MEETINGS OF MINISTERS OF JUSTICE OR
OTHER MINISTERS OR ATTORNEYS GENERAL
OF THE AMERICAS

OEA/Ser.K/XXXIV
CIBER-VII/doc.1/11
14 November 2011
Original: English

Seventh Meeting of the Working Group on Cyber-crime

PREPARATORY QUESTIONNAIRE
FOR THE SEVENTH MEETING OF THE WORKING GROUP ON CYBER-CRIME

INTRODUCTION

The object of this questionnaire is to collect useful information for the purposes of the Seventh Meeting of the Working Group on Cyber-Crime, which will take place at OAS Headquarters on February 6 and 7, 2012, with regard to the recommendations that have been put forward at previous meetings and that been adopted in the framework of the process of Meetings of Ministers of Justice or other Ministers or Attorneys General of the Americas (REMJA), which are in accordance therewith.

To that end, the questionnaire is divided into four thematic areas: (1) Legislation; (2) Specialized Units and National Efforts; (3) International Cooperation; and (4) Training.

Bearing the foregoing in mind, kindly submit the response of your State to this questionnaire by e-mail (LegalCooperation@oas.org) or fax (+ (202) 458-3598) to the OAS General Secretariat (Department of Legal Cooperation, Secretariat for Legal Affairs) by **Friday, December 16, 2011.**

Please use any extra space that might be required for each response, or attach additional pages, as necessary.

I. LEGISLATION

1.1. Has your country criminalized the following types of cyber-crime?

a)	Illegal access	Yes (X)	No ( )
b)	Illegal interception	Yes (X)	No ( )
c)	Data interference	Yes (X)	No ( )
d)	System interference	Yes (X)	No ( )
e)	Misuse of devices	Yes (X)	No ( )
f)	Computer-related forgery	Yes (X)	No ( )
g)	Computer-related fraud	Yes (X)	No ( )
h)	Child pornography	Yes (X)	No ( )
i)	Offences related to infringements of copyright and related rights	Yes (X)	No ( )
j)	Other offences (please list): _____	Yes (X)	No ( )

If you answered yes to any of the foregoing, please list and enclose a copy, preferably electronic, of those laws: _____

Illegal access: Section 342.1 of the *Criminal Code* makes it a hybrid offence for a person fraudulently and without of colour of right to obtain, directly or indirectly, any computer

service, or to intercept or cause to be intercepted, directly or indirectly, any function of a computer service by means of any device. The maximum term of imprisonment upon conviction for this indictable offence is ten years. Section 342.1 will also cover illegal access to computer services that could also be characterized as illegal interception.

Illegal interception: Section 184(1) of the *Criminal Code* makes it an indictable offence to willfully intercept a private communication by means of any electro-magnetic, acoustic, mechanical or other device. The maximum term of imprisonment upon conviction for this indictable offence is five years.

Data interference: Section 430(1.1) of the *Criminal Code* creates the offence of mischief to data, and provides that the offence can be committed by destroying or altering data, rendering data meaningless, or obstructing the use of, or denying access to data. The maximum term of imprisonment upon conviction for this indictable offence is ten years.

Misuse of devices: Section 191 of the *Criminal Code* makes it an indictable offence to possess, sell or purchase of illegal device for surreptitious interception of private communication. The maximum term of imprisonment upon conviction for this indictable offence is two years.

In addition, section 342.2 of the *Criminal Code* prohibits possession of a device, the design of which renders it primarily useful for committing an offence under section 342.1. The maximum term of imprisonment upon conviction for this indictable offence is two years.

Section 327 of the *Criminal Code* creates a related offence, possession of a device the design of which renders it primarily useful to obtain telecommunications services without payment.

Computer-related forgery: There is no specific offence of "computer-related forgery' but there are criminal offence for "forgery" under the *Criminal Code* which are equally used in the computer crime context. The general forgery offence is defined by section 366 of the *Criminal Code*. With respect to credit cards, section 342 of the *Criminal Code* deals with theft and forgery of credit cards while section 342.01 deals with making, having or dealing in instruments for forging or falsifying credit cards.

Computer-related fraud: There is no specific offence of "computer-related fraud" but there are a number of criminal offences for fraud under the *Criminal Code* which are used for computer related fraud. The general fraud offence is defined in by section 380 of the *Criminal Code*. For example, fraudulent telemarketing via Internet is a computer-assisted crime that could be charged under section 380 of the *Criminal Code*.

