Université de Montréal

VERS L'ORGANISATION D'UNE CYBERPOLICE AU CANADA ET AU QUEBEC

Par
Stéphane Lapointe
École de criminologie
Faculté des arts et des sciences

Mémoire présenté à la Faculté des Études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M. Sc.)
en criminologie

Décembre 1999

Université de Montréal

Faculté des études supérieures

Ce mémoire intitulé :

VERS L'ORGANISATION D'UNE CYBERPOLICE AU CANADA ET AU QUEBEC

présenté par :

Stéphane Lapointe

a été évalué par un jury composé des personnes suivantes

Jean-Luc Bacher, président-rapporteur

Mylène Jaccoud, directrice de recherche

Nicole Soullière, membre du jury

Mémoire accepté le : 29 août 2000

Remerciements

Nous souhaitons remercier tout d'abord notre directrice de recherche, Mylène Jaccoud, professeure à l'École de criminologie de l'Université de Montréal, pour son enthousiasme face à ce projet de recherche, la rigueur de ses commentaires et ses encouragements.

Nous remercions les policiers de la Gendarmerie royale du Canada, de la Sûreté du Québec et du Service de police de la Communauté urbaine de Montréal qui ont accepté de s'entretenir avec nous malgré leur horaire de travail chargé. Un merci tout particulier à madame Martine Fourcaudot ainsi qu'à messieurs Pierre Avon et Yvon Myette de la Sûreté du Québec pour la confiance qu'ils nous ont témoignée et l'aide qu'ils nous ont généreusement accordée au moment où nous en avions le plus besoin.

Merci à nos précieux amis qui nous ont accompagné pendant ce long pèlerinage et qui nous ont, selon notre humeur, réconforté, amusé, écouté et attendu à la ligne d'arrivée. Merci à Francis Fortin, Jean-Pierre Guay, Marie-France Blais, Daniel Comptois, Pierre Fortier, François-Philippe Dubé, Anie Gagné, Julie Grenon, Nancy Bélanger et Marc Lafortune. Je vous aime beaucoup.

Finalement, merci aux membres de notre famille : Harold, Yolande, Pierre, Lynne et Serge pour leur soutien et pour nous avoir encouragé, à la fois à entreprendre cette démarche et à ne pas l'abandonner en cours de route.

Sommaire

Le présent mémoire porte sur le processus d'organisation des corps policiers canadiens et québécois par rapport à Internet. On y examine l'aspect organisationnel de ce processus ainsi que les expériences, points de vue et pratiques des policiers qui sont au cœur de ce processus. Il s'agit de la première recherche criminologique du genre au Canada, ce qui lui confère donc un caractère exploratoire.

Notre étude repose sur une méthodologie qualitative et les données analysées ont été recueillies à l'aide de trois techniques de recherche différentes. Dix entretiens semi-directifs ont été réalisés avec des policiers de la Gendarmerie royale du Canada, de la Sûreté du Québec et du Service de police de la Communauté urbaine de Montréal. Nous avons également réalisé une analyse documentaire de la littérature « grise » publiée par ces trois corps policiers ainsi qu'une observation participante de plusieurs mois à la Direction des renseignements criminels de la Sûreté du Québec.

Notre analyse des données révèle que le processus d'organisation de ces corps policiers par rapport à Internet en est encore à ses débuts et qu'il s'inscrit lui-même à l'intérieur d'un vaste et récent processus d'organisation par rapport à la criminalité informatique en général.

Au cœur de ce double processus, on trouve une dizaine de policiers regroupés au sein d'unités spécialisées en criminalité informatique. Ceux-ci ont pour principal mandat de supporter les enquêteurs de leur organisation dans les enquêtes qui impliquent Internet. Ces policiers sont cependant confrontés à de nombreux obstacles. Les ressources humaines, matérielles et monétaires accordées à leur unité sont limitées alors que la charge de travail, déjà imposante, ne cesse d'augmenter.

Nous espérons que les résultats de notre démarche de recherche seront utiles aux criminologues et gestionnaires des corps policiers qui s'intéressent à cette nouvelle sphère d'activité des forces de l'ordre.

Table des matières

Introduction

1. Introduction

Qui n'a pas, à au moins une occasion, entendu parler d'Internet ? Dans la plupart des pays industrialisés, la réponse à cette question est simple. Personne. Internet, ce méta réseau informatique, est sans contredit l'une des innovations technologiques les plus marquantes du 20^{ième} siècle.

Bien qu'Internet fut initialement pensé et développé pour offrir aux militaires américains un moyen de communication capable de survivre à un conflit nucléaire, il est aujourd'hui utilisé par des millions d'internautes de par le monde. Chaque jour, ceux-ci utilisent Internet pour magasiner, s'informer, effectuer des transactions bancaires ou rencontrer et échanger avec des amis.

Même si la majorité des gens use d'Internet de façon tout à fait légitime, quelques-uns l'utilisent pour poser des gestes problématiques dont certains sont criminalisés au Canada. La distribution et la vente de matériel pornographique légal et la diffusion d'instructions pour fabriquer des explosifs sont des exemples d'usages problématiques d'Internet. Quant aux usages criminels d'Internet, on en distingue deux types. D'une part, on trouve des crimes « conventionnels » qui sont maintenant réalisés via Internet, tels la fraude, le blanchiment d'argent, l'extorsion, les menaces ou la diffusion de pornographie juvénile. D'autre part, on y trouve également quelques crimes « innovateurs » qui n'existent que depuis l'avènement d'Internet, par exemple, l'intrusion dans les systèmes informatiques ou les méfaits aux données informatisées.

Notre formation de criminologue nous amène à nous questionner sur la façon dont les corps policiers réagissent à l'apparition de même qu'à la prolifération des usages problématiques d'Internet. Aucune recherche criminologique ne s'est intéressée à cette réaction policière jusqu'à maintenant. Nous avons donc décidé, dans le cadre de ce mémoire, d'examiner le processus d'organisation des corps policiers, canadiens et québécois, par rapport à Internet en général.

Deux facettes de ce processus nous intéressent particulièrement. Chacune fait l'objet d'une analyse particulière et correspond à un de nos objectifs de recherche. Nous désirons d'abord analyser l'aspect organisationnel de ce processus, c'est-à-dire comment les corps policiers, en tant qu'organisations, se sont adaptés par rapport à Internet. Nous espérons en apprendre davantage sur des thèmes tels que les circonstances qui mènent à l'intervention policière sur Internet, les structures implantées ainsi que le(s) mandat(s) et les ressources attribuées à ces structures.

Ensuite, nous souhaitons explorer les pratiques, les expériences et les points de vue des policiers qui sont au cœur de ce processus d'organisation. Parmi les thèmes qui nous intéressent, il y a l'opinion qu'ont ces policiers d'Internet, les relations qu'ils entretiennent avec divers acteurs, la vision qu'ils ont de leur travail et les obstacles auxquels ils sont confrontés dans leurs interventions sur Internet.

L'étude de ce processus sera utile pour l'avancement des connaissances en criminologie ainsi que pour les gestionnaires de corps policiers qui sont appelés, dans le cadre de leurs fonctions, à superviser directement ou indirectement une unité spécialisée en criminalité informatique.

Ce mémoire comporte quatre chapitres distincts où l'on aborde, dans l'ordre, ce que la littérature nous apprend sur notre objet d'étude, la méthodologie utilisée pour réaliser ce mémoire, l'analyse de l'aspect organisationnel du processus étudié et l'analyse des pratiques des policiers et des points de vue sur ces pratiques concernant la manière dont s'organisent les corps policiers pour contrer les problèmes engendrés par Internet.

Le premier chapitre présente une revue de la littérature relative à certains aspects de notre objet d'étude. Nous y abordons notamment le développement d'Internet, ses caractéristiques, les services qui y sont disponibles et les acteurs impliqués dans son développement et sa gestion. Ce chapitre traite également du respect de la vie privée, du fossé qui se creuse entre les pays « info-riches » et ceux « info-pauvres » ainsi que des

usages problématiques, non-criminalisés et criminalisés, d'Internet. Cette revue de la littérature se termine par un bref survol des réactions de différents acteurs face aux usages problématiques d'Internet.

Dans le second chapitre, nous détaillons les choix méthodologiques relatifs à notre démarche de recherche tels que l'adoption d'une méthodologie qualitative, les techniques de recherche utilisées pour recueillir les données, les objectifs et sous-objectifs à la base de l'étude et les stratégies employées pour l'échantillonnage et l'analyse des données.

Les résultats de nos analyses face à notre premier objectif de recherche sont présentés dans le troisième chapitre. Cet objectif, qui vise spécifiquement l'examen de l'aspect organisationnel du processus étudié, nous permet d'en apprendre davantage sur les circonstances qui ont favorisé le processus d'organisation face à Internet, le mandat confié aux unités chargées d'intervenir sur Internet, les ressources accordées à celles-ci ou encore, les relations qu'entretiennent ces unités avec divers acteurs.

Le quatrième chapitre dévoile les résultats de nos analyses relatifs à notre deuxième objectif de recherche et aux sous-objectifs qui le composent. Il porte sur l'examen des expériences, points de vue et pratiques des policiers au cœur du processus d'organisation par rapport à Internet. Dans ce chapitre, nous analysons l'opinion qu'ont ces policiers d'Internet, les obstacles à l'intervention policière sur Internet, l'opinion qu'ont les interviewés de leur travail et leur utilisation d'Internet.

Revue de littérature

2. Revue de littérature

Alors qu'Internet était initialement réservé aux chercheurs universitaires, on compte aujourd'hui plus de 250 millions d'internautes répartis dans le monde entier (Nua, Page consultée le 25 octobre 1999). Utilisé à l'origine pour transmettre des données scientifiques, Internet est maintenant employé pour effectuer des transactions bancaires, pour magasiner, pour rencontrer des gens ou encore pour interroger des banques de données.

