

Canadian submission

On international cooperation, technical assistance, preventive measures, mechanisms of implementation and final provisions

For consideration at AHC 3

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.

In line with the UN General Assembly Resolution 74/247 and the AHC mandate to elaborate “a comprehensive international convention on countering the use of information and communications technologies for criminal purposes” “taking into full consideration existing international instruments”, Canada is of the view that the UN Conventions against transnational organized crime (UNTOC), against corruption (UNCAC) as well as the Council of Europe Convention on Cybercrime (Budapest Convention) provide good basis for the development of provisions for this convention on international cooperation, technical assistance, preventive measures, mechanisms of implementation and final provisions.

As per UN General Assembly resolution 75/282 and in accordance with its past submissions to the AHC, Canada reiterates the importance for the negotiations of the new convention to continue to be a transparent and inclusive process, ensuring civil society and other relevant stakeholders have a meaningful opportunity to participate and contribute to both the negotiation of the convention and its implementation.

International cooperation

International cooperation is vital in effectively combating the growing and changing global threat posed by cybercrime (cyber-dependent and cyber-enabled crimes). In considering the most effective approach to the international cooperation elements of a draft UN Cybercrime Convention, Canada draws on existing, well-established treaties such as UNTOC and the Budapest Convention. These are important instruments containing robust measures of international assistance that have already proven to be effective in fighting serious crime at a global level.

Canada supports the facilitation of both formal and informal international cooperation, including to obtain electronic evidence, for the detection, prevention investigation and prosecution of the cybercrime offences covered by the Convention, with appropriate

conditions and safeguards. Canada is still reflecting on the scope of the criminal offences for which electronic evidence may be preserved, collected and shared - whether the scope should be broad as in the Budapest Convention, or more limited to apply only to “serious crimes” as defined in UNTOC.

In identifying meaningful proposals for the international cooperation section of a UN Cybercrime Convention and considering the cybercrime context itself, Canada relies on common and well-understood principles and standards in the areas of extradition, mutual legal assistance, transfers of sentenced persons and other proven measures of assistance. Importantly, Canada is proposing an international cooperation framework that would protect freedom of expression, opinion and association, as well as the right not to be subjected to unlawful or arbitrary interference with privacy and the rights related to due process.

In the extradition context, Canada proposes broadening the grounds of refusal by expanding the list of discrimination set out in UNTOC to reflect modern realities. Canada also proposes that the extradition provisions apply only to offences covered by the criminalization provisions of this Convention. Canada advances the same position vis-à-vis the provisions related to the transfer of sentenced persons, international cooperation for purposes of confiscation, disposal of confiscated proceeds of crime or property, and the transfer of criminal proceedings.

In the mutual legal assistance context, Canada supports cooperation to the broadest extent possible, but in order to ensure the most effective and efficient use of strained resources on international cooperation, is proposing the inclusion of a de minimis clause in addition to the grounds for refusal set out in UNTOC.

Canada’s proposals attempt to balance the operational need for timely international cooperation with the need for strong protections and safeguards to protect human rights and privacy interests. Canada looks forward to working with all other Parties to establish international cooperation provisions that add value to our joint efforts to fight cybercrime, cyber-dependent and cyber-enabled crimes, both domestically and internationally.

Cybercrime prevention

Effective cybercrime prevention measures are well informed and designed to reach the public, in particular groups that are most vulnerable to cybercrime as well as other actors (governmental and non-governmental including private sector) who can both benefit from information and educational material on cybercrime and contribute to the creation and dissemination of such information and education material.

UNTOC and UNCAC both contain provisions relating to crime prevention that can inspire the AHC in developing provisions designed for the prevention of cybercrime. In particular, Article 28 UNTOC provides a good basis for developing a provision to facilitate the collection, exchange and analysis of information on the nature of cybercrime. Similarly, Article 13 UNCAC provides a good model to encourage the active participation of civil society and others to promote public awareness of cybercrime and to prevent cybercrime at the national and international levels. Canada is also proposing that the convention's crime prevention provisions encourage State Parties to incorporate mainstreaming a gender-based approach to the development of crime prevention and education programmes to ensure that the most vulnerable groups to cybercrime such as women, children and the elderly, are properly considered and addressed. See proposed text in Annex for a public awareness provision with a gender mainstreaming approach.

