LIBRARY of PARLIAMENT
BIBLIOTHÈQUE du PARLEMENT

BACKGROUND PAPER

Cybercrime: Issues

Publication No. 2011-36-E
5 April 2011

Dominique Valiquet

Legal and Legislative Affairs Division
Parliamentary Information and Research Service

Cybercrime: Issues
(Background Paper)

HTML and PDF versions of this publication are available on IntraParl (the parliamentary intranet) and on the Parliament of Canada website.

In the electronic versions, a number of the endnote entries contain hyperlinks to referenced resources.

Ce document est également publié en français.

Library of Parliament ***Background Papers*** present and analyze various aspects of current issues in an objective, impartial manner. They are prepared by the Parliamentary Information and Research Service, which carries out research for and provides information and analysis to parliamentarians and Senate and House of Commons committees and parliamentary associations.

Publication No. 2011-36-E
Ottawa, Canada, Library of Parliament (2011)

CONTENTS

CYBERCRIME: ISSUES

1 CYBERCRIME

In its *2009–10 Report on Plans and Priorities*, Public Safety and Emergency Preparedness Canada included developing a government-wide cybersecurity strategy as one of its priorities.[1] The purpose of that strategy is to achieve cross-government cyberintegrity, protect the economy and critical infrastructure, and combat cybercrimes.

The strategy, which is currently being implemented, requires modernizing, in a context of international cooperation, both the Canadian legislative framework and investigative techniques. This will allow law enforcement and national security agencies[2] to have access to the information they need and to lawfully investigate criminal and terrorist acts perpetrated through the illicit use of new technologies, as well as criminal and terrorist organizations using these technologies to advance their causes.[3]

1.1 DEFINITION

Although much is being said about cybercrime, there is not unanimous agreement on a single definition of the concept.[4] However, the following definition, used by the Canadian Police College, is gaining acceptance: cybercrime is "a criminal offence involving a computer as the object of the crime, or the tool used to commit a material component of the offence." [5]

According to this definition, cybercrime may for practical purposes be divided into two categories:

- *Pure computer crimes*, where a computer is the object of the crime. This category includes specific new offences that target computer systems and networks. Examples are hacking, denial-of-service attacks,[6] and malicious dissemination of computer viruses.
- *Computer-supported crimes*, where a computer is the instrument used in perpetrating the crime. This category includes the use of a computer to commit such traditional offences as child pornography, harassment, fraud and drug trafficking.

1.2 CHALLENGES

Cybercrime has given rise to a number of challenges for legislators and law enforcement agencies, including:

- the enforcement of Canadian laws in cyberspace and international cooperation in investigating cybercrime;

- the modernization – updating and creating – of offences to include new computer crimes or new forms of offences; and
- the modernization of investigative techniques.

This paper gives a brief overview of the three challenges.

2 INTERNATIONAL ASPECTS OF CYBERCRIME

The general principle of territoriality applied in Canada holds that no one can be convicted in Canada of an offence committed entirely outside Canada,[7] except in cases of certain very specific offences, such as torture, terrorism and child sex tourism.[8]

Cybercrime, however, knows no borders, a fact that significantly complicates police investigations. Cooperation among countries is therefore essential in combatting this type of crime.

2.1 JURISDICTION OF CANADIAN LAWS

The *Convention on Cybercrime* (the Convention),[9] to which Canada is a signatory,[10] requires that each State party prosecute cybercrimes committed within its territory.[11] This means that a country could claim territorial jurisdiction in a case where the computer system attacked is on its territory, even if the perpetrator of the attack is not.