Quoique la plupart des usages d'Internet soient légitimes et licites, quelques-uns sont considérés comme problématiques et même criminels dans plusieurs pays dont le Canada.

Suite à l'apparition et à la prolifération de ces usages problématiques, on sollicite de plus en plus l'intervention des corps policiers sur Internet. Toutefois, l'intervention policière dans ce nouvel univers virtuel diffère considérablement de l'intervention policière dans la rue et, par conséquent, exige des corps policiers qu'ils s'adaptent à la réalité du cyberespace.

Le questionnement à la base de notre démarche de recherche porte précisément sur le processus d'organisation des corps policiers, canadiens et québécois, face à Internet. Même si la littérature criminologique sur ce processus est quasi inexistante, quelques auteurs se sont intéressés à des thèmes connexes dont nous présentons l'analyse maintenant.

Cette revue de la littérature aborde, premièrement, quelques facettes d'Internet, soit son développement, ses caractéristiques, les services qu'on y trouve ainsi que les acteurs impliqués dans son développement et sa gestion. Nous examinons ensuite l'impact social d'Internet, puis les usages problématiques qu'on en fait, qu'ils soient criminalisés ou non. Nous terminons par un survol des écrits sur différentes réactions d'acteurs face à ces usages problématiques.

2.1 Internet

Cette revue de littérature ne prétend pas détailler, de façon exhaustive, toutes les facettes d'Internet puisque, malgré son jeune âge, Internet a déjà fait couler beaucoup d'encre. Nous y abordons, sommairement, ce qui caractérise Internet, nous examinons son développement et les usages qu'il est possible d'en faire et, finalement, nous mentionnons quelques acteurs impliqués dans le développement et la gestion d'Internet.

2.1.1 Définition et caractéristiques d'Internet

Définitions

L'Office de la langue française (OLF) définit Internet de la façon suivante :

> Réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole de communication TCP-IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs. (Office de la langue française, Page consultée le 21 octobre 1999)

Le terme « internaute » désigne l'utilisateur du réseau Internet (OLF, Page consultée le 21 octobre 1999).

Caractéristiques d'Internet

Internet est un méta réseau constitué de plusieurs réseaux informatiques. Les ordinateurs qui forment ces réseaux utilisent différents médiums pour communiquer entre eux (Dufour, 1996). Il peut s'agir de lignes téléphoniques, de câbles sous-marins, de fibres optiques ou même, dans certains cas, de liaisons satellites.

Pour que tous ces ordinateurs puissent « dialoguer » entre eux, il ne suffit pas qu'ils soient reliés par une ligne téléphonique ou une fibre optique, encore faut-il que ces appareils, peu importe leurs caractéristiques, puissent parler le même langage. Ce langage est le protocole TCP/IP (Transmission Control Protocol/Internet Protocol) que l'Office de la langue française définit de la façon suivante :

> Ensemble des protocoles de communication utilisés dans Internet, permettant de gérer la circulation des données dans le réseau tout en assurant le bon échange des données entre un point et un autre du réseau. (OLF, Page consultée le 21 octobre 1999)

Le protocole TCP/IP régit donc la transmission des informations sur Internet. Ainsi, lorsqu'un internaute envoie un message électronique à un autre internaute, son ordinateur, par le biais du protocole TCP/IP, découpe son message en plusieurs « paquets » de données[1] avant de les envoyer sur Internet.

Une fois sur Internet, des ordinateurs spécialisés (routeurs IP) envoient ces « paquets » de données vers l'ordinateur auquel ils sont destinés. Chaque paquet est aiguillé sur Internet en fonction de l'état du réseau à ce moment précis. Lorsqu'ils sont tous arrivés à l'ordinateur auquel ils sont destinés, celui-ci reconstitue le message électronique ou le fichier d'origine. (Colombain, 1996).

Il importe de comprendre qu'il est pratiquement impossible de bloquer la route aux paquets de données qui circulent sur Internet. Un paquet qui rencontre un obstacle sur son itinéraire est simplement aiguillé, par un routeur IP, vers une route alternative lui permettant d'atteindre sa destination. Cette caractéristique d'Internet rend le réseau à la fois fiable et difficile à contrôler. Il suffit d'ailleurs d'examiner le contexte dans lequel Internet fut développé pour comprendre que les créateurs d'Internet recherchaient cette caractéristique.

2.1.2 Développement d'Internet

Le Réseau inter-ordinateurs scientifique québécois (RISQ), responsable du maillon québécois d'Internet, associe la naissance d'Internet à la mise en orbite, par l'URSS, du premier satellite humain autour de la Terre en 1957[2] (RISQ, Page consultée le 6 avril

---

[1] Ensemble de données numériques, constituant un message ou une partie de message, et d'éléments numériques de service, comprenant une adresse, organisé selon une disposition déterminée par le procédé de transmission et acheminé comme un tout (OLF, Page consultée le 21 octobre 1999).

[2] Le satellite soviétique Spoutnik

1998). Cette réussite soviétique motive le gouvernement américain à investir dans de nouveaux projets technologiques. Pour ce faire, il crée « l'Advanced Research Project Agency » (ARPA) et lui donne le mandat de doter la Défense américaine d'un système de communication performant et pouvant survivre à un conflit nucléaire. En 1962, deux chercheurs de « l'University of California » à Los Angeles (UCLA), Vinton Cerf et Leonard Kleinrock, s'associent à l'ARPA et proposent le développement de protocoles de communication qui permettent l'échange d'informations entre ordinateurs reliés en réseaux (RISQ, Page consultée le 6 avril 1999).

ARPANet, nom donné au premier réseau, devient opérationnel en 1969 (RISQ, Page consultée le 6 avril 1999). Alors que seulement quatre universités sont reliées en 1969, on en compte vingt-trois dès 1971. La première connexion internationale entre deux ordinateurs est réalisée en 1973 entre « l'University College of London » d'Angleterre et le « Royal Radar Establishment » de Norvège. En 1974, Vinton Cerf et Robert Kahn créent le protocole TCP/IP qui permet l'échange d'informations entre ordinateurs de différents types et, indirectement, le développement d'Internet (Internet Society, Page consultée le 12 juillet 1999).

À la fin des années 70, des centres de recherche universitaires exclus d'ARPANet parce qu'ils ne travaillent pas pour la Défense américaine, créent d'autres réseaux informatiques tels TheoryNet en 1977, BITNet en 1981 (Because It's Time Network) ou CSNet (Computer Science Network, 1981). En 1984, ces réseaux parallèles se joignent à ARPANet, ce qui incite les militaires à fonder leur propre réseau (MILNet) afin de s'y retrouver en privé. ARPANet, qui est alors une véritable courtepointe de réseaux interconnectés, change tranquillement d'appellation pour Internet qui signifie « **Inter**connected **Net**works ».

En 1995, le gouvernement américain décentralise et privatise la gestion d'Internet et remet celle-ci entre les mains des fournisseurs Internet (RISQ, Page consultée le 6 avril

1999). Ceux-ci gèrent maintenant les infrastructures d'Internet et vendent l'accès au réseau à la majorité des internautes.

Malgré l'âge relativement jeune d'Internet, des chercheurs et experts préparent déjà l'Internet de demain. Le 10 octobre 1996, le gouvernement américain annonçait son engagement dans le développement d'un nouvel Internet par le biais de programmes de recherche et de développement mis de l'avant dans certaines de ses agences (Next Generation Internet Initiative, Page consultée le 22 octobre 1999).

Même s'il est difficile d'évaluer la taille d'Internet parce qu'elle varie constamment et que nous manquons de techniques de mesure sophistiquées, nous pouvons baliser sa croissance par les données suivantes. De 4 ordinateurs hôtes[3] en 1969, Internet passa à 617 000 en octobre 1991 puis à 9 472 000 en janvier 1996 et 64 136 417 ordinateurs hôtes en 1999 (Québec Science, 1996; Telcordia Technologies, Page consultée le 14 octobre 1999).

Quant au nombre d'internautes de par le monde, Nua Internet Surveys (Page consultée le 25 octobre 1999), une entreprise spécialisée dans la publication sur Internet, estime qu'ils étaient 55 millions en 1996, en compte actuellement 250 millions et évalue à 350 millions le nombre d'internautes en 2005.

Si les internautes sont si nombreux à naviguer dans cet univers virtuel, c'est en raison des multiples services qu'on y trouve et que nous allons détailler dans les pages qui suivent.

2.1.3 Services disponibles sur Internet

Les services disponibles sur Internet sont nombreux et diversifiés. Ils permettent de communiquer, de s'informer, d'acheter et de vendre des biens et même de rencontrer des

---

[3] Ordinateurs qui diffusent de l'information sur Internet et consultés par les internautes selon leurs besoins (OLF, Page consultée le 21 octobre 1999).

gens. Bien que généralement utilisés dans le cadre d'activités légitimes, il arrive que des internautes utilisent les services d'Internet à mauvais escient. Il s'agit d'ailleurs de la principale facette d'Internet à laquelle les corps policiers consultés tentent de s'adapter. Voici un bref portrait des principaux services disponibles sur Internet.

Le courrier électronique est actuellement le service le plus populaire sur Internet. Il permet l'envoi de messages électroniques[4] textuels, auxquels on peut joindre des fichiers informatiques, dans la boîte aux lettres électronique d'autres internautes. Actuellement, 94% des internautes disent utiliser le courrier électronique et 84% estiment ne plus pouvoir s'en passer (Innovation Ressources, Page consultée le 28 octobre 1999).

