Canada

Submission of draft text and contributions on the specific chapters and provisions to be examined during the second session of the Ad Hoc Committee, namely on criminalization, general provisions and procedural measures and law enforcement

In preparing this submission, Canada is inspired by the important work that has been done within the United Nations (UN) on cybercrime over more than twenty years under the auspices of the United Nations Commission on Crime Prevention and Criminal Justice, in particular by the United Nations Intergovernmental Expert Group on Cybercrime, the United Nations Office on Drugs and Crime through its Global Programme on Cybercrime and the United Nations Congresses on Crime Prevention and Criminal Justice.

The UN General Assembly Resolution 74/247 establishing the Ad Hoc Committee states that the elaboration of "a comprehensive international convention on countering the use of information and communications technologies for criminal purposes" shall be "taking into full consideration existing international instruments". Consequently, Canada's submission on the criminalization, procedural powers and general provisions takes into consideration, and in some circumstances replicates, relevant provisions included in the United Nations Convention against Transnational Organized Crime (UNTOC), the United Nations Convention against Corruption (UNCAC) and the Council of Europe Convention on Cybercrime.

Definitions (related to the criminalization and procedural powers provisions)

Definitions	**Rationale and practical examples**
"computer system" means any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or telecommunications functions.	This definition would include most technological means that may be used to process and communicate data, including computer systems, cell phones, satellites, fax and telephone (whether digital or analogue, wired or wireless).
"computer data" means any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.	This definition would include all types of data: content data (the actual message), computer programs, traffic data, subscriber information, passwords, and connexion codes.
"traffic data" means any computer data to identify, activate or configure a device relating the creation, transmission or reception of a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the	This definition includes, for both telephony and internet services, the data necessary for dialing, routing and addressing or signalling; for example: phone numbers, date and time of a call (and other elements in call data logs), the source and destination of messages (such as

communication's origin, destination or termination, route, time, date, size, duration, or type of underlying service.	email or text messages), as well as IP addresses and data pertaining to the protocol used. This definition excludes content data and differs from subscriber information (which involves attribution of a communication to a person or the linkage between a device and a specific person).
"service provider" means: a) any public or private entity that provides to users of its service the ability to communicate by means of a computer system, including over the Internet; and b) any other entity that processes or stores computer data that is available over the Internet.	This definition would include access providers (telephone and Internet), social media platforms, and online data storage services/Cloud services.

General provisions

	Rationale	**Proposed text**
Purpose	This provision would set out the overarching objective or purpose of the convention.	The purpose of this convention is to promote cooperation in the prevention, investigation and prosecution of cybercrime more effectively.
Scope of application	This provision would set out the scope of application of the convention, by providing greater detail regarding the means by which the convention aims to meet the goals set out in the purpose provision.	This convention shall apply, except as otherwise stated and subject to appropriate safeguards: 1. to promote and strengthen legislative and other measures to prevent, investigate and prosecute cybercrime and serious offences that are frequently committed through the use of computer systems as established in the convention; 2. to promote, facilitate and support international cooperation and assistance in relation to the prevention, investigation and prosecution of offences established in this convention; 3. to promote, facilitate and support efficient and effective mutual legal assistance in relation to electronic evidence pertaining to the offences established in this convention and any other criminal offences; and 4. to promote, facilitate and support technical assistance in the prevention of and fight against cybercrime.

Conditions and safeguards	Cybercrime has a devastating impact on victims, including through the violation of their privacy rights. Likewise, efforts to investigate and prosecute cybercrime can potentially infringe upon human rights, including privacy rights, due process rights and freedom of expression. It is therefore imperative that conditions and human rights safeguards be incorporated into this convention.	1. Each State Party shall ensure that the establishment, implementation and application of the provisions of this convention are subject to conditions and safeguards provided for under its domestic law, which shall provide for the full protection of human rights and liberties, including rights arising pursuant to obligations under the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principles of the rule of law, legality, necessity and proportionality. 2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of the power or procedure. 3. Each State Party shall implement measures to improve our understanding of the linkages between gender and cybercrime, including the ways in which cybercrime can affect women and men differently. The measures shall aim to promote gender equality and the empowerment of women, including by mainstreaming it in relevant legislation, policy development, research, projects and programmes, as appropriate and in accordance with the fundamental principles of domestic law. 4. The measures set forth in this Convention shall be interpreted and applied in a way that does not interfere with freedom of expression, including freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of choice, and applicable rights concerning respect for privacy and data protection. The interpretation and application of those measures shall be consistent with