Article 39 UNCAC also provides a good starting point for the development of a provision that sets out a clear role for the private sector, in particular communication service providers, in the early detection of cybercrime trends and potential criminal activity as well as facilitating public reporting of cybercrime related incidents to law enforcement.

Technical assistance and capacity building

Technical assistance and capacity building provisions invite Member States to strengthen the capacity of law enforcement and other relevant authorities to prevent, detect and combat cybercrime through technical assistance, training and capacity building provisions modelled after UNTOC and UNCAC, with adaptations to reflect the specificities of cybercrime and with a particular emphasis on the sharing of information and experience. Canada is proposing to ensure these provisions set out a clear role for the civil society and other relevant non-governmental stakeholders in cybercrime prevention efforts, as well as in technical assistance and capacity building related measures. Canada also believes that mainstreaming a gender-based approach to the delivery of technical assistance and capacity building, as well as specific training on employing a gender-based approach to policy making, legislation, programming and law enforcement are important and should be incorporated into these provisions. See proposed text in the Annex.

Implementation measures

The convention's implementation measures could be modelled after UNTOC.

In addition, Canada proposes that implementation provisions of this convention invite State Parties to apply a gender mainstreaming approach to identify the differential impacts of cybercrime on diverse communities, in particular women and children and the elderly, and to consult with civil society, industry and other relevant non-governmental organizations when developing legislation

and other measures to implement this convention to ensure broad-based support and to ensure that the measures contemplated are responsive and relevant to their specific national needs.

Canada considers that the timely sharing of relevant information can contribute to strengthening the implementation of the convention, and thus proposes that the convention build on UNCAC article 63 paragraph 6 to facilitate sharing of relevant information between the Parties and with the public. Canada also proposes to include in the text of the convention provisions that commit the States Parties to early, ongoing, and effective review of implementation of the Convention. Finally, Canada considers that the UN Office on Drugs and Crime should serve as the Secretariat for the convention.

Final provisions

The convention’s final provisions could be modelled after UNTOC’s final provisions with minor adaptations.

Annex - Proposed text

NB: The textual references below to UNTOC and the Budapest Convention include only those articles or paragraphs to which Canada is proposing modifications (with some text removed in strikethrough and other text added in bold). Otherwise Canada supports the inclusion of the existing text of those provisions referenced in the “Sources and Rationale” column as a basis for negotiation.

Proposed text:	Sources and Rationale:
<i>International Cooperation</i>	
General principles relating to international cooperation	
<p>The State Parties shall cooperate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.</p>	<p>Article 23 Budapest Convention</p> <p>This general provision applies to the entire international cooperation chapter.</p> <p>The purpose of this Convention is to promote international cooperation in the collection of electronic evidence and the prevention, investigation and prosecution of cybercrime.</p> <p>As this overarching general provision speaks to the principle of international cooperation, specific mention of other international</p>

Proposed text:	Sources and Rationale:
	<p>treaties, or arrangements based on uniform or reciprocal legislation, is not required here. These more specific references appear in provisions related to extradition mutual legal assistance set out below.</p>
Extradition	
<p>1. This article shall apply to the offences covered by this Convention as set out in the [articles on criminalization] or in cases where an offence referred to in article 3, paragraph 1 (a) or (b), involves an organized criminal group and the person who is the subject of the request for extradition is located in the territory of the requested State Party, provided that the offence for which extradition is sought is punishable under the domestic law of both the requesting State Party and the requested State Party.</p> <p>(...)</p> <p>8. States Parties shall, subject to their domestic law and in appropriate circumstances, endeavour to expedite extradition procedures and to simplify evidentiary requirements relating thereto in respect of any offence to which this article applies.</p> <p>(...)</p> <p>14. Nothing in this Convention shall be interpreted as imposing an obligation to extradite if the requested State Party has substantial grounds for believing that the request has been made for the purpose of prosecuting or punishing a person on account of that person’s sex, race, religion, nationality, language, colour, sexual orientation, mental or physical disability, ethnic origin or political opinions or that compliance with the request would cause prejudice to that person’s position for any one of these reasons.</p>	<p>Article 16 UNTOC with small adjustments to reflect cybercrime. The UNTOC provides a solid basis for the article on extradition for this Convention. Extradition through this Convention should only be available in relation to the clearly established listing of offences for which criminalization is required.</p> <p>Paragraph 16(1): there is no need to refer to “organized criminal groups” as this is particular to UNTOC.</p> <p>Paragraph 8: In contrast to organized crime offences, cybercrime offences may vary in severity from relatively minor to very serious offences. As a result, this paragraph, taken from the UNTOC, should be qualified since not all extradition requests in the context of cybercrime necessarily merit expedited treatment.</p> <p>Paragraph 14: Additional grounds have been added to reflect a deeper understanding of what characteristics could make certain persons or groups of persons more vulnerable in the passage of time following the entry into force of UNTOC.</p>