Australia, for instance, has expressly given its authorities the power to prosecute a computer hacker who attacks a computer in Australia from outside Australia.[12] The United States has also amended its legislation to permit prosecutions of individuals abroad who hack computers in the United States, as well as individuals in the United States who attack computers in other countries.[13] The amendments also allow the American authorities to investigate hacking from outside the country in cases where a computer in the United States is used as an intermediary.[14]

To eliminate "safe havens," the Convention requires that State parties that do not extradite an offender because of his or her nationality must have jurisdiction to prosecute the individual within their own territory.[15] Although Canada does prosecute offences committed in this country and extradites its nationals, some clarification is needed regarding enforcement of Canadian laws in relation to offences committed in cyberspace.

2.2 MUTUAL LEGAL ASSISTANCE TREATIES

Under bilateral mutual legal assistance treaties and multilateral conventions, Canada is able to receive and provide assistance in collecting evidence in criminal cases involving other countries, using coercive measures where necessary. However, according to Canadian law enforcement agencies and prosecutors, those mechanisms often take too long.[16] Given the speed with which computer data can be moved around, altered or deleted, a possible solution would be to establish a speedy

procedure for preserving evidence in the possession of Canada's international partners.

As well, evidence in cybercrime prosecutions often comes from numerous different jurisdictions. Witnesses in other countries must therefore come to Canada to testify in court. A report prepared for the Canadian Association of Police Boards proposed that an amendment to the *Canada Evidence Act* to allow affidavit or video evidence would be worth considering in those cases.[17]

3 MODERNIZATION OF OFFENCES

Although Canadian law covers most cybercrimes, the emergence of new technologies suggests that a review of Canadian criminal offences could be needed, with updating where necessary.

3.1 VIRUSES

At present, only disseminating or attempting to disseminate computer viruses (as well as other malicious codes, such as worms and Trojan horses) is an offence.[18]

To ratify the *Convention on Cybercrime*, Canada would have to amend its *Criminal Code* (the Code) to make the following activities offences in Canadian law: the production, importation, sale, or the making available or possession of a virus or another malicious code for the purpose of committing a cybercrime.

3.2 CHILD PORNOGRAPHY

The child pornography provisions currently in the Code seem to be well suited to cyberspace. In addition to production and possession, accessing child pornography (for example, by visiting a web page) and making child pornography available (for example, through the use of a file-sharing program such as P2P) constitute offences.

To help police services combat major cybercrimes like these, a federal–provincial–territorial working group on cybercrime is examining the possibility of compelling Internet service providers (ISPs) to report incidents of child exploitation that occur on their networks.

In June 2008, the Manitoba legislature enacted legislation[19] requiring that individuals report any child pornography they become aware of to Cybertip.ca.[20] Alberta, Nova Scotia and Ontario soon enacted similar legislation.[21]

At the federal level, Bill C-22,[22] which received Royal Assent on 23 March 2011, requires ISPs and other persons providing Internet services (e.g., Facebook, Google and Hotmail) to report any incident connected with child pornography.[23]

The United States[24] and Australia[25] adopted legislation in 2002 and 2005, respectively, imposing this type of obligation on telecommunications service providers.

3.3 IDENTITY THEFT

The Code covers most fraudulent uses of personal information by identity thieves. However, before Bill S-4[26] came into force in January 2010, the Code did not apply to collecting, possessing and unlawfully trafficking in personal information (except in respect of credit cards and computer passwords) for future criminal use.

Bill S-4 has corrected this situation by creating two new offences: identity theft and trafficking in identity information. In addition to updating credit card offences, the bill provides that a judge may order an offender to compensate a victim of identity theft.[27]

3.4 SPAM

Spam is unsolicited electronic messages. It has evolved from a nuisance to a vehicle for committing offences such as virus dissemination, fraud and identity theft. Although spam represents about 80% of global email,[28] Canada was, until recently, the only G8 nation with no anti-spam law.