Les sites Web sont également très populaires. Le Web est un système basé sur l'utilisation de l'hypertexte[5], qui permet la recherche, l'accès et la visualisation d'informations dans Internet (OLF, Page consultée le 21 octobre 1999). Une information peut prendre la forme d'un texte, d'une image, d'un son ou d'un vidéo-clip (Québec Science, 1996). Ces informations sont présentées sur les millions de sites Web personnels, privés, commerciaux et gouvernementaux. D'autres services semblables au Web (ex. FTP, Gopher), quoique moins populaires, sont également accessibles via Internet. En plus de donner accès à diverses informations, les sites Web permettent également d'acheter des biens neufs et usagés, de réaliser des opérations bancaires, de s'inscrire à une université ou de télécharger[6] un formulaire gouvernemental de déclaration d'impôts en quelques secondes.

Le service de bavardage Internet (« Internet Relay Chat ») permet des conversations interactives en temps réel et l'échange de fichiers informatiques entre internautes du

---

[4] Le terme courriel peut également être employé pour désigner un message électronique (OLF, Page consultée le 21 octobre 1999).

[5] Présentation de l'information qui permet une lecture non linéaire grâce à la présence de liens sémantiques activables dans les documents (OLF, Page consulté le 21 octobre 1999).

[6] Transférer des données ou des programmes stockés dans un ordinateur distant vers un ordinateur local à travers un réseau, ou transférer des données ou des programmes stockés dans un ordinateur central vers un micro-ordinateur (OLF, Page consultée le 21 octobre 1999).

monde entier. On trouve plusieurs milliers de bavardoirs[7] thématiques (« chat rooms ») où les internautes peuvent se rencontrer et échanger. Il existe maintenant des bavardoirs, tel le Palace[8], où les participants sont représentés par un icône et peuvent discuter de vive voix en branchant un microphone à leur ordinateur.

Le réseau Usenet met en contact plus de 30 000 groupes de discussion traitant d'une panoplie de sujets (OLF, Page consultée le 21 octobre 1999). Les internautes peuvent lire les messages affichés dans chacun de ces groupes et y répondre. À la différence du service de bavardage Internet, les échanges sur le réseau Usenet sont en différé ou asynchrones, puisqu'on doit laisser le temps aux internautes de réagir aux messages affichés.

Les internautes peuvent également, à partir de leur ordinateur personnel, recourir au protocole Telnet pour employer des programmes ou consulter des données sur des ordinateurs hôtes. Par exemple, un étudiant peut utiliser le protocole Telnet pour consulter, de la maison, le catalogue d'une bibliothèque universitaire (Québec Science, 1996).

Chaque jour, des millions d'individus, de partout dans le monde, naviguent sur Internet et utilisent les différents services que nous avons énumérés. Ils consultent des sites Web, interrogent des banques de données et discutent entre eux. Ces activités seraient impossibles si la croissance et le développement d'Internet n'étaient pas encadrés par certains acteurs. Nous allons examiner quelques-uns de ces acteurs.

2.1.4 Acteurs impliqués dans le développement et la gestion d'Internet

Comme l'explique le Réseau inter-ordinateurs scientifique québécois (Page consultée le 23 mars 1998), c'est grâce à l'encadrement de certains organismes qu'Internet a survécu à

---

[7] Lieu de rencontre virtuel, accessible à partir d'un site de bavardage, que l'internaute peut choisir, suivant le sujet proposé ou l'intérêt du moment, afin de converser en temps réel et par clavier interposé, avec un nombre relativement restreint de participants. (OLF, Page consultée le 21 octobre 1999)

[8] http://www.thepalace.com

sa formidable croissance et qu'il offre les services que nous avons énumérés. Le RISQ identifie ces principaux acteurs internationaux, canadien et québécois.

Niveau international

L'Internet Society (**ISOC**), dont le siège social est aux Etats-Unis, fut créée en 1992 dans le but de coordonner le développement d'Internet et les technologies et applications d'interconnexion de réseaux qui y sont associées. L'ISOC veille à la préservation du caractère éducatif d'Internet, à sa vocation spécifique de forum d'échange d'idées et s'intéresse également à la sécurité des réseaux.

L'architecture d'Internet repose sur des normes développées par l'Internet Engineering Task Force (IETF). Cette organisation regroupe une multitude d'experts qui s'intéressent à la sécurité des réseaux, à leur gestion et à la circulation des informations sur ceux-ci (IETF, Page consultée le 28 octobre 1999). Certains membres de l'IETF forment l'Internet Engineering Steering Group (IESG).

C'est justement l'IESG qui veille à normaliser, sur le plan mondial, les normes en matière de communication entre ordinateurs. Les travaux de l'IETF sont supervisés par l'Internet Architecture Board (IAB) qui est en quelque sorte le conseil consultatif technique de l'ISOC (RISQ, Page consultée le 23 mars 1998). Tous les réseaux connectés à Internet doivent respecter les normes de l'IAB.

Le Web3 Consortium veille au développement et au respect de la norme WWW dans l'ensemble du Web. Le Web3 Consortium collabore avec le Massachusetts Institute of Technology (MIT) aux USA, le Centre européen de recherche nucléaire (CERN) en Suisse et l'Institut national de recherche en informatique et en automatique (INRIA) en France (World Wide Web consortium, Page consultée le 5 août 1999).

Finalement, l'Electronic Frontier Foundation (EFF) s'intéresse aux effets et changements sociaux qui découlent de l'utilisation des ordinateurs et des réseaux ainsi qu'au respect

des droits d'auteur et à la démocratisation de l'accès aux réseaux. L'EFF fait également des pressions auprès des gouvernements pour qu'ils respectent les libertés civiles des internautes, notamment la liberté d'expression sur Internet (Electronic Frontier Foundation, Page consultée 12 septembre 1999).

Niveau canadien

L'implication du gouvernement canadien face à Internet se fait par l'octroi de fonds qui visent à favoriser le développement de l'autoroute de l'information (RISQ, Page consultée le 23 mars 1999). Les organismes et projets suivants sont liés au développement d'Internet au Canada:

- Réseau canadien pour l'avancement de la recherche, de l'industrie et de l'enseignement ;
- Conseil national de recherches du Canada ;
- Projet CANARIE[9] ;
- Electronic Frontier Canada (EFC).[10]

Depuis 1995, l'implication gouvernementale dans la gestion de l'architecture d'Internet est minimale. L'infrastructure physique du réseau est maintenant entre les mains des fournisseurs Internet (RISQ, Page consultée le 6 avril 1999). L'Association canadienne des fournisseurs Internet (ACFI) regroupe plusieurs fournisseurs et tente de promouvoir les intérêts collectifs des fournisseurs auprès des instances décisionnelles (CAIP, Page consultée le 28 octobre 1999). Les membres de l'ACFI ont un code de conduite auquel ils adhèrent de façon volontaire qui prône le respect des diverses lois canadiennes. L'ACFI collabore également avec les corps policiers canadiens sur une base régulière.

---

[9] CANARIE fut créé en 1993 et collabore depuis avec le gouvernement et les milieux de l'industrie, de la recherche et de l'enseignement afin de renforcer l'infrastructure, les applications, le développement et l'utilisation d'Internet au Canada (CANARIE, Page consultée le 28 octobre 1999).

[10] L'EFC veille au respect des principes énoncés dans la Charte canadienne des droits et des libertés, lors de l'introduction dans la société canadienne des nouvelles technologies de calcul, de communication et d'information (EFC, Page consulté le 17 septembre 1999).

Niveau québécois

Au Québec, le développement d'Internet fut initié par le Secrétariat de l'autoroute de l'information (SAI) fondé en 1995 et rattaché au ministère de la Culture et des Communications. Le SAI élabora et coordonna, avec l'aide de partenaires, la stratégie québécoise de mise en œuvre de l'autoroute de l'information (RISQ, Page consultée le 6 avril 1999). Le SAI a été aboli en février 1998 et la gestion d'Internet au Québec est maintenant entre les mains du ministère de la Culture et des Communications.

On ne peut observer le fonctionnement d'Internet et les multiples services qui s'y trouvent sans se questionner sur l'impact social d'un tel réseau de communication. Qu'en est-il du contrôle des informations qui circulent sur Internet ? La vie privée des internautes et de la population est-elle menacée d'une quelconque façon ? Nous allons nous pencher sur ces questions dans les pages qui suivent.

2.2 Internet comme phénomène social

Les récentes innovations dans le domaine des technologies de l'information, dont la plus importante est sans contredit le développement d'Internet, sont de nature à bouleverser certaines facettes de nos vies. La technologie à la base du développement d'Internet est relativement récente et, selon Johnson (1989 : 44), l'assimilation de chaque nouvelle technologie comporte deux principales étapes.

> The process by which new technologies are assimilated into a society seems to involve at least two fundamental stages. First, there is what might be called a transition period, during which conceptual and moral puzzles arise and there is a need for explication of specific rules, conventions, or laws to tell us how to behave with regard to the new technology. This stage is probably one that we are still in with regard to computer networking. The second stage is the period after we have finally digested the new technology and have developed (formally and/or informally) fairly clear rules of behavior.

Johnson estimait donc, il y a de cela dix ans, que nous étions dans une phase de transition par rapport aux réseaux informatiques, une phase marquée par des dilemmes

moraux, des questionnements quant à la façon d'agir avec ces réseaux et la recherche de lois ou règlements qui encadreraient ces actions.

Un simple coup d'œil aux propos relatifs à Internet dans les médias permet de constater qu'à certains égards nous sommes toujours dans cette phase de transition. Un jour on y acclame le développement d'Internet et le lendemain on énumère les problèmes qui lui sont liés. Nous allons examiner brièvement l'impact d'Internet sur le fossé qui se creuse entre les nations info-riches et info-pauvres ainsi que sur le respect de la vie privée.