Proposed text:	Sources and Rationale:
Transfer of sentenced persons	
	<p>Article 17 UNTOC This provision would permit States Parties to enter into multilateral or bilateral arrangements for the transfer of persons sentenced to offences covered by this Convention, consistent with similar UN treaties.</p>
Mutual legal assistance	
<p>1. States Parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions and judicial proceedings in relation to the offences covered by this Convention as provided for in article 3 [articles on criminalization] and shall may also reciprocally extend to one another similar assistance where the requesting State Party has reasonable grounds to suspect that the offence referred to in article 3, paragraph 1 (a) or (b), is transnational in nature, including that victims, witnesses, proceeds, instrumentalities or evidence of such offences are located in the requested State Party and that the offence involves an organized criminal group seeks the collection of evidence in electronic form of a criminal offence.</p> <p>(...)</p> <p>5. The transmission of information pursuant to paragraph 4 of this article shall be without prejudice to inquiries and criminal proceedings in the State of the competent authorities providing the information. The competent authorities receiving the information shall comply with a request that said information remain confidential, even temporarily, or with restrictions on its use. However, this shall not prevent the receiving State Party from disclosing in its proceedings information that is exculpatory to an accused person. In such a case, the receiving State Party shall notify the transmitting State Party prior to the disclosure and, if so requested, consult with the transmitting State Party. If, in an exceptional case, advance notice is not possible,</p>	<p>Article 18 UNTOC The UNTOC provides a solid basis for the overarching article on mutual legal assistance for this Convention.</p> <p>Paragraph 1: The provisions on mutual legal assistance should apply to the offences covered in the Convention. Canada is reflecting on the added-value and desirability of extending the measures for mutual legal assistance to “the collection of evidence in electronic form of a criminal offence” (taken from paragraph 25(1) Budapest Convention) or limiting the scope of electronic evidence in relation to “serious crimes” as per UNTOC.</p> <p>Paragraph 5: As the requirement regarding exculpatory evidence is a requirement impacting domestic evidentiary law, we propose that this portion of paragraph 5 is neither required nor advisable.</p>

Proposed text:	Sources and Rationale:
<p>the receiving State Party shall inform the transmitting State Party of the disclosure without delay.</p> <p>(...)</p> <p>14. Requests shall be made in writing or, where possible, by any means capable of producing a written record, in a language acceptable to the requested State Party, under conditions allowing that State Party to establish authenticity. The Secretary-General of the United Nations shall be notified of the language or languages acceptable to each State Party at the time it deposits its instrument of ratification, acceptance or approval of or accession to this Convention. In urgent circumstances and where agreed by the States Parties, requests may be made orally, but shall be confirmed in writing forthwith.</p> <p>14bis. Each State Party may, in urgent circumstances, make requests for mutual legal assistance or communications related thereto by expedited means of communication, including fax or email, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested State Party. The requested State Party shall accept and respond to the request by any such expedited means of communication.</p> <p>(...)</p> <p>19. The requesting State Party shall not transmit or use information or evidence furnished by the requested State Party for investigations, prosecutions or judicial proceedings other than those stated in the request without the prior consent of the requested State Party. Nothing in this paragraph shall prevent the requesting State Party from disclosing in its proceedings information or evidence that is</p>	<p>Paragraph 14: We suggest replacing the last sentence in paragraph 14 with the more detailed and modern text on urgent requests set out in paragraph 25(3) of the Budapest Convention with minor additions in bold.</p> <p>Paragraph 19: For the reasons provided in relation to paragraph 5 above, we propose the deletion of the last three sentences of this paragraph.</p>