Child pornography: Section 163.1 of the *Criminal Code* makes it an offence to possess, transmit, distribute, make available and access child pornography, among other offences. The definition of child pornography in Canada is very broad and not only includes images depicting the abuse of actual children, but also depictions of non-real children (adults depicted as children, cartoons, drawings, etc.). The definition also covers a variety of media including video and audio recording as well as certain forms of written material.

Section 164.1 of the *Criminal Code* (notice and takedown**)** allows a judge to issue a warrant to seize any material from a computer system presumed to constitute child pornography. The Internet Service Provider or custodian of the system may be ordered to remove the material, provide the court with electronic copies of it, and/or provide information on the identity and location of the person who posted it. If the material is proven to be child pornography, the custodian may be ordered to delete the material.

Section 172.1 of the *Criminal Code* deals with luring of children on the Internet. Section 172.1 of the *Criminal Code* criminalizes electronic communications with a person believed to be a child for the purpose of facilitating the commission of a sexual offence against that child. The maximum term of imprisonment upon conviction for this indictable offence is up to ten years. This offence is also punishable on summary conviction with a prison term of up to eighteen months.

Most of the child sexual exploitation offences also carry mandatory minimum penalties. Bill C-10, currently before Parliament, would increase mandatory minimum sentences in respect of these offences and have them apply to all child sexual exploitation offences.

Bill C-22 (*An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service*) came into force on December 8, 2011, along with its accompanying Regulations (*Internet child pornography reporting Regulations*). This new Act requires those who provide Internet services to the public to make a report to the Canadian Centre for Child Protection (designated agency as per the Regulations) when they are advised of an Internet address where child pornography may be available to the public. Those providers are also required to notify police and safeguard evidence if they believe that their Internet service is being or has been used to commit a child pornography offence. Failure to comply with the duties under this new Act constitutes an offence punishable by summary conviction with a graduated penalty scheme. However, nothing in the Act either requires, or authorizes, any individual or company to actively seek out incidences of child pornography. In other words, those who provide an Internet service to the public are not required to monitor their networks for this type of material. This new federal legislation moves this type of reporting out of the voluntary sphere and is designed to work with and complement the recent provincial legislation on mandatory reporting of child pornography found in the provinces of Manitoba (S.M. 2008, c. 9, proclaimed into force on April 15, 2009), Nova Scotia (S.N.S. 2008, c. 35, proclaimed into force on April 13, 2010), Alberta (S.A. 2010, c. M-3.3, awaiting proclamation) and Ontario (2008, S.O. 2008, c. 21, awaiting proclamation). It should be noted that these provincial statutes were enacted under the provinces' civil jurisdiction over child welfare, making it mandatory for all citizens to report all forms of child pornography (adding to existing provincial reporting obligations in relation to child abuse and neglect).

Offences related to infringements of copyright and related rights: There are a number of statutes which govern Canada's intellectual property regime. The

Copyright Act, the *Trade-Marks Act* , the *Industrial Designs Act* and the *Patent Act* are the primary domestic legislative instruments in this area, however, only the Copyright Act contains provisions the purpose of which is to provide criminal remedies, namely sections 42 and 43. It should be noted that the *Criminal Code* contains certain relevant provisions, as well. For instance, section 406 to 412 of the *Criminal Code* deal with trademarks, and the proceeds of crime regime may also be used in the enforcement of certain copyright offences, including unauthorized recording of a movie (s. 432)

In addition, the Canadian government has tabled Bill C-11 this fall, also known as the *Copyright Modernization Act*. When enacted, this act will bring Canada's copyright legislation in line with the protections afforded by the World Intellectual Property Organization (WIPO) Treaties. To this effect, one should note that a new offence will be created against the circumvention of technological protection measures. Finally, it is worth mentioning that Canada signed the *Anti-Counterfeiting Trade Agreement* on Oct, 1 2010. Section 4 of the ACTA contains obligations for State Parties to provide criminal procedures and penalties in cases of both trademark counterfeiting and copyright piracy. Section 27 also provides that both civil and criminal remedies should be available under Parties' law against acts of infringement taking place in the digital environment.

Other offences: Section 326 of the *Criminal Code* creates the offence of theft of telecommunication services.