2.2.1 Pays info-riches et info-pauvres

Le développement fulgurant des réseaux de communication dont Internet est la figure de proue, annonce un important changement social qui se produit actuellement à l'échelle mondiale : le passage de la société industrielle à la société informationnelle (Toffler cité dans Schwartz, (Page consultée le 14 juillet 1997); Rosnay, 1996). Dans ce nouvel ordre mondial, les pays ne seront plus jugés selon leur capacité à produire massivement et à faible coût des biens matériels mais bien selon leur habilité à gérer, créer et rentabiliser le savoir et l'information. Selon Toffler (1982), l'information sera la principale richesse de la société de demain et l'information, c'est justement ce qui coule dans les veines d'Internet.

Toutefois, les pays de l'hémisphère nord exercent actuellement un monopole sur la circulation de l'information. Sur approximativement 30 millions d'utilisateurs du courrier électronique, seuls quelques milliers se trouvent en Amérique latine et quelques centaines en Afrique (Bissio, 1994). Même si, selon Renaud et Torrès (1995), le taux d'individus ayant accès au réseau progresse maintenant beaucoup plus rapidement dans ces pays du Sud que dans ceux du Nord, il n'en demeure pas moins que les entreprises du Nord semblent actuellement les mieux placées pour influencer la nature de l'information qui circule sur Internet et imposer leurs standards de communication et d'échange de données (Quéau, 1995).

Déjà, la plupart des grandes compagnies dans le domaine de la fabrication d'équipement informatique et de logiciels se trouvent aux États-Unis. Le géant Microsoft, dont les systèmes d'exploitation sont installés sur la plupart des ordinateurs, est un bon exemple de monopole lié aux nouvelles technologies de l'information.

La menace d'une monopolisation dans le monde informatique est donc bien réelle et, comme le dit Nicholas Negroponte (cité dans Carlander, 1996), il faut réagir immédiatement si nous ne voulons pas voir un fossé se creuser entre les pays info-riches et ceux info-pauvres.

On peut d'ailleurs se demander s'il n'y a pas déjà des info-riches et des info-pauvres à l'intérieur même des pays où les nouvelles technologies de l'information sont les plus développées. Bien que cela tende à changer, la quatrième enquête du RISQ (Page consultée le 4 décembre 1999) sur le profil socio-démographique des internautes québécois démontre que l'internaute type est encore un jeune professionnel hautement scolarisé et ayant un revenu supérieur au revenu moyen des Québécois.

L'internaute type est d'ailleurs au cœur d'un débat entourant Internet et le respect de la vie privée dont nous allons parler dans la section qui suit.

2.2.2 Respect de la vie privée

Internet, de par son incroyable potentiel de diffusion, de recherche et de croisement des informations, est maintenant au cœur d'un important débat qui porte sur l'atteinte à la vie privée.

Aux États-Unis, il est maintenant possible d'accéder à de nombreuses banques de renseignements personnels par le biais d'Internet (Eudes, 1997). On peut notamment obtenir des informations sur des registres civils, les enregistrements de véhicules, les citoyens qui ont versé une contribution à un candidat ou encore la liste des prisonniers de certains États. Eudes mentionne que des organisations vont jusqu'à modifier leurs

banques de données afin de vendre les renseignements qu'elles contiennent à des entreprises privées ou les utiliser à d'autres fins. Bien qu'il s'agisse d'un phénomène encore embryonnaire, on assiste même à l'apparition d'agences d'enquête dont les « cyberdétectives » se spécialisent dans la recherche de renseignements personnels sur Internet (Eudes, 1997).

Puisque l'internaute type est un individu hautement scolarisé et ayant un revenu annuel supérieur au revenu moyen de la population, il est, évidemment, une cible intéressante pour les compagnies de marketing. Il existe différentes stratégies pour recueillir des informations sur les caractéristiques des internautes.

Par exemple, pour accéder à certains sites Web, les internautes doivent répondre à des questions qui portent sur leurs caractéristiques et habitudes de vie. Selon une étude du Electronic Privacy Information Center (Page consultée le 4 août 1997), réalisée en juin 1997, 49 des 100 sites les plus fréquentés exigent de telles informations par le biais d'un enregistrement en ligne, de sondages ou d'autres formes de questionnement. Sur ces 100 sites, seul 17 rendent publique leur politique de traitement des informations personnelles. L'Electronic Privacy Information Center estime que plusieurs sites Web vendent des informations à des agences de publicité et à d'autres organisations.

Des outils ont également été développés pour recueillir, cette fois à l'insu des internautes, des informations sur leurs habitudes de navigation. Par exemple, les « cookies[11] » sont de petits fichiers laissés par les serveurs qui hébergent des sites Web dans les ordinateurs des internautes qui les visitent. Ces « cookies » contiennent des informations sur les préférences et les habitudes de navigation des internautes tels que les pages du site Web consultées, le temps passé devant chacune d'elles, les publicités

---

[11] Élément d'information transmis par le serveur au navigateur lorsque l'internaute visite un site Web, et qui peut être récupéré par le serveur lors de visites subséquentes. (OLF, Page consultée le 21 octobre 1999)

explorées, la fréquence des visites, etc. (Cassius de Linval, 1996). À partir de ces informations, il est possible de dresser le profil de consommation des internautes et ainsi de cibler les publicités les plus susceptibles d'intéresser les internautes qui fréquentent ces sites Web. Quoique cela soit parfaitement légal, il peut être vexant, en tant que consommateur, d'être sollicité par des entreprises qui connaissent si bien nos intérêts.

Toutes les informations obtenues à notre sujet lors de nos escapades sur le Net, à l'aide du relevé de nos achats à crédit ou encore par le biais de banques de données accessibles via Internet, ne représentent que l'ombre de notre personnalité. Pourtant, comme le souligne Martine Gingras (1996) ces informations sont parfois utilisées pour créer notre profil de consommateur et celui-ci est à son tour utilisé par certaines institutions pour prendre d'importantes décisions sur notre compte. Les questions suivantes méritent alors d'être soulevées. Qu'advient-il si, par mégarde, des informations erronées sont utilisées pour constituer notre double numérique? Risquons-nous de perdre un emploi ou une promotion, de nous voir refuser une police d'assurance ? Mais surtout, apprendrons-nous l'existence de ces mauvaises informations et pourrons-nous corriger rapidement la situation ? Toutes ces questions et plusieurs autres demeurent toujours sans réponse.

De l'avis de certains, Internet menace également la vie privée des gens au travail. Cela est dû au fait que l'accessibilité à Internet dans le milieu de travail entraîne une baisse de la productivité des employés. Ceux-ci ne peuvent s'empêcher de naviguer sur Internet pendant leurs heures de travail, ce qui fait perdre de l'argent aux employeurs. En réponse au cri d'alarme des entreprises, la compagnie américaine SilverStone Sofware Corp a lancé le logiciel com.Policy. Ce logiciel permet à un gestionnaire de visionner, à partir de son ordinateur, le contenu de l'écran de n'importe lequel de ses employés qui navigue sur Internet et ainsi identifier ceux qui perdent inutilement leur temps. On peut également enregistrer le temps passé sur chacun des sites Web, l'historique des sites visités, et même bloquer l'accès aux sites qui ne sont pas utiles à l'entreprise (SilverStone Software Corp., Page consultée le 5 décembre 1999). L'utilisation d'un tel

logiciel vient alimenter le débat entourant la protection de la vie privée dans le monde du travail. Selon l'hebdomadaire Voir (Page consultée le 9 décembre 1997 : 21), les États-Unis assisteraient à l'apparition de mouvements universitaires de défense de la vie privée des employés.

> Déjà, le débat entre entreprises et universitaires s'engage. Les premiers croyant avoir l'outil nécessaire pour autodiscipliner leurs employés; les seconds, considérant cette approche comme une intrusion immorale dans la vie privée, d'inspiration orwellienne. Big Brother is watching you ! qu'ils disaient. Et c'est lui qui signe votre chèque de paye.

Mais si la population et les internautes ont des motifs de s'inquiéter, ils en ont aussi de se réjouir. En plus de permettre un accès rapide à de nombreuses sources d'information, Internet donne également le pouvoir à chaque internaute de diffuser à son tour des informations qui seront accessibles de n'importe quel ordinateur branché à Internet. Il est probable que ce pouvoir dont disposent les internautes entraînera des changements sociaux et politiques majeurs dans de nombreux pays.

Prenons l'exemple des sympathisants du mouvement zapatiste au Mexique. En 1994, le combat du sous-commandant Marcos et de ses guérilleros zapatistes contre les autorités fédérales mexicaines est soudainement détaillé sur des sites Web d'étudiants universitaires mexicains et américains. La légende des guérilleros « high tech » est née. Les guérilleros zapatistes disposent maintenant d'une formidable tribune mondiale pour informer le monde entier de l'évolution du conflit et de leur version des faits (Planète Internet, Page consultée le 2 juillet 1997).

Internet peut donc être utilisé par des individus ou des groupes qui cherchent à exprimer leurs opinions, fausses ou véridiques, à travers le monde entier. Par exemple, Internet peut être utilisé par la population d'un pays pour dénoncer l'oppression qu'exerce le gouvernement ou, par ce même gouvernement, pour camoufler cette oppression en projetant, dans le monde entier, l'image d'un pays paisible et stable politiquement.

Il ne fait aucun doute que le développement d'Internet a un impact social important et qu'il risque d'agrandir le fossé entre les pays info-riches et info-pauvres puisqu'à l'heure actuelle ce sont encore les pays du Nord qui maîtrisent le mieux l'information qui circule sur Internet. Alors que de plus en plus de familles des pays développés ont accès à Internet à la maison, plus de deux milliards de personnes n'ont pas encore accès à l'électricité (Ramonet. 1996)

La problématique du respect de la vie privée retient également l'attention. Les internautes représentent une clientèle alléchante pour les entreprises et celles-ci tentent par tous les moyens de s'approprier des informations sur ces clients potentiels. Personne ne peut s'assurer qu'elles font un bon usage de ces informations. La prochaine section de cette revue de littérature porte sur un autre problème social associé à Internet et qui fait les manchettes : les usages problématiques d'Internet.