Proposed text:	Sources and Rationale:
<p>exculpatory to an accused person. In the latter case, the requesting State Party shall notify the requested State Party prior to the disclosure and, if so requested, consult with the requested State Party. If, in an exceptional case, advance notice is not possible, the requesting State Party shall inform the requested State Party of the disclosure without delay.</p> <p>(...)</p> <p>21. Mutual legal assistance may be refused:</p> <p>(a) If the request is not made in conformity with the provisions of this article;</p> <p>(b) If the requested State Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests;</p> <p>(c) If the authorities of the requested State Party would be prohibited by its domestic law from carrying out the action requested with regard to any similar offence, had it been subject to investigation, prosecution or judicial proceedings under their own jurisdiction;</p> <p>(d) If it would be contrary to the legal system of the requested State Party relating to mutual legal assistance for the request to be granted;</p> <p>(e) If the use of resources required to execute the request are not justified in light of the minor nature of the alleged criminal conduct.</p>	<p>Paragraph 21: Given the potential range in the degree of severity of cybercrime offences and the already overstrained MLA resources in some Parties, we propose the inclusion of a <i>de minimis</i> clause. Similar <i>de minimis</i> grounds of refusal are found in other instruments, such as paragraph 8(1)(g) of the Revised Scheme Relating to Mutual Legal Assistance in Criminal Matters within the Commonwealth, which reads: “by reason of the trivial nature of the alleged offending or the low value of the likely penalty or any property likely to be forfeited or confiscated, the requested country would not have made a similar request to another country in connection with a like criminal matter arising in the requested country.”</p>

Proposed text:	Sources and Rationale:
Expedited preservation of stored computer data	
	<p>Article 29 Budapest Convention</p> <p>This article would provide for international cooperation in obtaining expeditious preservation of stored computer data. Computer data is highly volatile and easily subject to being deleted, altered or moved, rendering it impossible to trace a crime to its perpetrator or destroying critical evidence. Some forms of computer data are stored for only short periods of time before being deleted. Thus, a mechanism is required in order to ensure temporary preservation of such data pending the lengthier and more involved process of executing a formal mutual legal assistance request.</p>
Expedited disclosure of preserved traffic data	
	<p>Article 30 Budapest Convention</p> <p>This article would provide for the expedited and limited disclosure of a service provider related to a third party state not contemplated by the initial mutual legal assistance request. Obtaining this information early on would permit the Requesting Party to make another mutual legal assistance request to the appropriate State.</p>
Mutual legal assistance - stored computer data	
	<p>Article 31 Budapest Convention</p> <p>This article would provide for international cooperation between Each Party (requesting/requested) to have the ability to, for the benefit of another Party, search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within its territory.</p>
Mutual legal assistance regarding the real-time collection of traffic data	
<p>1. The State Parties shall shall may provide mutual legal assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, This assistance shall be governed by the conditions and procedures provided for under domestic law.</p>	<p>Art 33 Budapest Convention</p> <p>Paragraph 1: The assistance covered by this article is a form of mutual “legal” assistance.</p> <p>The provision of expedited preservation of stored computer data (article 29 BC) and mutual legal assistance in respect of stored computer data (article 31 BC) are both framed as discretionary</p>