It should be noted that Canadian law does not generally criminalize theft of intangibles, where the owner is not deprived of his or her enjoyment of the property. However, in the context of the theft of intellectual property, section 322 (Theft) has been successfully prosecuted when software was stolen via a computer system.

1.2. If your country does not have a cyber-crime law that criminalizes any of the above conduct, are there currently any efforts to enact such laws: Yes ( ) No ( )

If so, please describe those efforts: _____
_____
_____

1.3. Do the emergency laws or other emergency measures in your country permit criminal investigators to compel Internet Service Providers to preserve electronic evidence without the need for a court order? Yes () No (X)

If so, kindly provide a brief description of the provisions and/or other measures in place in that regard, together with a copy, preferably electronic, thereof:

The Government previously introduced a Bill that proposed new procedural provisions, which included a data preservation scheme. While this Bill died on the Order Paper with the prorogation of Parliament in March 2011, it is anticipated that this Bill will eventually

be re-introduced. This comprehensive Bill, among other things, amended substantive offences and procedural powers of the *Criminal Code* to better address cyber-crime and updates the *Criminal Code* to enable it to respond to today's telecommunications reality. In relation to data preservation, the proposed legislation would have allowed a peace officer or public officer to demand data preservation without a court order. This provided peace or public officers with time to obtain a judicial order for further preservation or production of the computer data (or in some cases, to obtain a search warrant).

1.4. Has your country adopted substantive or procedural legislation or other necessary measures whereby its competent authorities can:

a) Seize, confiscate, or attach computer systems or computer-data storage media? Yes (X) No ( )

b) Copy and keep the computer data accessed? Yes (X) No ( )

If so, kindly provide a brief description of the provisions and/or other measures in place together with a copy, preferably electronic, thereof:

Section 487 of the *Criminal Code* authorizes the issuance of a search warrant in respect of "a building, receptacle or place". With respect to computer-stored evidentiary data, the search warrant may be directed to the place in which the "receptacle" is located, or to the receptacle itself, if the data being sought is at that location or is available to the computer system. This provision contains specific powers pertaining to the search of computer systems, including some third party assistance. More involved third party assistance may also be obtained through the issuance of an assistance order (s.487.02).

Further, the General Warrant (s. 487.01 of the *Criminal Code*)allows police to ask a court to authorize any type of investigative technique not already covered by another warrant/order/authorization provision in the *Criminal Code*.

1.5. Do the procedural laws in your country allow for the lawful interception of electronic communications transmitted in its territory via computer systems? Yes (X) No ( )

If so, kindly provide a brief description of the provisions and/or other measures in place in that regard, together with a copy, preferably electronic, thereof:

Part VI of the *Criminal Code* is the main piece of legislation governing electronic surveillance and the interception of private communications in Canada for law enforcement.

II. SPECIALIZED UNITS & NATIONAL EFFORTS

2.1. Is there a specialized unit or agency in your country specifically charged with the investigation of computer crimes? (police authority) Yes (X) No ( )

If so, please supply the following information:

- Name of the unit or agency: RCMP Technological Crime Program
- Institution to which it reports: Royal Canadian Mounted Police
- Internet address of the unit or agency: www.rcmp.gc.ca
- Contact information:
    - Name of contact: Superintendent Tony Pickett
    - Address: 1426 Blvd St-Joseph, Ottawa, Ontario, K1A 0R2
    - Telephone(s): 613-949-8909 Fax: 613-993-2963
    - E-mail address: tony.pickettt@rcmp-grc.gc.ca

2.2. Is there a specialized unit or agency in your country specifically assigned the responsibility of prosecuting cyber-crimes? Yes () No ()

If so, please supply the following information:

- Name of the unit or agency: _____
- Institution to which it reports: _____
- Internet address of the unit or agency: _____
- Contact information:
    - Name of contact: _____
    - Address: _____
    - Telephone(s): _____ Fax: _____
    - E-mail address: _____

The prosecution of *Criminal Code* offences largely falls to Canada's provincial Crown attorneys. While the federal government is responsible for the *Criminal Code* and amendments to that Act, the provinces are responsible for administering the majority of *Criminal Code* offences, the significant exceptions being drug offences and proceeds of crime. The federal and provincial governments share jurisdiction in respect of organized crime and terrorism offences. Some provincial governments have specialized cyber-crime prosecution units, but not all. Partners seeking assistance from Canadian authorities should inquire whether or not a specialized unit exists in the province that relates to the inquiry.