2.3 Usages problématiques d'Internet

Nous l'avons constaté précédemment, plusieurs services sont disponibles sur Internet. Bien que la plupart des internautes utilisent ces services à bon escient, certains les utilisent de façon problématique. L'intervention envers ces usages problématiques fait partie intégrante du processus d'organisation des corps policiers par rapport à Internet.

Nous distinguons deux principaux groupes d'usages problématiques. Les usages problématiques non-criminalisés et les usages criminalisables. Parmi les seconds, certains mènent à la perpétration de crimes « conventionnels » et d'autres à celle de crimes « innovateurs ».

2.3.1 Usages problématiques non-criminalisés

Internet est un moyen de communication et de diffusion de l'information très efficace puisqu'il est rapide, difficilement contrôlable et relativement anonyme. La plupart des usages problématiques d'Internet sont liés à ces caractéristiques. Parmi ceux-ci, on trouve la diffusion d'informations pouvant être utilisées à des fins criminelles, une

surabondance de matériel pornographique, ainsi que l'échange d'informations entre criminels qui s'adonnent à des activités illicites similaires (pédophilie, trafic de stupéfiants, etc.).

Il y a sur Internet des contenus qui, selon certains, ne doivent pas être accessibles si aisément (Grabosky, Smith, Wright, 1998). Par exemple, des sites Web expliquent comment fabriquer des explosifs à partir de produits ménagers. (Sterling, 1992; Sussman, 1995). D'autres, révèlent comment accéder frauduleusement à des banques de données ou comment cultiver de la marijuana (Duncan, 1997). Comme le souligne Eudes (1997), l'arrivée d'Internet vient faciliter l'accès à ce genre d'informations :

> Auparavant, la confidentialité des informations était protégée *de facto* par l'éparpillement géographique des fichiers, la fragmentation des informations entre administrations et la lourdeur des démarches pour les consulter. Désormais tout est accessible de n'importe où. Internet abolit les distances et les cloisonnements, et permet les croisements, compilations et duplications à l'infini (Eudes 1997 : B4).

Internet regorge de sites Web qui vendent du matériel pornographique (Duncan, 1997, Sussman, 1995a, Sussman, 1995b, Francescon, 1996). Certains dénoncent l'exposition des jeunes internautes à ce matériel pornographique et s'interrogent quant à l'impact que cela peut avoir sur leur perception de la femme et de la sexualité.

Certes, il existe des logiciels qui permettent de bloquer l'accès aux sites Web à caractère pornographique (Net Nanny, Cyber Patrol, CYBERsitter, etc.), mais les policiers rencontrés nous révèlent deux facteurs qui compliquent leur utilisation. D'une part, tous les parents ne possèdent pas les connaissances nécessaires pour installer adéquatement ces logiciels. D'autre part, certains enfants, à l'inverse de leurs parents, possèdent suffisamment de connaissances en informatique pour désinstaller ces logiciels de contrôle.

Les pédophiles utilisent Internet, et plus spécifiquement le service de bavardage Internet, pour identifier et contacter des victimes potentielles (Le Devoir, 1996; Cassius de Linval, 1996; Francescon, 1996; Denning, 1995; Forde & Patterson, 1998). L'utilisation d'Internet permet au pédophile de demeurer anonyme et d'agir à partir de son domicile plutôt que de fréquenter les lieux publics à la recherche d'enfants. Il est donc plus difficile pour les policiers de l'identifier puisque personne ne peut donner son signalement.

Une étude de l'Australian Institute of Criminology[12] révèle que les pédophiles utilisent également Internet pour se regrouper en réseaux informels, échanger du matériel pornographique et communiquer entre eux (Forde, Patrick, Patterson, Andrew, 1998). De plus, cette étude nous apprend que la plupart des pédophiles qui naviguent sur Internet le font de façon anonyme. Ceux-ci s'échangent d'ailleurs des informations et des conseils sur les différentes façons de cacher leur identité.

Des trafiquants de drogue ont recours au courrier électronique ainsi qu'à l'encodage pour communiquer avec leurs clients ou avec leur(s) fournisseur(s) de drogues (Duncan, 1997; Francescon, 1996). Pour ces criminels, il est moins risqué de communiquer via Internet que d'utiliser le téléphone qui peut être mis beaucoup plus aisément sous écoute électronique.

Des internautes utilisent le service de courriel anonyme, qui permet d'expédier du courrier électronique sans dévoiler leur identité, pour envoyer des menaces, pour harceler ou pour tenir des propos diffamatoires tout en demeurant anonymes (Denning, 1995). D'autres s'abonnent simplement à un service de courrier électronique gratuit comme Hotmail[13] en donnant de fausses informations personnelles et utilisent ensuite cette adresse pour envoyer leurs messages problématiques. Dans les deux cas, l'identification des auteurs des messages s'avère difficile pour les corps policiers.

---

[12] http://www.aic.gov.au/
[13] Site Web : http://www.hotmail.com

2.3.2 Usages problématiques criminalisés

Les criminels savent profiter des innovations technologiques (GRC, Page consultée le 28 octobre 1999). Ceux-ci comprirent rapidement que les nouvelles technologies de l'information, et particulièrement Internet, permettent la réalisation de nombreux crimes (Hannaford, 1995). En effet, plusieurs actes criminels sont maintenant perpétrés sur Internet (Duncan, 1997; Grabosky, Smith, Wright, 1998) et comme l'explique Francescon (1996) cela est en partie lié aux avantages qu'Internet offre aux criminels :

> En l'état actuel des choses, le monde des nouvelles techniques d'information et de communication est un lieu dans lequel le crime paie, car les risques pour le criminel sont très faibles, les gains souvent très élevés et rapide à obtenir, sans qu'une organisation de taille soit nécessaire (Francescon, 1996 : 65).

De plus, la popularité sans cesse grandissante d'Internet, qui se traduit par une plus grande affluence des internautes et des entreprises sur le réseau, entraîne une inflation du nombre d'opportunités délinquantes qui impliquent l'informatique (Rosé, 1992).

Définition d'un crime réalisé sur Internet

Un crime perpétré sur Internet implique automatiquement et au minimum un système informatisé quelconque. C'est pourquoi il ne s'agit pas d'un crime en matière de télécommunication, mais bien d'un crime informatique. Il existe différentes définitions du crime informatique. Pour notre part, nous utilisons la définition employée par la Gendarmerie royale du Canada :

> Par crime informatique, on entend tout acte illégal au cours duquel le système informatique devient l'objet d'un crime ou en est l'instrument et contient des éléments de preuves. (GRC, Page consultée le 28 octobre 1999).

Crimes conventionnels

On peut croire à tort que les actes illicites commis sur Internet sont tous de nouveaux crimes, alors qu'il s'agit souvent de versions « électroniques » de crimes perpétrés au

Canada depuis de nombreuses années (Duncan, 1997; Piragoff et Holthius, Page consultée le 29 septembre 1999). Cependant, les organisations policières, habituées à lutter contre ces crimes dans nos rues, doivent maintenant s'adapter à leur déplacement sur Internet. Voici quelques crimes conventionnels que l'on retrouve aujourd'hui sur Internet.

Le développement d'Internet a grandement facilité la circulation et la diffusion de la pornographie juvénile (Francescon, 1996). Certains bavardoirs et groupes de discussion sont clairement identifiés comme des lieux d'échange de pornographie juvénile. On trouve également des sites Web plus discrets qui se spécialisent dans les textes à caractère pédophile (Forde & Patterson, 1998). Les pédophiles sont probablement ceux qui profitent le plus de cette situation puisque l'approvisionnement en pornographie juvénile sur Internet est pour eux moins risqué et onéreux que l'achat de ce matériel par la poste (Duncan, 1997). De leur côté, les corps policiers constatent que les techniques d'enquêtes traditionnelles sont inefficaces sur Internet.

Internet est également utilisé comme tribune pour diffuser des propos haineux (Québec Science, 1996; Sussman, 1995; Duncan, 1997; Francescon, 1996). À cet effet, Fitzpatrick (cité dans Sussman, 1995) mentionne le cas de Ernst Zundel qui diffuse de la propagande haineuse à caractère antisémite à partir d'un site Web[14] situé en Californie, là où une telle activité n'est pas illégale (Duncan, 1997). Comme le souligne Francescon (1996: 64), Internet offre de nombreux avantages aux individus qui désirent diffuser de tels propos :

- on ne peut contrôler systématiquement les informations qui circulent sur Internet ;
- l'utilisation de techniques de codage complique l'interception des communications ;
- le milieu de l'information éprouve une certaine réticence à s'engager dans la lutte contre ce fléau ;

[14] http://www.lebensraum.org/index.html

- les frontières et la souveraineté des États ne conditionnent pas les échanges sur Internet ce qui leur donne un caractère presque toujours international ;

- l'immatérialité de l'information, sa mobilité et le peu de moyens nécessaires à la création, à la diffusion et à la recherche de celle-ci font qu'il est difficile de repérer la circulation d'informations problématiques.

Le jeu sur Internet est une industrie très lucrative dont on estime les profits annuels en l'an 2000 à 10 milliards de dollars américains et ce, même s'il est illégal dans plusieurs pays, provinces ou États (Griffin, 1998; Francescon, 1996). La plupart du temps, ces pays ne disposent d'aucun recours puisque les ordinateurs sur lesquels se trouvent ces casinos sont situés dans des pays où le jeu sur Internet est légal (Duncan, 1997). De plus, plusieurs spécialistes américains estiment qu'il est important d'agir face au jeu sur Internet avant que le crime organisé, très impliqué dans le secteur du jeu, ne s'empare de ce nouveau marché lucratif.

