territory, taking into account due regard for sovereignty;

When Canada receives a request for assistance from another State whose CI is subject to malicious ICT acts, we respond and do our best to assist that State, and to address any threat emanating from Canadian territory.

A) Canada is active in many fora that encourage information sharing and cooperation during incidents. Canada is also an active participant in regional organizations, particularly the OSCE, that have established CBMs to encourage support and information sharing on incidents.

B) One of the key goals of the **Cyber Centre** is to work collaboratively with Canada's critical infrastructure owners as well as all levels of government, academia, and private industry to combat these threats.

The passage of the *CSE Act* in June 2019 also gave the Cyber Centre new authorities to share cyber threat advice, guidance, and services with the owners of critical infrastructure. For example, the legislation authorized the Cyber Centre to deploy its unique cyber security tools onto non-Government systems, when those systems have been designated by Canada's Minister of National Defence as systems of importance to the Government of Canada. These activities could also only be conducted at the request of the owners of those systems.

C) Canada's capacity building efforts continually seek to improve information-sharing, coordination and cooperation throughout the Americas and with the international community in order to better respond to the transnational nature of cyber threats. This includes technical level collaboration among CSIRTs, legal cooperation in the fight against cybercrime and hemispheric political dialogue around international law and voluntary norms of behaviour in cyberspace.

Norm 9 – States should take reasonable steps to ensure the integrity of the supply chain, so end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

A) The Canadian Centre for Cyber Security works closely with stakeholders in critical sectors to provide advice and guidance to help mitigate supply chain risks in critical infrastructure that Canadians rely on every day. For example, since 2013, the CSE's Security Review Program has helped mitigate supply chain threats to the telecommunications sector for 3G, 4G and LTE technology. To date, CSE and its government partners have worked with companies representing over 99% of the Canadian mobile market to help mitigate the risk of cyber espionage and network disruption. This program has helped mitigate risk by excluding designated equipment and services from sensitive areas of Canada's telecom networks.

B) Efforts to enhance IoT security to reduce risks and build consumers trust

At the 2019 Five Country Ministerial, Canada and its likeminded partners committed to supporting 'security by design' in their respective industries on connected devices, or IoT. Beyond the Five Eyes, Canada is aligning itself with the EU, Japan and the OECD to signal how security and trust can be supported in the IoT market. Canada recently concluded a year-long multistakeholder initiative with the Internet Society (ISOC). The final report was released to showcase the work of this group and signal where Canadian stakeholders are getting involved on IoT security issues globally. At a high level, there is agreement among governments that:

- There should be an evergreen baseline level of security for IoT devices that can be urgently implemented by manufacturers. National industry bodies and consumer protection agencies can support setting this baseline.
- New regulation, or application of existing marketplace frameworks (e.g., PIPEDA), can enforce baseline requirements. It is unclear what degree or target of government action will be necessary to meaningfully address IoT security.
- International cooperation– instead of competition – across fora is vital. Information sharing and collaboration will help advance shared goals (e.g., on standards etc.)
- There are many opportunities to raise consumer awareness on IoT security. Governments and non-government organizations are expected to leverage education efforts to supplement other work on standards, marketplace frameworks, etc.

Norm 10 – States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities, in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

The **Cyber Centre** issues alerts and advisories on potential, imminent or actual cyber threats, vulnerabilities or incidents affecting Canada's critical infrastructure.

The **CSE's Equities Management Framework** is a standardized decision-making process used by CSE to identify information technology vulnerabilities. The framework helps CSE manage discovered vulnerabilities in a responsible way.

Norm 11 – States should not conduct or knowingly support activity to harm the information systems of another State's authorized emergency response teams (sometimes known as CERTS or CSIRTS). A State should not use authorized emergency response teams to engage in malicious international activity;

Canada will not conduct or knowingly support any activities to harm another State's CERT, nor use our own CERT to engage in malicious international activity.