		internationally recognized principles of non-discrimination.
Participation and attempt	The purpose of this provision would be to ensure that criminal liability for participation and attempt in cybercrime offences is covered in domestic legislation.	1. Each State Party shall adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, participation in any capacity such as an accomplice, assistant or instigator in an offence established in accordance with this convention. 2. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, any attempt to commit an offence established in accordance with this convention. 3. Each State Party may adopt the necessary legislative and other measures to establish as a criminal offence, in accordance with its domestic law, the preparation for an offence established in accordance with this convention.
Corporate liability	This provision would deal with the liability of legal persons – corporations, associations and similar legal persons - for the criminal actions undertaken for the benefit of the legal person.	1. Each State Party shall adopt the necessary legislative and other measures, consistent with its legal principles, to establish the liability of legal persons for participation in the commission of the offences established in the convention. 2. Subject to the legal principles of the State Party, the liability of legal persons may be criminal, civil or administrative. 3. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offences. 4. Each State Party shall, in particular, ensure that legal persons held liable in accordance with this article are subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

Criminalization

The criminalization provisions would require State Parties to have in their domestic law baseline offences using technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved.

Offences	Rationale and examples	Proposed text
Illegal access to a computer system	This provision would criminalize fraudulent and illegal access (hacking) to a computer as this is the first step to almost all forms of cybercrime, such as DOS and DDOS attacks, computer trespass, critical infrastructure attacks, botnets, malware, spyware, illegally accessing connexion codes, and ID and personal data for identity theft/phishing.	Establish as a criminal offence to, fraudulently and without right, access the whole or any part of a computer system.
Illegal interception of non-public computer system transmission	This provision would be aimed at protecting the right to privacy in non-public transmission of communications. Illegal interception can also be a precursor to other criminal activity, for example botnets, malware, spyware, identity theft/phishing, computer trespass and critical infrastructure attacks, unauthorized tapping and recording of private telephone communications or emails.	Establish as a criminal offence to, fraudulently and without right, intercept, by any technical means, non-public transmissions of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such data.
Computer data interference	This provision would criminalize unlawful acts affecting the integrity and proper functioning or use of stored computer data, such as offences targeting computer systems and networks, and/or computer data. Illegal computer data manipulation is involved in many cybercrime manifestations like defacing of websites, spoofing, ransomware, Trojan horses, DDOS attacks and viruses, fraud, modification of IP packet header (to conceal identity of perpetrator), botnets, malware, spyware, identity theft/phishing, computer trespass and critical infrastructure attacks.	Establish as a criminal offence to, intentionally and without right, damage, delete, deteriorate, alter, or suppress computer data.

Computer system interference	This provision would target illicit acts that seriously interfere with the proper functioning of a computer system through the manipulation of data. Computer data interference that results in serious computer system failure or malfunction is a common element to many cybercrimes, for example computer system sabotage, ransomware, Trojan horses, DDOS attacks and viruses, fraud, modification of IP packet header (to conceal identity of perpetrator), botnets, malware, spyware, identity theft/phishing, computer trespass and critical infrastructure attacks.	Establish as a criminal offence to, intentionally and without right, seriously hinder the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data.
Misuse of devices	This provision would criminalize the development and dissemination of devices and hacking tools/malware designed to facilitate the commission of an offence targeted at computer systems or computer data. This offence would target the means by which cybercriminals commit a wide range of offences - thereby attacking the cybercriminal supply chain at its source. Examples include spyware, hacking software, online selling of stolen ID, passwords, connexion codes, banking information, and malware.	1. Establish as criminal offences, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution, or otherwise making available of: i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the cybercrime offences included in this convention, ii) a computer password, access code, or similar data by which the whole or any part of a *computer system* is capable of being accessed, with intent that it be used for the purpose of committing any of the cybercrime offences included in this convention; and b) the possession of an item referred to in paragraphs a(i) or (ii), with intent that it be used for the purpose of committing any of the cybercrime offences included in this convention. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use,