La divulgation d'informations confidentielles tels que des numéros de carte de crédit, mot de passe de tous genres ou des informations corporatives privées, dans le cyberespace, constitue également un crime.

On peut aisément créer un site Web où l'on dépeint une personne comme étant un sympathisant néo-nazi et ainsi porter atteinte à sa réputation. Il s'agit alors de libelle diffamatoire tel que stipulé à l'article 298 du Code criminel canadien (Denning, 1995; Barret, 1996).

Le commerce sur le Net est voué à un important développement dans les années à venir (CRIM, Page consultée le 4 mai 1998) mais, en attendant, la prudence est de mise lorsque l'on se procure des biens par le biais du cyberespace puisqu'il est possible d'être victime de fraude. Certains internautes participent également à des ventes pyramidales et ne revoient jamais la couleur de leur argent (Duncan, 1997).

Les institutions financières transfèrent quotidiennement d'importantes sommes d'argent via les réseaux informatiques. Les États-Unis craignent que la réserve fédérale, qui transfert jusqu'à 600 millions de dollars par jour par le biais de lignes téléphoniques, soit attaquée par des hackers (Sussman, 1995). La création de banques virtuelles et la réalisation de transactions bancaires via Internet, facilitent grandement le blanchiment d'argent par le crime organisé (Grabosky, Smith, Wright, 1998; Duncan, 1997).

Le vol de la propriété intellectuelle est également une réalité dans le cyberespace. On peut maintenant faire des copies de logiciels rapidement et aisément et leur distribution via Internet ne demande que des connaissances minimales. Des logiciels copiés sont distribués via des babillards électroniques et des numéros de série y sont également distribués afin de permettre l'enregistrement illégal de ces logiciels (Grabosky, Smith, Wright, 1998; Denning, 1995). La « Software & Information Industry Association » (Page consultée le 4 décembre 1999) estime à 11 milliards de dollars américains les pertes liées au piratage de logiciels pour l'année 1998. Mentionnons qu'il existe également d'autres formes de vol de propriété intellectuelle, notamment pour les textes, les images, les vidéos, la musique (MP3) et les logos.

Crimes innovateurs

Le développement d'Internet ne fait pas qu'ouvrir de nouveaux horizons aux fraudeurs, trafiquants de drogues et pédophiles, il rend également possible la réalisation de quelques crimes autrefois inexistants. Nous allons examiner quelques-uns de ces crimes innovateurs.

L'utilisation non autorisée d'un ordinateur, qui consiste à pénétrer illégalement dans un système informatique, est un de ces crimes (GRC, Page consultée le 28 octobre 1999). Les stratégies pour y parvenir sont nombreuses. Certains pirates informatiques fourbes utilisent la ruse pour amener un utilisateur du système attaqué à dévoiler des

informations qui permettront d'y pénétrer.[15] D'autres ont recours à des logiciels qui interceptent et enregistrent les mots de passe des usagers du système attaqué et utilisent ensuite ces mots de passe pour se brancher au système (Barret, 1996). L'accès à des systèmes informatiques ou leur utilisation sans autorisation sont interdits par l'article 342.1 du Code criminel canadien.

L'altération, la destruction et l'interférence dans l'utilisation de données, sans autorisation, sont également des actes criminels propres à Internet (Piragoff et Holthius, Page consultée le 29 septembre 1999). Ce sont spécifiquement des comportements comme l'implantation de virus ou de bombes logiques et l'utilisation de chevaux de Troie qui sont visés par cet article 430 du Code criminel. Les articles 342.1 et 430 furent modifiés approximativement en 1995 afin de rendre ces actes criminels.

L'examen des divers crimes conventionnels et innovateurs réalisés sur Internet soulève un problème auquel sont confrontés les corps policiers dans leur processus d'organisation par rapport à Internet : celui de la diversité des incriminations dans le monde. Bien que ce problème ne soit pas propre uniquement aux crimes réalisés sur Internet, il est amplifié lorsqu'il est question de ceux-ci. Comment déterminer les lois criminelles qui ont préséance face à un geste posé sur Internet lorsque les pays concernés ont des lois différentes ? À cet égard, Internet risque de forcer les États, qui désirent contrôler certaines activités unanimement considérées comme problématiques, à uniformiser leurs lois criminelles.

Nous l'avons constaté, les nombreux services disponibles sur Internet peuvent être utilisés de façon problématique et même de façon criminelle. Internet permet aux criminels de perpétrer des crimes conventionnels de façon plus efficace et en courant moins de risques et de plus, il permet la réalisation de nouveaux crimes impossibles auparavant tels l'utilisation non-autorisée d'un ordinateur et les méfaits aux données.

---

[15] Le terme anglais « social engineering » est fréquemment utilisé pour décrire cette stratégie des délinquants informatiques.

Nous terminons cette revue de littérature par l'examen des réactions de divers acteurs face à ces usages problématiques d'Internet.

2.4 Réactions face aux usages problématiques d'Internet

Les réactions face à l'apparition et à la prolifération des usages problématiques d'Internet sont nombreuses. Du côté des internautes, celles-ci sont partagées. Certains sont en faveur de l'intervention de l'État tandis que d'autres sont offensés à l'idée d'une telle intervention, et souhaitent que l'on laisse le cyberespace s'auto-contrôler.

Quant au gouvernement canadien, il hésite à légiférer face aux usages problématiques d'Internet, mais il se doit également de réagir face à certains comportements que la population juge inacceptables. Coincés entre l'arbre et l'écorce, les corps policiers canadiens et québécois tentent à la fois de répondre aux plaintes formulées face à ces usages problématiques, tout en respectant les droits des internautes et en intervenant de façon minimale dans la gestion d'Internet.

Nous allons examiner, à tour de rôle, la réaction des corps policiers canadiens et québécois, celle des internautes, des acteurs du secteur privé et celle du gouvernement face à ces usages problématiques d'Internet.

2.4.1 Réaction des corps policiers canadiens et québécois

La Gendarmerie royale du Canada (GRC), la Sûreté du Québec (SQ) et le Service de police de la Communauté urbaine de Montréal (SPCUM), en réponse à l'apparition des usages problématiques d'Internet, ont adopté diverses stratégies.

La GRC, par le biais de ses unités spécialisées en criminalité informatique et de sa Sous-Direction de la sécurité technique (S-DST), occupe l'avant-scène canadienne. Le mandat de la S-DST est d'offrir au gouvernement fédéral une gamme de services au niveau de la sécurité des technologies de l'information (TI) ainsi que de fournir aux forces policières

des services de haute technologie judiciaire (Sous-Direction de la sécurité technique, Page consultée le 4 décembre 1999). La S-DSTI est composée de différentes unités : les Sections de consultation en matière de sécurité matérielle sont chargées de résoudre les divers problèmes de sécurité matérielle qui peuvent survenir dans un milieu de travail. On trouve également les Sections de la sécurité des technologies de l'information et la Section des interventions qui conseillent les institutions fédérales sur des questions de sécurité relatives aux systèmes informatiques appartenant à l'État ou exploités pour le compte de l'État. La Section de la haute technologie judiciaire est impliquée dans la répression des crimes liés aux ordinateurs et aux mémoires à microprocesseurs. Et, finalement, la Section des moyens antitechniques dont les membres ont pour responsabilité première d'exécuter les inspections techniques (balayages) pour le gouvernement fédéral et certaines administrations provinciales et municipales, en plus de fournir de l'aide sous ce rapport à d'autres services de police (Sous-Direction de la Sécurité Technique, Page consultée le 4 décembre 1999).

Au Québec, la Sûreté du Québec dispose également d'unités spécialisées en criminalité informatique ainsi que d'un site Web où l'on affiche des informations sur l'organisation et où les citoyens peuvent laisser des informations sur des activités illicites dont ils désirent informer la SQ (SQ, Page consultée le 9 décembre 1999). Toutefois, ce site n'est pas réservé exclusivement à la lutte contre la criminalité sur Internet. Il s'agit plutôt d'un site où l'on présente l'image corporative de la Sûreté du Québec.

Finalement, la section des crimes informatiques du SPCUM est également présente dans ce champ d'activités ainsi que sur le Web (SPCUM, Page consultée le 9 décembre 1999). Le site Web du SPCUM, tout comme celui de la SQ, contient des informations corporatives (structure de l'organisation, liste des unités spécialisées, etc.) et peut être utilisé pour rejoindre les policiers de la section des crimes informatiques.

2.4.2 Stratégies adoptées par les corps policiers

La stratégie la plus commune et offrant le meilleur rapport résultats/efforts est sans aucun doute la diffusion d'informations. Par le biais de leur site Web, les organisations policières peuvent recevoir les plaintes des internautes et les informer des activités problématiques réalisées sur le réseau. Pour le moment, seule la GRC affiche ce genre d'informations sur son site. Les autres corps policiers utilisent plutôt leur site Web pour afficher différentes informations corporatives.

La Gendarmerie royale du Canada, la Sûreté du Québec ainsi que le Service de police de la Communauté urbaine de Montréal tentent, bien sûr, de dissuader les délinquants informatiques par le biais d'actions en justice contre ceux qui sont identifiés. Ces poursuites judiciaires sont habituellement médiatisées de façon à ce que les délinquants qui courent toujours sachent que le cyberespace n'est pas une terre sans loi.

Francescon (1996) croit que deux facteurs expliquent le peu d'intérêt que manifestent actuellement les organisations policières envers la criminalité sur Internet. Les crimes informatiques ne laissent pas de sillage de violence derrière eux et n'attirent généralement pas l'attention de l'appareil judiciaire puisqu'ils n'émeuvent pas l'opinion publique.