In May 2005, Canada's Task Force on Spam recommended legislation to prohibit unsolicited commercial electronic messages.[29] Bill C-28,[30] which received Royal Assent on 15 December 2010, provides a clear regulatory scheme, including administrative monetary penalties, with respect to both spam and related threats from unsolicited electronic contact, including identity theft, phishing,[31] spyware,[32] viruses and botnets.[33] It also grants an additional right of civil action to businesses and consumers targeted by the perpetrators of such activities.[34]

3.5 OTHER EMERGING OFFENCES IN CYBERSPACE

In a 2008 survey of law enforcement agencies carried out for the Canadian Association of Police Boards, Crown prosecutors and other representatives of governments in Canada identified two increasingly important issues: cyberbullying of children and organized crime on the Internet.[35]

Although existing offences seem to apply to these two phenomena, it may be worthwhile to examine them further.

4 MODERNIZATION OF INVESTIGATIVE TECHNIQUES

Law enforcement agencies say that new technologies often impede the lawful interception of communications, specifically in relation to users' anonymity, encrypted messages, and the relatively ephemeral nature of the information. The following sections briefly describe these issues as well as possible approaches to them.[36]

4.1 INTERCEPTION CAPABILITY

At present, no Canadian legislation compels all telecommunications service providers to use apparatus capable of intercepting communications.[37] The absence

of standards regarding telecommunications service providers' interception capabilities could be remedied by legislation, which could also require all telecommunications service providers – such as Internet service providers or manufacturers of devices such as the BlackBerry – to use technology that would enable law enforcement agencies to intercept telecommunications for investigation purposes after obtaining a judicial authorization.[38]

Australia, the United States and the United Kingdom, among others, have imposed these requirements for more than 10 years.[39]

4.2 Request for Subscriber Information

At present, law enforcement agencies generally require a warrant to compel telecommunications service providers to provide them with personal information concerning their customers.[40] This means that law enforcement agencies holding an Internet protocol address (IP address)[41] associated with the commission of an offence must obtain a warrant to compel the telecommunications service provider to supply the name of the subscriber associated with the IP address. Furthermore, the warrant application must include the name of the person suspected of the offence.

These difficulties could be remedied by adopting special rules to allow law enforcement agencies to compel a telecommunications service provider – without a warrant, but subject to certain requirements – to supply basic identifying information about a subscriber, such as the individual's name, IP address, email address or telephone number.[42] It has been argued that this kind of information request should still be subject to prior approval by a judge.[43]

It is worth noting that in a February 2009 decision,[44] the Ontario Superior Court of Justice held that subscribers do not have a reasonable expectation of privacy regarding basic information held by their ISP. Later that year, the Ontario Court of Justice clarified the issue, holding, in *R.* v. *Cuttell*,[45] that an ISP can disclose the names and addresses of subscribers to law enforcement agencies without a warrant only if the service agreement allows it. Most service agreements with the major ISPs in Canada permit such disclosure.

Recently, the Supreme Court of British Columbia – of the opinion that an ISP receiving a request for subscriber information from a law enforcement agency is not an "Agent of the State" – held that such an ISP may voluntarily disclose this information to the police without the prior approval of a judge.[46]

Considering the uncertainty of the case law on the requirement for a warrant, this debate will probably continue until the Supreme Court of Canada settles the issue.

4.3 Obligation to Retain Telecommunications Data

On 15 March 2006, the European Union adopted Directive 2006/24/CE on the retention of telecommunications data.[47] This directive requires telecommunications

service providers to retain this type of data for six months to two years and provide national authorities with access to it for the purposes of the detection and prosecution of serious crime.

In Canada, telecommunications service providers are not required to collect and retain information about their subscribers' use of their services, such as individuals' Internet surfing activities.

4.4 Anonymous Services

According to law enforcement agencies, prepaid cell phone cards, Internet access cards, Internet cafés and Internet access terminals in public libraries complicate law enforcement investigators' jobs, because they allow users to remain anonymous.

At present, telecommunications providers have no obligation to verify their users' identity.

4.5 Preservation Order

The speed and ease with which information on the Internet can be destroyed or modified can lead to the loss of evidence. Provision in the Code for a preservation order would be one way to guard against this.[48] Such a temporary judicial order, which would be in effect during the time the law enforcement agency sought a search warrant, would require a telecommunications service provider to preserve information about a specific telecommunication or individual.