2.3. Has your country established any Internet pages to provide citizens with information on how to avoid falling prey to cybercrimes and on how to detect and report such crimes to competent authorities when they do occur?

Yes (X) No ( )

If so, kindly provide the respective Internet address/es of the page/s, as well as a brief description of the website/s:

www.getcybersafe.ca
Getcybersafe.ca is a public awareness campaign first launched on October 1, 2011 during Cyber Security Awareness Month. The campaign, which comprised of television, radio and online advertising, aimed to sensitize Canadians to some of the risks in cyberspace and provides them with tips to protect themselves. While the advertising portion of the campaign was not extended beyond October, the website remains available for Canadians to consult and is referenced in other cyber-related communications products aimed at Canadians.

Canadian Anti-Fraud Centre (www.antifraudcentre-centreantifraude.ca)
The Canadian Anti-Fraud Centre provides information on how to recognize fraud (both online and offline) and allows Canadians to report it. Although the Canadian Anti-Fraud Centre is run by Canadian law enforcement agencies, it does not conduct investigations. It gathers information on frauds and criminal organizations, which is then analyzed for connections between suspects and between victims, and it prepares investigative reports to provide law enforcement with a situational awareness on the latest fraud methods and trends. If a person wishes for the police to investigate an occurrence of suspected fraud, they need to file a police report with their local authorities.

Canada's Anti-Spam Centre (www.fightspam.gc.ca)
Canada's Anti-Spam law (Bill C-28) received Royal Assent on December 15 2010. Once the requisite regulations are in place, the legislation will be brought into force and generally prohibit the following actions:

- sending of commercial electronic messages without the recipient's consent (permission), including messages to email addresses and social networking accounts, and text messages sent to a cell phone;
- alteration of transmission data in an electronic message which results in the message being delivered to a different destination without express consent;
- installation of computer programs without the express consent of the owner of the computer system or its agent, such as an authorized employee

The fightspam.gc.ca website currently provides background information on the Anti-Spam law, and how individuals and businesses can protect themselves. Once the Anti-Spam Centre is operational, Canadians will also be able to use the website to report spam.

www.cybertip.ca
Cybertip.ca is a website run by the Canadian Centre for Child Protection (a charitable organization) with funding from the Government of Canada and Canadian companies. It is Canada's national reporting hotline for the sexual exploitation of children. Credible reported incidents are reported to the relevant law enforcement authorities for further action.

2.4. Has your country developed and/or implemented a national cyber-security strategy that includes efforts to deter, investigate and prosecute cybercrime, as part of a broader and more coordinated effort to protect the computers and networks of their citizens?

Yes (X) No ( )

If so, kindly provide a brief description of that strategy:

Pillar three of *Canada's Cyber Security Strategy* is to help Canadians to be secure online. As part of this pillar, the Government of Canada is preparing legislation to permit the

ratification of the *Budapest Convention on Cyber-crime* (more on this in question 3.1). Canada has also enhanced the capacity of law enforcement by establishing the Cyber Crime Fusion Centre, which provides the RCMP with a better situational awareness of the cyber crime environment. The entire strategy can be accessed at the following link: http://www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx

III. INTERNATIONAL COOPERATION

3.1. Has your country acceded to the Council of Europe Convention on Cybercrime?

Yes ( ) No (X)

If not, has your country considered applying any of the principles contained in that Convention?

Yes (X) No ( ) Do Not Know ( )

If so, please describe what that consideration has entailed:

Canada has been a signatory to the Council of Europe Convention on Cyber-crime since 2001 and plans to ratify the *Convention* as soon as the necessary implementing amendments have been enacted.

3.2. Has your country joined the G8 24/7 High Tech Crime Network? Yes (X) No ( )

If not, has your country taken any steps to join it? Yes ( ) No ( ) Do Not Know ( )

If so, please describe those steps: _____
_____
_____

3.3. Do the laws of your country allow for the processing of requests for mutual assistance from other states for the purpose of obtaining evidence in electronic form?