2.4.3 Chez les internautes et les acteurs du secteur privé

Suite à l'apparition d'usages problématiques du cyberespace, certains internautes ont adopté une attitude plus prudente dans leurs activités sur Internet. Ils évitent de divulguer des informations personnelles sur le réseau. Ils sont également plus prudents avec les gens qu'ils rencontrent sur Internet et ne téléchargent pas de fichier informatique sans d'abord détecter la présence de virus.

Quant aux jeunes internautes, certains programmes peuvent les empêcher de s'aventurer sur des sites au contenu problématique. Ces logiciels, une fois installés sur un ordinateur, bloquent l'accès à de nombreux sites. On peut penser à la pornographie, à la

propagande haineuse, etc. Il existe plusieurs logiciels de ce type et les plus populaires sont : Net Nanny, Net Cop, Cyber Patrol, SurfControl, SurfWatch, etc. (Cassius de Linval, 1996; Cloutier, 1997). Malheureusement, comme le souligne Cloutier (1997), ces logiciels ne font pas toutes les distinctions qui s'imposent lorsque vient le moment de trier les sites problématiques de ceux qui ne le sont pas. Prenons le cas de Cybersitter : il peut aisément, à l'aide des mots-clés contenus dans sa base de données, interdire l'accès à plusieurs sites problématiques. Par contre, les critères utilisés pour classer les sites font en sorte qu'il bloque également l'accès au site Web du « National Organisation of Women » ainsi qu'au site de la communauté virtuelle The Well qui sont sans danger.

Les internautes qui craignent que leurs données ne tombent entre les mains de pirates informatiques peuvent encoder leur courrier électronique (Garfinkel, 1997; Linval, 1996). Le logiciel Pretty Good Privacy (PGP), distribué gratuitement sur Internet, peut rendre un message textuel indéchiffrable pour qui ne possède pas la clé de décodage correspondant à celle utilisée par l'expéditeur. Philip Zimmermann, l'inventeur de PGP a même lancé dernièrement PGPhone qui permet d'encoder les conversations de vive voix diffusées par le biais d'Internet à l'aide d'un microphone. Comme nous l'avons mentionné plus tôt, l'utilisation de l'encodage représente une arme à double tranchant, puisque les forces de l'ordre ne peuvent pas, pour le moment, décoder les conversions et messages que les délinquants encodent. Un important débat fait d'ailleurs rage aux États-Unis à ce propos. Les agences gouvernementales américaines souhaitent qu'il n'existe qu'une seule norme de codage. Ces agences aimeraient également posséder une copie de la clé de codage utilisée par les citoyens. Elles pourraient ainsi décoder toutes les informations échangées, moyennant l'obtention d'un mandat auprès d'un juge, un peu comme en matière d'écoute électronique pour les conversations téléphoniques.

Certains fournisseurs Internet ont également adopté des politiques ou lignes de conduite sur lesquelles ils se basent pour déterminer quels forums de discussion ne sont pas

tolérables. Ces fournisseurs coupent habituellement l'accès aux forums qui ne respectent pas ces lignes de conduite.

Malheureusement, ces lignes de conduite n'étant pas standardisées, elles diffèrent donc d'un fournisseur d'accès à un autre et un forum de discussion retiré d'un serveur peut tout de même être disponible et accessible chez un compétiteur.

Sur le plan légal, Francescon (1996) propose plusieurs solutions dont l'adoption d'un modèle de double responsabilité semblable à celui des États-Unis : celle de l'auteur de l'acte criminel et, concurremment, celle des responsables du réseau qui permettent, de manière intentionnelle ou même par négligence coupable, son utilisation à des fins illicites. Francescon suggère également l'adoption d'accords multilatéraux entre divers pays comme c'est le cas dans le domaine du blanchiment d'argent ou du trafic de stupéfiants. Pensons à la déclaration politique des Nations Unies sur le contrôle global des drogues à laquelle ont adhérés plusieurs pays (Nations Unies, Page consultée le 13 décembre 1999).

2.4.4 Au niveau gouvernemental

Plusieurs gouvernements sont tentés par l'idée de légiférer et de réglementer l'industrie des nouvelles technologies de l'information. Il s'agit toutefois d'une entreprises délicate comme l'a constaté le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC).

En juillet 1998, le CRTC, qui a pour mandat d'autoriser, réglementer et surveiller les entreprises canadiennes de radiodiffusion et de télécommunications tout en servant l'intérêt public, annonçait une vaste consultation publique visant à déterminer si l'organisme devait intégrer à son mandat les nouveaux médias comme Internet. Le 17 mai 1999, le CRTC expliqua qu'il ne réglementerait pas Internet au Canada, de peur de

désavantager cette industrie sur le plan de la concurrence qui s'exerce à l'échelle mondiale (CRTC, Page consultée le 9 décembre 1999).

Francescon (1996), suggère l'élaboration de normes juridiques réellement adaptées aux spécificités des nouvelles techniques d'information et de communication et la création d'organes de contrôle, de renseignement et de poursuite pénale spécialisés. Ces initiatives ne doivent pas être prises uniquement à l'échelle locale ou nationale, mais bien à l'échelle internationale puisque l'on parle d'une problématique qui dépasse les frontières. Il croit de plus qu'un organe spécialisé doit faire appel à des spécialistes dotés des moyens nécessaires. Il doit s'agir de structures spécialisées qui s'occupent des activités préventives et répressives. Toutes ces structures doivent absolument collaborer entre elles sur le plan international tant de façon bilatérale que multilatérale et, si possible, sans devoir recourir à l'appareil politique. Cette proposition coïncide avec les propos de nombreux interviewés qui déplorent la lenteur des voies administratives traditionnelles.

Plusieurs législations touchent déjà Internet de façon directe ou indirecte. Nous nous intéressons davantage aux questions législatives relatives aux comportements problématiques réalisés sur Internet. Un acte illégal dans la vie de tous les jours sera également illégal s'il est réalisé sur Internet. Une fraude commise sur Internet, tout comme une fraude commise dans un commerce ou une institution, peut être traitée selon la loi pénale sur la fraude. Même chose pour des crimes tels que le vol, la vente et la possession de matériel pornographique illégal, la diffamation, etc. (Piragoff, 96).

Quant aux actes problématiques possibles grâce à l'avènement d'Internet, certains articles du Code criminel s'adressent spécifiquement à ceux-ci (Piragoff, 1996).
L'article 430 (1.1) du Code criminel ; méfait contre des données, permet de protéger ces dernières contre toute forme d'altération résultant de l'utilisation de moyens comme les virus, chevaux de Troie, le sabotage, etc. D'autres articles furent également ajoutés au

---

[16] http://www.crtc.gc.ca/

Code criminel pour contrer l'accès à des systèmes informatiques ou leur utilisation sans autorisation. Cet article incrimine le fait de frauduleusement et sans apparence de droit:

a) directement ou indirectement, obtenir des services d'ordinateur ;
b) directement ou indirectement, utiliser ou faire utiliser un ordinateur dans l'intention d'obtenir des services d'ordinateur, d'intercepter toute fonction d'un ordinateur (y compris les fonctions de communication) ou de causer un méfait concernant des données.

Les articles qui suivent protègent également les gens de certains méfaits :

- l'accès à des systèmes informatiques ou leur utilisation sans autorisation (alinéas 342.1 (1)a) & c) du Code criminel) ;
- l'interception de communications par ordinateur sans autorisation (alinéa 342.1 (1)b) du Code criminel) ;
- l'appropriation illicite d'informations (article 342.1 du Code criminel) ;
- la fraude en matière de télécommunications (paragraphe 326 (1) du Code criminel).

Des modifications furent également apportées à la Loi sur la preuve au Canada afin de permettre aux policiers de présenter les fichiers informatiques devant les tribunaux plutôt que les ordinateurs qui les contiennent. Cela évite de mettre en péril les activités d'une entreprise en saisissant ses équipements suite aux activités criminelles de l'un de ses employés.

2.5 Conclusion

La lecture d'ouvrages spécialisés en criminalité informatique, tout comme celle des journaux révèle que, même si la plupart des internautes utilisent Internet de façon tout à fait légale, certains en font un usage problématique et parfois même criminel. Cela s'explique principalement par les nombreux avantages qu'offre Internet aux individus qui désirent poser un geste problématique. Par exemple, Internet permet à ceux-ci de demeurer relativement anonyme et leur offre un grand bassin de victimes et de complices potentiels.

Face aux usages criminels d'Internet, la littérature nous apprend que, même si certains de ces crimes sont très innovateurs et que leur réalisation n'est possible que par le biais d'un réseau informatique tel qu'Internet, la majorité d'entre eux ne sont cependant que des versions électroniques de crimes conventionnels.

La littérature nous documente également sur le fait que l'apparition des crimes commis via Internet, qu'ils soient innovateurs ou conventionnels, n'en est pas moins problématique et qu'elle entraîne une réaction sociale, politique et pénale de plus en plus forte en Amérique du Nord. Parmi les formes que prend cette réaction, on compte l'apparition d'un processus d'organisation chez certains corps policiers par rapport à Internet.

Problématique et méthodologie

3. Problématique et méthodologie

À la lecture de la revue de littérature, on constate que de nombreux ouvrages, tantôt scientifiques, tantôt journalistiques, traitent des usages problématiques des nouvelles technologies de l'information et plus particulièrement d'Internet. Cependant, on remarque également qu'aucune recherche criminologique, canadienne ou québécoise, ne s'est encore intéressée au processus d'organisation des corps policiers par rapport à Internet.