Former Bill C-51,[49] which died on the *Order Paper* when the federal general election was called on 26 March 2011, included such orders with regard to the preservation of computer data.[50]

4.6 Production Order

A production order and a search warrant are similar in that they are both provided by a judge. The difference between the two is that in the case of a production order, the person in possession of the information must produce it on request, whereas in the case of a search warrant, the law enforcement agency goes to the place where the information exists to obtain it by seizing it. Law enforcement agencies can more easily obtain documents that are located in another country using a production order.

At present, the Code provides a procedure for obtaining a general production order, one that applies regardless of the type of information a law enforcement agency is seeking.[51] The order is issued based on the existence of reasonable grounds *to believe* that an offence has been committed. Because there are some who think that the expectation of privacy is lower for telecommunications data than for other types of information, consideration could be given to creating a production order specifically to obtain telecommunications data[52] based on the less stringent criterion of reasonable grounds *to suspect* that an offence has been committed.[53]

Former Bill C-51, mentioned above, included such orders with regard to the production of certain types of information, such as telecommunications and tracking data.

4.7 Interception of Electronic Mail

The treatment of electronic mail is the subject of debate: Does a law enforcement agency that wants to obtain a suspect's electronic mail have to apply for a search warrant or for an authorization to intercept under Part VI of the Code? (The rules in Part VI – which allow police services to intercept a "private communication"[54] – are more stringent than the rules relating to search warrants.)

Some argue that, although an email may be a communication, it is not certain that the author can reasonably expect that only the recipient will see it, in other words, that it is private. They contend that, because an email can be easily intercepted,[55] and the author has ready access to encryption technology to guarantee its confidentiality, it cannot be considered a "private communication" within the definition in the Code.[56]

On the other hand, one could argue that this logic also applies to a communication by telephone. Why should a distinction be made between the protection applicable to an email and to a telephone communication, particularly when electronic mail, just as a telephone communication, may well contain a variety of content, including sensitive personal information?

4.8 Encryption

Encryption is a process used to make information unreadable to anyone who does not possess the proper key to decipher it. To protect the confidentiality of messages transmitted on the Internet, encryption technologies have become increasingly sophisticated and accessible.

While useful to protect legitimate communications on the Internet, encryption impedes law enforcement agencies' lawful interception of communications in the course of criminal investigations.

As a result, telecommunications service providers could be required to give law enforcement agencies access to decrypted communications, regardless of the technology those service providers use.[57] As well, all encryption technologies could be required to contain a decryption key to which law enforcement agencies would have access. However, such a measure raises privacy-related issues.