Proposed text:	Sources and Rationale:
2. Each State Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	provisions, the mutual legal assistance regarding the real-time collection of traffic data, which is more invasive, should also be framed in a discretionary manner even when such collection is available domestically. Hence, the proposed deletion of “subject to the provisions of paragraph 2”.
Mutual legal assistance regarding the interception of content data	
The State Parties shall provide mutual legal assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws	Article 34 Budapest Convention As the provision of co-operation for interception of content is an emerging area of mutual assistance practice, the provision would defer to existing mutual assistance regimes and domestic laws regarding the scope and limitation on the obligation to assist.
Confiscation and seizure (to be included in the procedural measures chapter)	
	Article 12 UNTOC In relation to confiscation and seizure, article 12 of UNTOC contains distinct provisions for domestic law that are required for international cooperation for freezing, seizure and confiscation (articles 13 and 14 UNTOC). Article 12 could be incorporated into the procedural measures chapter of the Convention. Together these provisions achieve a balance between specificity as to elements that States must have in place, while allowing for the differences between the various legal systems.
International cooperation for purposes of confiscation	
	Article 13 UNTOC Suggest mirroring the provision of Article 13 of UNTOC. Together with articles 12 and 14 UNTOC these provisions achieve a balance between specificity as to elements that States must have in place, while allowing for the differences between the various legal systems.
Disposal of confiscated proceeds of crime or property	
(...) <p>3. When acting on the request made by another State Party in accordance with articles 12 and 13 [the article on confiscation and</p>	Article 14 UNTOC Article 14 of UNTOC contains provisions for international cooperation for the purposes of the disposal of confiscated proceeds of crime that could be incorporated into this Convention. Together with

Proposed text:	Sources and Rationale:
<p>seizure and the article on international cooperation for the purposes of confiscation] of this Convention, a State Party may give special consideration to concluding agreements or arrangements on:</p> <p>(a) Contributing the value of such proceeds of crime or property or funds derived from the sale of such proceeds of crime or property or a part thereof to the account designated in accordance with article 30, paragraph 2 (c), of this Convention and to intergovernmental bodies specializing in the fight against organized crime;</p> <p>(b) Sharing with other States Parties, on a regular or case-by-case basis, such proceeds of crime or property, or funds derived from the sale of such proceeds of crime or property, in accordance with its domestic law or administrative procedures.</p>	<p>articles 12 and 13 UNTOC, these provisions achieve a balance between specificity as to elements that States must have in place, while allowing for the differences between the various legal systems.</p> <p>Paragraph 3 (a): We propose its exclusion given that not all States are able to contribute the value of proceeds of crime to a special fund.</p>
24/7 Network	
	<p>Article 35 Budapest Convention Mirrors the provision of the Budapest Convention by providing the necessary tools for law enforcement and prosecutors to combat cybercrime, including the rapid response to collect information and data in electronic form.</p>
Joint investigations	
	<p>Article 19 UNTOC Article 19 UNTOC provides for joint investigations in a manner that is respectful of the sovereignty of States and the distinct requirements of States in entering into joint investigation arrangements.</p>
Transfer of criminal proceedings	
	<p>Article 21 UNTOC Article 21 UNTOC provides for the possibility of the transfer of criminal proceedings without imposing such transfers. This flexibility accounts for the diversity in criminal justice systems.</p>
Law enforcement cooperation	

Proposed text:	Sources and Rationale:
<p>1. States Parties shall cooperate closely with one another, consistent with their respective domestic legal and administrative systems, to enhance the effectiveness of law enforcement action to combat the offences covered by this Convention. Each State Party shall, in particular, adopt effective measures:</p> <p>(a) To enhance and, where necessary, to establish channels of communication between their competent authorities, agencies and services in order to facilitate the secure and rapid exchange of information concerning all aspects of the offences covered by this Convention, including, if the States Parties concerned deem it appropriate, links with other criminal activities;</p> <p>(b) To cooperate with other States Parties in conducting inquiries with respect to offences covered by this Convention concerning:</p> <p>(i) The identity, whereabouts and activities of persons suspected of involvement in such offences or the location of other persons concerned;</p> <p>(ii) The movement of proceeds of crime or property derived from the commission of such offences;</p> <p>(iii) The movement of property, equipment or other instrumentalities used or intended for use in the commission of such offences;</p> <p>(c) To provide, when appropriate, necessary items or quantities of substances data for analytical or investigative purposes;</p>	<p>Article 27 UNTOC Article 27 UNTOC provides a useful framework for law enforcement cooperation that needs only be adapted to the cybercrime context.</p> <p>Paragraph 1 (c): A reference to data for analytical or investigative purposes is included.</p>