		import, distribution, or otherwise making available or possession referred to in paragraph 1 is not for the purpose of committing a cybercrime offence included in this Convention, such as for the authorised testing or protection of a computer system.
Child sexual exploitation related offences	This provision is aiming at 1) protecting children from sexual exploitation and abuse and 2) addressing the supply and demand for child sexual exploitation material (CSEM) which normalizes the behaviour and puts more children at risk. Including CSEM offences which are cyber-enabled in this convention, is justified due to the widespread use of the Internet for child sexual exploitation and the significant and lasting harms of such offences on the victims. Consideration should be given to limiting criminal liability for making and possessing CSEM that is self-generated, depicts lawful sexual activity and was made and possessed for the person's personal use (for example 2 persons who are under 18 years of age but above the age of consent to lawful sexual activity). Examples of situations that would be captured by this offence include trafficking in CSEM, child exploitation rings where production of CSEM takes place and is live streamed as well as activities of NAMBLA and similar groups.	1. Establish as criminal offences, when committed intentionally and without right, the following conduct: a) producing child sexual exploitation material for the purpose of its distribution through a computer system; b) offering, advertising, or making available child sexual exploitation material through a computer system; c) distributing or transmitting child sexual exploitation material through a computer system; d) procuring child sexual exploitation material through a computer system for oneself or for another person; e) accessing or possessing child sexual exploitation material in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1, the term "child sexual exploitation material", includes child pornography as defined in the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, and any: a) visual material, including photographic, video and live-streaming media, that depicts: i) a child engaged in or in the presence of sexual activity,

		ii) a person appearing to be a child engaged in or in the presence of sexual activity, iii) realistic images representing a child engaged in or in the presence of sexual activity; b) written material that: i) advocates sexual activity with a child, ii) is written for a sexual purpose and has as a dominant characteristic the description of sexual activity with a child; and c) audio recordings that: i) advocates sexual activity with a child, ii) is recorded for a sexual purpose and has as a dominant characteristic the description of sexual activity with a child.
Grooming and luring of a child	This provision would criminalize the preparatory steps, specifically the communications between persons where their purpose is to facilitate the commission of a sexual offence against a child, in order to prevent actual harm coming to the child. The availability of the Internet and pervasiveness of online services used by children has provided criminals with greater accessibility to potential victims. In Canada, there are a few thousand incidents of this type of behaviour investigated by police per year. Examples of situations that would be captured by this provision include contacting and befriending a child in a video game or social media platform, for the purpose of facilitating the commission of a child sexual exploitation offence.	1. Establish as criminal offences, when committed intentionally and without right, the following conduct: a) transmitting, distributing, selling, or making available through a computer system sexually explicit material to a child or a person believed to be a child; b) communicating with a child, or a person believed to be a child, through a computer system; or c) agreeing or making arrangements with a child, or a person believed to be a child, through a computer system; for the purpose of facilitating the commission of any child sexual exploitation offences established under this Convention, the Optional Protocol to the UN Convention on the Rights of

		the Child on the sale of children, child prostitution and child pornography or the domestic law of the State Party. 2. No criminal liability is established if a person has taken reasonable steps to ascertain the person is not a child.
Non consensual dissemination of intimate images ("Revenge porn")	The provision would protect a person's privacy and address the negative consequences of the non-consensual dissemination of such intimate images to a person's reputation, character, personal safety, etc. Women and girls are predominantly victims of this type of criminal activity. The use of the Internet for the rapid non-consensual dissemination of intimate images and the near impossibility of having these images fully removed significantly amplifies the devastating impact of this crime on victims. This criminal activity creates lasting negative effects on victims. The non-consensual dissemination of intimate images is a form of gender-based violence that can have a particularly chilling effect on women in society. This provision would apply to situations involving cyber bullying, ransomware, criminal harassment, and extortion/blackmail.	1. Establish as criminal offences, when committed intentionally and without right, publishing, distributing, transmitting, selling, making available, or advertising an intimate image of a person by any means of a computer system, knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct. 2. For the purpose of paragraph 1, intimate image means a visual recording of a person made by any means including a photographic, film, or video recording: a) in which the person is nude, is exposing their genital organs, anal region or breasts, or is engaged in explicit sexual activity; b) in respect of which, at the time of the recording, there were circumstances that gave rise to a reasonable expectation of privacy; and c) in respect of which the person depicted retains a reasonable expectation of privacy at the time the offence is committed. 3. No criminal liability is established if the non-consensual sharing is for the public good or has a legitimate purpose.