NOTES

1. Public Safety and Emergency Preparedness Canada, *2009–10 Report on Plans and Priorities*, Ottawa, 2009, p. 10.
2. This paper uses the expression “law enforcement agencies” to include both law enforcement and national security agencies, as the context requires.
3. Public Safety and Emergency Preparedness Canada (2009), p. 18.
4. This absence of a definition impedes the collection of statistics on cybercrime.
5. Canadian Police College, quoted in Canadian Centre for Justice Statistics, *Cyber-crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics*, Statistics Canada Catologue No. 85-558-XIE, December 2002, p. 5.
6. A “denial-of-service attack” is an attack on a computer system or network that results in loss of service for users.
7. *Criminal Code*, R.S.C., 1985, c. C-46, s. 6(2). See also *Libman* v. *The Queen*, [1985] 2 S.C.R. 178, in which the Supreme Court of Canada addressed the “real and substantial link” between an offence and a country.
8. The exceptions to the general rule of territoriality are set out in s. 7 of the *Criminal Code*.
9. Council of Europe, *Convention on Cybercrime* [Convention], 23 November 2001.
10. Canada signed the Convention on 23 November 2001.
11. Convention, art. 22.
12. Richard W. Downing, “Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime,” *Columbia Journal of Transnational Law*, Vol. 43, No. 3, 2005, p. 737.
13. Ibid. As a result, a 24/7 network has been created to implement a speedy and effective procedure for collaboration among the G8 countries’ law enforcement agencies (see the G8 Moscow agreement: Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, *Communiqué*, Moscow, 19–20 October 1999). The *Convention on Cybercrime* also provides for this kind of network.
14. To cover their tracks, hackers often use a network of intermediary computers (referred to as “zombie” computers) between their own computer and the hacked computer.
15. Convention, art. 22.
16. Deloitte & Touche LLP, *A report on cybercrime in Canada*, Prepared for the Canadian Association of Police Boards, Ottawa, 29 April 2008, p. 14. Some law enforcement organizations therefore prefer to seek the direct cooperation of private enterprises in the other country. An example is Microsoft, which manages the servers for Hotmail in the United States.
17. Ibid., p. 14.
18. *Criminal Code*, ss. 342.1(1)(*c*) and 430(1.1).
19. Manitoba, *The Child and Family Services Amendment Act (Child Pornography Reporting)*, s. 18(1.0.1).
20. Cybertip.ca is the Canada-wide service for reporting sexual exploitation of children on the Internet.

21. Alberta, *Mandatory Reporting of Child Pornography Act*, S.A. 2010, c. M–3.3; Nova Scotia, *Child Pornography Reporting Act*, c. 35, 2008; Ontario, *Child and Family Services Act*, R.S.O. 1990, c. 11, s. 72(1.1).

22. Bill C-22: An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, 3rd Session, 40th Parliament.

23. For more information on this subject, see Dominique Valiquet, *Legislative Summary of Bill C-22: An Act respecting the mandatory reporting of Internet child pronography by persons who provide an internet service*, Publication no. 40-3-C22-E, Parliamentary Information and Research Service, Library of Parliament, revised 15 February 2011.

24. United States, *United States Code* (USC), Title 18, Chapter 110, art. 2258A.

25. Australia, *Criminal Code Act 1995, Schedule*, s. 474.25.

26. Bill S-4: An Act to amend the Criminal Code (identity theft and related misconduct), 2nd session, 40th Parliament.

27. For more information on Bill S-4, see Nancy Holmes and Dominique Valiquet, *Legislative Summary of Bill S-4: An Act to amend the Criminal Code (identity theft and related misconduct)*, Publication no. LS-637E, Parliamentary Information and Research Services, Library of Parliament, 5 June 2009.

28. Ibid.

29. Canada, Task Force on Spam, *Stopping Spam: Creating a Stronger, Safer Internet – Report of the Task Force on Spam*, Industry Canada, Ottawa, May 2005.

30. Bill C-28: An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, 3rd Session, 40th Parliament.

31. Phishing is the impersonation of a trusted person or organization in order to steal a person's personal information, usually for the purposes of identity theft.

32. Spyware is software that collects information about a user, or modifies the operation of the user's computer, without the user's knowledge or consent.

33. A "zombie" is a computer that runs a virus allowing the creator, distributor or controller of the virus to remotely control another computer. A botnet is a collection of "zombie" computers used to send spam or for another purpose.

34. For more information on Bill C-28, see Alysia Davies and Terrence J. Thomas, *Legislative Summary of Bill C-28: An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities*, Publication no. 40-3-C28-E, Parliamentary Information and Research Services, Library of Parliament, 14 February 2011.

35. Canadian Association of Police Boards (2008), p. 11. International mutual assistance in relation to organized crime will be provided in many cases under the *United Nations Convention Against Transnational Organized Crime and the Protocols Thereto* (Palermo Convention). (See François Blanchette, "Entraide juridique et cybercriminalité au Canada : le cadre légal national et international," in *Legal.TI, droit et technologies de l'information : Devenir aujourd'hui l'avocat de demain*, Éditions Yvon Blais, Cowansville, Que., 2008, pp. 18–19.

