Elaboration of a convention on countering the use of information and communications technologies for criminal purposes - A United Nations Convention on Cybercrime:

Canadian perspective on the scope, objectives, and structure of the convention

Canada's submission is in response to the Ad-Hoc Committee (AHC) Secretariat's August 11th invitation requesting Member States (MS) to submit *"views on the scope, objectives and structure (elements) of the new convention".*

In preparing these comments, 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 Drugs and Crime Office through its Global Programme on Cybercrime and the United Nations Congresses on Crime Prevention and Criminal Justice. These initiatives have set the stage for the elaboration of a UN convention that should exclusively focus on the fight against cybercrime and not deal with cyber security, cyber governance and other related matters better addressed in other UN fora.

As per UN General Assembly resolution 75/282 and in accordance with its past submissions to the AHC, Canada would like to reiterate that the negotiations of the new convention must be a transparent and inclusive process, allowing civil society and other relevant stakeholders a meaningful opportunity to participate.

Scope:

The new convention should provide a framework to counter cybercrime and serious criminal offences that are frequently committed through the use of computer systems that includes the following elements:

- Provisions for substantive cybercrime offences and the investigation and prosecution of cybercrime and serious criminal offences that are frequently committed through the use of computer systems;
- Provisions for international cooperation in relation to the above, as well for obtaining electronic evidence of other criminal offences;
- Provisions that include measures that seek to prevent cybercrime; and,
- Provisions that include measures that encourage Member States and other stakeholders to provide sustained technical assistance and capacity building initiatives.

The elements of the new convention must be consistent with international human rights obligations, in particular the freedoms of expression, opinion and association, as well as the right not to be subjected to unlawful or arbitrary interference with one's privacy.

Objectives:

The new convention should have the following objectives:

- On the basis of a common understanding, establish a baseline for substantive criminal offences, procedural powers and international cooperation to fight cybercrime;
- Ensure provisions are drafted in a "technology-neutral" way to ensure that the provisions do not become obsolete or unenforceable as technologies evolve;
- Promote and facilitate international cooperation in the common fight against cybercrime;
- Establish authorities to collect, obtain and share electronic evidence of other offences;
- Eliminate safe havens for cybercrime perpetrators;
- Ensure compliance with international human rights obligations, in particular for the freedoms of expression, opinion and association, as well as the right not to be subjected to unlawful or arbitrary interference with privacy;
- Ensure consistency with existing UN treaties in the field of crime prevention and criminal justice, in particular the United Nations Convention against Transnational Organized Crime, the United Nations Convention against Corruption and take into account multilateral instruments that have already proven their usefulness in the fight against cybercrime, in particular the Council of Europe Convention on Cybercrime; and,
- Support Member States to strengthen their capacity to address cybercrime through technical assistance and capacity building.

Structure:

In regards to the structure of the new convention, and in addition to clear definitions and final provisions, Canada considers important that the following five elements form part of the structure of the convention.

1. **Substantive offence provisions** requiring Member States to adopt legislative and other measures as may be necessary:
    - To establish as criminal offences actions affecting the confidentiality, integrity and availability of computer systems, networks and computer data, misuse of computer systems, networks and computer data; and,

- To ensure that specified traditional crimes frequently committed through the use of computer systems are adequately covered by their criminal law – for example, dissemination of child pornography.

2. **Procedural provisions** requiring Member States to adopt legislative and other measures, as may be necessary, to establish authorities to preserve and obtain electronic evidence of criminal offence that is stored on computer systems in foreign, multiple, or unknown jurisdictions. While more general investigative powers, such as search and seizure and production orders, should be included in the new convention, more specialized investigative tools should also be included to address the speed at which offences can be committed and the transience and volatility of electronic evidence. These provisions should be subject to safeguards to ensure that law enforcement activities comply with international human rights obligations.

3. **International cooperation** is important in combating cybercrime. The new convention needs to include mechanisms to facilitate both formal and informal international cooperation for the detection, investigation and prosecution of cybercrime as well for obtaining electronic evidence of other criminal offences.

4. The new convention needs to include **preventive measures** similar to those found under the United Nations Convention against Transnational Organized Crime and the United Nations Convention against Corruption, for instance provisions on awareness-raising and educational initiatives. Multi-stakeholder partnerships and civil society can play a vital role and this should be reflected in these provisions.

5. The new convention should encourage Member States to strengthen capacity to address cybercrime through **technical assistance and capacity building**. This could include provisions to:

   - Support multi stakeholder involvement;
   - Encourage collaboration with the United Nations Office on Drugs and Crime and its Global Programme on Cybercrime to enhance the skills of practitioners and central authorities on their use of technology to facilitate international cooperation in fighting cybercrime; and,
   - Develop training programmes for investigators and prosecutors and support sharing information and experiences with relevant stakeholders.