Proposed text:	Sources and Rationale:
<p>(d) To facilitate effective coordination between their competent authorities, agencies and services and to promote the exchange of personnel and other experts, including, subject to bilateral agreements or arrangements between the States Parties concerned, the posting of liaison officers;</p> <p>(e) To exchange information with other States Parties on specific means and methods used by organized criminal groups cybercrime perpetrators and their accomplices, including, where applicable, routes and conveyances and the use of false identities, altered or false documents or other means of concealing their activities, the use of illicit encrypted platforms, cybercrime tactics, techniques and procedures, as well as operational indicators of compromise and concern;</p> <p>(f) To exchange information and coordinate administrative and other measures taken as appropriate for the purpose of early identification of the offences covered by this Convention.</p> <p>3. States Parties shall endeavour to cooperate within their means to respond to transnational organized crime committed through the use of modern technology.</p>	<p>Paragraph 1 (e): The reference to organized crime groups is replaced by “cybercrime perpetrators and their accomplices” to capture a broad range of perpetrators.</p> <p>Paragraph 3: Is redundant.</p>

Technical assistance and Capacity Building

Law Enforcement and other personnel training

Proposed text:

1. Each State Party shall, to the extent necessary, initiate, develop or improve specific training programmes for its law enforcement personnel, including **central authorities**, prosecutors, investigating magistrates and customs personnel, and other personnel charged with the prevention, detection and control of the offences covered by this Convention. Such programmes may include secondments and exchanges of staff. Such programmes shall deal, in particular and to the extent permitted by domestic law, with the following:

(a) Methods used in the prevention, detection and control of the offences covered by this Convention;

(b) ~~Routes and techniques~~ **Modus operandi** used by persons suspected of involvement in offences covered by this Convention, ~~including in transit States~~, and appropriate countermeasures;

(c) Monitoring of the movement of contraband;

(d) Detection and monitoring of **cybercrime, including child sexual abuse and exploitation material, the use of illicit encrypted platforms, ransomware, network intrusions, and other malware-based threats** ~~the movements of proceeds of crime, property, equipment or other instrumentalities and methods used for the transfer, concealment or disguise of such proceeds, property, equipment or other instrumentalities, as well as methods~~

Sources and Rationale:

Art 29 UNTOC

Article 29 UNTOC provides a solid basis for a law enforcement training provisions with appropriate adaptations to reflect the cybercrime context. This provision is designed to enhance the skills of practitioners and central authorities and to support the sharing of information and experiences to facilitate investigations, prosecution and international cooperation in fighting cybercrime.

Paragraph 1: A reference to training for central authorities is included given the critical role they play in international cooperation.

Paragraph 1 (d): Specific references to certain types of cybercrime, including technology-as-target cybercrime or cyber-dependent crime types is included for illustrative purposes.

<p>used in combating money laundering and other financial crimes;</p> <p>(e) Collection of electronic evidence;</p> <p>(f) Control techniques in free trade zones and free ports;</p> <p>(g) Modern law enforcement equipment and techniques, including electronic surveillance, controlled deliveries and undercover operations;</p> <p>(h) Methods used in combating transnational organized crime committed through the use of computers, telecommunications networks or other forms of modern technology cybercrime; and</p> <p>(i) Methods used in the protection of victims and witnesses; and</p> <p>(j) Methods for incorporating gender mainstreaming into policy making, legislation and programming.</p>	<p>New Paragraph 1(j): is designed to incorporate the gender mainstreaming lens.</p>
--	---

Preventive measures	
Public awareness	
Proposed text:	Sources and Rationale:
<p>1. Each State Party shall endeavour to develop, facilitate and promote national and international public awareness programmes, public information campaigns and policies aimed at the prevention of cybercrime. Such information may be disseminated, where appropriate, through the mass media and</p>	<p>Inspired by UNTOC paragraphs 31(1), (5) and (7). This provision would encourage and facilitate public information, awareness and education on cybercrime.</p>

shall include measures to promote public participation in preventing and combatting cybercrime.

- 2. State Parties should apply a gender mainstreaming approach to assist in identifying differential impacts of cybercrime on diverse communities in particular women and children and the elderly in the development and implementation of these programmes, information campaigns and policies. This includes developing and providing programs and campaigns specifically designed for segments of the population most vulnerable to cybercrime and for social workers, educators and other professionals interacting with them.**
- 3. State Parties shall endeavor to assist one another in developing and implementing the programs, campaigns and policies referred to in paragraph 1 including by sharing educational materials and programs.**