Yes (X) No ( ) Do Not Know ( )

If so, kindly provide a brief description of the provisions and/or other measures in place in that regard, together with a copy, preferably electronic, thereof:

3.4. Section 18 of the *Mutual Legal Assistance in Criminal Matters Act* provides that a court order may be obtained to gather information held by an Internet Service Provider and s. 15 of the same legislation provides that a search warrant may be obtained to seize a computer.Has your government presented or received requests for mutual assistance for the investigation or prosecution of computer crimes or for the purpose of obtaining evidence in electronic form and taking other steps necessary to facilitate the investigation or prosecution of computer crimes? Yes (X) No ( ) Do Not Know ( )

If so, please indicate the number of requests presented and/or received and the status of those requests: Although the questionnaire does not specify a time period, Canada can advise that it has received a number of requests for the purpose of obtaining data in electronic form over the last 3 years. From 2008 to 2010, Canada received or sent abroad 87 requests for mutual legal assistance (66 received, 21 sent abroad) in relation to a number of offences, including interference with computer systems, illegal internet pornography, child exploitation or the exploitation of women, luring and internet threats.

IV. TRAINING

4.1. Does your country provide training to law enforcement personnel on computer crimes and the collection of electronic evidence? Yes (X) No ( )

If so, please provide a brief description on the type of training and number of personnel trained:

Canadian law enforcement has standardized their computer crime and electronic evidence collection training through the Canadian Police College (CPC), which offers a comprehensive cybercrime training program. This national approach to technological crime investigations is critical in maintaining response capability in terms of common knowledge, skills and abilities. The Technological Crime Learning Institute's (TCLI) centralized training approach, relatively unique internationally, ensures consistent, high-quality standards in Canadian high-tech crime investigations. These courses are also open to international law enforcement agencies. A list of available courses and related information can be found at: www.cpc.gc.ca/en/technological-crime-learning-institute

4.2. Does your country provide training to prosecutors on computer crimes and the collection of electronic evidence? Yes (X) No ()

If so, please provide a brief description on the type of training and number of personnel trained:

Each year, the Public Prosecution Service of Canada offers a module of wiretap training to their prosecutors.

4.3. Regarding your country's efforts to provide training on investigating and prosecuting crimes involving computers and the Internet, please describe your country's goals for the next two years and the necessary conditions to achieve those goals:

The Canadian Police College's objectives over the next two (2) years is to ensure their current course curriculum remains relevant to the needs of law enforcement officials in Canada. No specific training needs outside the current curriculum have been identified at this time.

4.4. Has your country sent officials to workshops presented by the Working Group on Cyber-crime? Yes (X) No ( ) Do Not Know ( )

If so, please provide a brief description of who has participated in these workshops, whether the workshops have provided useful training, and how the participants have applied this training in their work:

The Department of Justice has sent a representative to at least two of the OAS Workshops and Meetings (Madrid and Port of Spain). Canada was one of the training countries giving instruction at these workshops. Although not an end-user, Canada believes these to be useful networking exercises which are vital in the fight against the global phenomenon of cyber-crime. The Royal Canadian Mounted Police has only participated with the Working Group on one occasion and is not in a position to evaluate either the usefulness of the training or the application of the training to our duties. The RCMP however remains committed to partnerships with other organizations to further technological expertise in this area.

4.5. Please provide recommendations on the most important topics related to computer crime and electronic evidence that should be incorporated into Working Group workshops for the next two years:

We recommend the Working Group review the new Council of Europe's Cyber-crime Convention Committee (T-CY) "Cybercrime Strategy" efforts. Their new workshops are distinct from, but entirely complimentary to the COE Budapest Convention on Cyber-crime. The RCMP would be pleased to collaborate in this effort.

4.6. Within the mandates of the REMJA, please provide recommendations on how the Working Group on Cyber-crime can best assist your country in developing or enhancing its ability to address crimes involving computers and the Internet:

Cross-border investigations present unique challenges. Canada recommends that the Working Group on Cyber-crime may wish to look at ideas to address jurisdictional and legal issues in relation to cross-border searches whether through legislative reforms or bilateral arrangements.

INFORMATION ON THE OFFICIAL RESPONSIBLE FOR COMPLETION OF THIS QUESTIONNAIRE

Please provide the following information:

(a) State: Canada
(b) The official to be consulted regarding the responses to the questionnaire is:
(X) Ms.: Normand Wong
Title/position: Counsel
Agency/office: Department of Justice Canada
Address: 5033-284 Wellington, , Ottawa, Ontario K1G 0J3
Telephone number: 613-941-2341
Fax number: 613-941-9310
E-mail address: nwong@justice.gc.ca