Procedural powers

	Rationale	Proposed text
Scope of procedural powers	This provision would create an obligation for States Parties to establish procedural measures for the purpose of criminal investigations of the offences established in the convention and the collection of evidence in electronic form of a criminal offence.	1. Clarify that powers and procedures provided for in this section are for the purpose of specific criminal investigations or proceedings. 2. Except as specifically provided otherwise, a State Party shall apply the powers and procedures referred to in paragraph 1 to: a) the criminal offences established in accordance with this convention; b) other criminal offences committed by means of a computer system; and c) the collection of evidence in electronic form of a criminal offence.
Expedited preservation of stored computer data	Police investigations are often undermined by the loss of this electronic evidence, which can be destroyed because it is transient and not needed for business purposes. Expedited preservation ensures the availability of important electronic evidence pending the lawful seizure of such data.	1. Each State Party shall adopt the necessary legislative and other measures to enable its domestic competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2. If a State Party gives effect to paragraph 1 by means of an order to a person to preserve specified stored computer data in that person's possession or control, the State Party shall adopt the necessary legislative and other measures to oblige that person to preserve and maintain the integrity of that data for a period of time as long as necessary, up to a

		maximum of ninety days, to enable the competent authorities to seek its disclosure. A State Party may provide for such an order to be subsequently renewed. 3. Each State Party shall adopt the necessary legislative and other measures to oblige, where justified and authorized, the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
Expedited preservation and partial disclosure of traffic data	Expedited preservation and disclosure of traffic data is important for identifying suspects. For example, in the context of a botnet, multiple service providers and multiple computers are implicated. This procedural tool would allow for the rapid identification of service providers used in the criminal transaction.	In respect of traffic data that is to be preserved under the previous article: a) ensure that the expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b) Ensure the expeditious disclosure to the State Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the State Party to identify the service providers and the path through which the communication was transmitted.
Production order	Production orders are particularly useful because they compel custodians of data to produce specific data for the purpose of a criminal investigation. They further enhance privacy protections because the custodians of the data have the ability to extract and produce only what has been ordered by the court or lawfully authorized authority.	Each State Party shall adopt the necessary measures to empower its domestic competent authorities to order a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium.

	Consideration could be given to enacting specific production orders tailored to the level of privacy interest in the data/information sought for production. For example, a general production order could be included in the convention, with a higher level of judicial scrutiny for all data associated with an investigation, and specific production orders could also be included with a lower level of judicial scrutiny for narrower classes of data with a lower level of privacy interest.	
Search and seizure of stored computer data	This provision would ensure that State Parties' domestic search and seizure provisions are updated to apply to computer data in addition to the usual tangible items.	1. Each State Party shall adopt the necessary measures to empower its domestic competent authorities to search or similarly access: a) a computer system or part of it and computer data stored therein; and b) a computer-data storage medium in which computer data may be stored in its territory. 2. Each State Party shall adopt the necessary measures to enable its domestic competent authorities to expeditiously extend the search or similar accessing to the other system where they have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the system. 3. Each State Party shall adopt the necessary measures to empower its domestic competent authorities to seize or similarly secure computer data accessed according to paragraphs

		1 or 2. These measures include the power to: a) seize or similarly secure a computer system or part of it or a computer-data storage medium; b) make and retain a copy of those computer data; c) maintain the integrity of the relevant stored computer data; and d) render inaccessible or remove those computer data in the accessed computer system. 4. Each State Party shall adopt the necessary measures to empower its domestic competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data to provide, as is reasonable, the necessary information to enable the undertaking of the measures referred to in paragraphs 1 and 2.
Jurisdiction	This provision would ensure that State Parties establish jurisdiction and take steps to ensure offences are addressed under domestic law. It also recognises sovereignty and the importance of consultations and coordination, given the transnational nature of the crimes.	1. Each State Party shall adopt the necessary measures to establish its jurisdiction over the offences established in this convention when: a) the offence is committed in the territory of that State Party; b) the offence is committed on board a vessel that is flying the flag of that State Party or an aircraft that is registered under the domestic law of that State Party at the time

		that the offence is committed; or c) the offence is committed by a national of that State Party or a stateless person who has his or her habitual residence in its territory. 2. Enable a State Party to establish its jurisdiction over the offences established in accordance with this convention when the alleged offender is present in its territory and it does not extradite such person solely on the ground that he or she is one of its nationals. 3. Enable a State Party to establish its jurisdiction over the offences established in accordance with this convention when the alleged offender is present in its territory and it does not extradite him or her. 4. If a State Party exercising its jurisdiction under paragraph 1 or 2 has been notified, or has otherwise learned, that any other State Party is conducting an investigation, prosecution, or judicial proceeding in respect of the same conduct, the competent authorities of those State Parties shall, as appropriate, consult one another with a view to coordinating their actions. 5. Without prejudice to norms of general international law, this convention does not exclude the exercise of any criminal jurisdiction established by a State Party in accordance with its domestic law.