36. Most of the measures presented derive from public consultations that the federal government conducted in preparing former Bill C-74 (the Modernization of Investigative Techniques Act, 1st Session, 38th Parliament), between 2002 and 2005. Bill C-74 was introduced in November 2005 and died on the *Order Paper* before second reading in the House of Commons.

37. Only licensees that use radio frequencies for wireless voice telephone services have been required, since 1996, to have facilities that permit such interceptions. There is no similar legislation for other telecommunications service providers.

38. Former Bill C-74 (see note 36) and former Bill C-52 (Investigating and Preventing Criminal Electronic Communications Act, 3rd Session, 40th Parliament, which died on the *Order Paper* on 26 March 2011) included a similar requirement for telecommunications service providers, but not for manufacturers of devices.

39. For more information on this topic, see Dominique Valiquet, *Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia*, Publication no. 2005-66-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 28 February 2006.

40. See para. 7(3)(*c.1*) in the Personal *Information Protection and Electronic Documents Act*.

41. An IP address can be a fixed address, or it can change with each connection (a "dynamic" IP address).

42. Former bills C-74 (see note 36) and C-52 (see note 38) included a provision of this nature.

43. In 2007, the government supported that position. See Carly Weeks, "Warrant Needed to Pull Data on Internet Users: Day," *Ottawa Citizen*, 14 September 2007.

44. *R.* v. *Wilson* (10 February 2009), No. 4191/08. The Court held that a subscriber's name and address are not intimate details of the lifestyle or personal choices of the subscriber (see *R.* v. *Plant*, [1993] 3 S.C.R. 281 and *R.* v. *Gomboc*, [2010] 3 S.C.R. 211). The Ontario Court of Justice had previously decided the opposite in *R.* v. *Kwok*, [2008] O.J. 2414.

45. *R.* v. *Cuttell,* 2009 ONCJ 471, [Ontario Court of Justice] (2009 CarswellOnt 5896).

46. *R.* v. *McNeice*, 2010 BCSC 1544 [Supreme Court of British Columbia].

47. "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC," *Official Journal of the European Union*, L105/54, 13 April 2006. Telecommunications data are essentially data that show the origin, destination, date, time, duration and location of a telecommunication. They do not disclose the content of a telecommunication. The terms "traffic data," "transmission data" and "communications data" are also used.

48. There is provision for this type of measure in the *Convention on Cybercrime*.

49. Bill C-51: An Act to amend the Criminal Code, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act, 3rd Session, 40th Parliament.

50. For more information on Bill C-51, see Dominique Valiquet and Katherine Simonds, *Legislative Summary of Bill C-51: Investigative Powers for the 21st Century Act*, Publication no. 40-3-C51-E, Parliamentary Information and Research Service, Library of Parliament, Ottawa, 3 February 2011.

51. *Criminal Code*, s. 487.012. There is also provision for this type of measure in the *Competition Act*, para. 11(1)(*b*).

52. There is provision for this type of measure in the *Convention on Cybercrime*.

53. The *Criminal Code* already applies the *reasonable grounds to suspect* test in the case of orders to produce telephone number records (s. 492.2(2)) and banking information (ss. 487.013(1) and (4)), and, in the case of warrants, to install a tracking device (s. 492.1(1)).

54. Section 183 of the *Criminal Code* defines a "private communication" as:

> any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.

55. See *R.* v. *Weir*, [1998] 8 W.W.R. 228 (Alta Q.B.).

56. Robert W. Hubbard, Peter M. Brauti, and Scott K. Fenton, *Wiretapping and Other Electronic Surveillance: Law and Procedure*, Vol. 2, Canada Law Book, Aurora, Ont., March 2008, p. 15-20.

57. Former bills C-74 (see note 36) and C-52 (see note 38) contained a provision of this nature.