Ceux-ci font face à deux défis de taille relatifs à Internet. D'une part, les corps policiers doivent apprendre à tirer profit des possibilités qu'offrent les nouvelles technologies de l'information et plus particulièrement Internet, par exemple, en se dotant d'un site Web corporatif par le biais duquel les internautes peuvent obtenir des informations générales sur l'organisation et communiquer avec elle. D'autre part, et c'est peut-être là où se trouve le plus grand défi, les corps policiers doivent s'organiser de façon à réagir efficacement à l'apparition et à la prolifération des usages problématiques d'Internet.

La démarche de recherche à la base de ce mémoire repose précisément sur l'analyse de ce processus d'organisation des corps policiers par rapport à Internet. Suivant le conseil de Quivy et Campenhoudt (1988), nous avons débuté cette démarche en formulant une question de départ qui exprimait bien notre projet de recherche : « *Quel est le processus d'organisation des corps policiers, canadiens et québécois, par rapport à Internet ?* »

Nous avons utilisé cette question de départ en gardant en tête deux objectifs de recherche spécifiques poursuivis dans le cadre de ce mémoire. Ceux-ci portent sur des facettes distinctes du processus d'organisation des corps policiers, canadiens et québécois, par rapport à Internet.

Premier objectif : l'étude du processus d'organisation des corps policiers canadiens et québécois par rapport à Internet.

Nous voulons explorer comment les services policiers canadiens et québécois s'organisent par rapport à Internet. Plus particulièrement, comment la police utilise-t-elle Internet ? Comment, depuis quand et pourquoi Internet influence-t-il la police ? Quelles ressources ces corps policiers allouent-ils à leur organisation par rapport à Internet ? Quelles structures ont été et seront mises en place par rapport à Internet ? Quel est le mandat de la police par rapport à Internet ? Quelles sont ses politiques ? Comment sont sélectionnés les dossiers où l'on intervient ? Quels sont les projets futurs par rapport à Internet ? Qu'en est-il des relations intra et extra-organisationnelles ? Comment sont sélectionnés et formés les policiers qui sont en contact avec Internet et quel statut ont-ils au sein de l'organisation ? Existe-t-il des statistiques ou des données sur le travail de l'organisation face à Internet ? Quelle place occupe la réactivité et la pro-activité lorsqu'on parle d'Internet ? Quels sont les usages que l'organisation définit comme problématiques ? Quels sont les points de vue des gens qui supervisent l'action policière par rapport à Internet ?

Deuxième objectif : l'examen des expériences, points de vue et pratiques des policiers qui sont au cœur de ce processus.

Nous voulons savoir s'il existe un rapport entre l'opinion qu'ont ces policiers d'Internet en général et leurs expériences, points de vue et pratiques. C'est la raison pour laquelle nous souhaitons d'abord explorer leur point de vue sur Internet, en particulier ce qu'ils pensent d'Internet ? Comment pensent-ils qu'Internet influencera la police dans le futur ? Quelle utilisation personnelle et professionnelle font-ils d'Internet ?

Ensuite, nous examinons leurs expériences, points de vue et pratiques, en réponse, notamment, aux questions suivantes : comment en sont-ils venus à faire ce type de travail ? Quel impact pensent-ils que cette affectation aura sur leur carrière ? Quelle

place accordent-ils à Internet dans le travail policier ? Quelle est leur opinion de la formation qu'ils reçoivent ? Travaillent-ils sur, avec ou contre Internet et de quelle(s) façon(s) ? Quels sont les obstacles rencontrés lors d'enquêtes ? Quel est le rôle joué par la formation ? Comment se comporte l'appareil juridique par rapport à Internet ? Quelles sont les étapes d'une enquête impliquant Internet ? Comment perçoivent-ils leur charge de travail ? Sur quels usages problématiques travaillent-ils ?

3.1 Choix méthodologiques

La démarche de recherche entreprise dans le cadre de ce mémoire repose sur l'utilisation d'une méthodologie qualitative. Trois motifs distincts nous poussent à adopter une telle méthodologie.

3.1.1 Caractère exploratoire

Tout d'abord, cette étude est la première à s'intéresser au processus d'organisation des corps policiers canadiens et québécois par rapport à Internet. Cette situation lui confère donc un caractère exploratoire et, par conséquent, il importe de choisir une méthode de recherche bien adaptée à ce type d'étude. Or, les méthodes de recherche qualitatives se prêtent particulièrement bien à la réalisation d'études exploratoires (Poupart et al., 1997).

En effet, la recherche exploratoire est l'une des quatre formes que peut prendre la recherche qualitative (Poupart et al., 1998). Dans notre cas, le caractère exploratoire de notre démarche ne s'applique pas tant à la nouveauté de la démarche qu'à la nouveauté du questionnement et de l'objet. Quant à la forme exploratoire de la recherche exploratoire, Poupart et al. (1998 : 33) insistent sur le fait « qu'elle n'est pas qu'une simple activité préparatoire ou préliminaire à une recherche plus large, mais bien une activité de recherche en soi. »

De plus, les méthodes de recherche plus rigides, notamment les méthodes quantitatives, conviennent moins bien aux études à caractère exploratoire comme en témoigne ces propos de Quivy et Campenhoudt (1988 : 61) :

> [...] les méthodes très formelles et structurées telles que les enquêtes par questionnaires ou certaines techniques sophistiquées d'analyse de contenu conviennent moins bien pour le travail exploratoire que celles qui présentent une grande souplesse d'application comme les entretiens peu directifs ou les méthodes d'observation où un degré de liberté important est laissé à l'observateur.

3.1.2 Intérêt envers les expériences, points de vue et pratiques

Notre intérêt envers les expériences, points de vue et pratiques de certains acteurs justifie également le recours aux méthodes qualitatives et plus précisément à l'entretien. Comme le souligne Boutin (1997 : 43-44),

> Il arrive que les méthodes plus classiques (questionnaires fermés, tests standardisés, etc.) ne nous permettent pas d'avoir accès à des données parfois essentielles : attitudes, perceptions, représentations, etc. L'entretien de recherche de type qualitatif qui nous intéresse ici au premier chef, par son côté ouvert, permet davantage l'accès à de telles données.

Afin d'atteindre nos objectifs, nous utilisons également deux autres techniques de recherche propres aux méthodes qualitatives : l'observation participante et l'analyse documentaire.

L'observation participante permet de compléter les informations obtenues par le biais des entretiens et donc d'en apprendre davantage sur les expériences, points de vue et pratiques des policiers qui participent à ce processus d'organisation. L'observation permet notamment de dépasser le discours officiel des policiers.

Quant à l'analyse documentaire, celle-ci facilite l'atteinte de notre premier objectif de recherche puisqu'elle nous procure des informations sur l'aspect organisationnel du processus étudié que les interviewés ont oubliées ou qu'ils ignorent.

Finalement, parce que le processus d'organisation des corps policiers par rapport à Internet est très récent et que les données statistiques sur le phénomène sont quasi-

inexistantes, il nous apparaît difficile, voire impossible, d'analyser ce processus en recourant à des méthodes quantitatives.

3.2 Techniques de recherche

Trois techniques de recherche ont été utilisées pour recueillir les données nécessaires à la réalisation de nos analyses :

1. L'analyse documentaire
2. L'entretien de type qualitatif
3. L'observation participante

Quoique l'utilisation de trois techniques de recherche différentes représente une charge de travail importante, cela offre l'avantage de permettre une certaine triangulation des informations.

3.2.1 Analyse documentaire

Cette technique a été utilisée afin d'obtenir des informations sur l'aspect organisationnel du processus qui nous intéresse. La littérature « grise » analysée provient des corps policiers sélectionnés et comprend des rapports, des documents internes et même des sites Web. Toutes ces informations étaient disponibles au public.

À l'instar de Poupart et al. (1997), nous estimons utile de recourir à des documents écrits pour reconstituer un passé éloigné qui date dans la mémoire de tous les interviewés. Les informations recueillies permettent de mieux circonscrire l'histoire du processus d'organisation pour des corps policiers ciblés.

3.2.2 Entretiens exploratoires

Notre démarche de recherche a débuté par la réalisation de quelques entretiens exploratoires comme le suggèrent Quivy et Campenhoudt (1988). Ces entretiens visent à bien orienter notre champ d'investigation et à éviter d'importantes pertes de temps. Ils ont été réalisés auprès « d'informateurs-clés » qui ont une bonne connaissance du processus qui nous intéressent.

Nous avons mené des entretiens que Quivy et Campenhoudt qualifient d'entretiens « libres » où nous cherchions à être le moins directif possible tout en captant beaucoup d'informations afin de bien orienter notre démarche de recherche.

3.2.3 Entretiens qualitatifs

L'entretien qualitatif est l'un des instruments de recherche les plus fréquemment employés dans les sciences sociales (Poupart et al., 1997). Puisque cette technique est particulièrement efficace pour rendre compte des points de vue des acteurs et de leur expérience (Poupart et al., 1997 p. 183), nous l'avons utilisée pour recueillir les données nécessaires à l'atteinte de notre deuxième objectif de recherche, c'est-à-dire la mise à jour de l'opinion qu'ont ces policiers d'Internet et celle de leurs expériences, points de vue et pratiques.

Nous avons réalisé des entretiens semi-directifs comportant des thèmes qui correspondent à nos sous-objectifs de recherche. Toutefois, malgré l'introduction de thèmes, notre démarche lors de la réalisation de nos entretiens demeure essentiellement non-directive puisque chaque interviewé est libre d'explorer ces thèmes à sa guise.

Mentionnons finalement que les entretiens réalisés auprès de ces policiers ont aussi rapporté de précieuses informations sur l'aspect organisationnel du processus que nous étudions.

Déroulement des entretiens

Les policiers que nous avons interviewés ont un horaire très chargé et cela influence nos entretiens de deux façons. Premièrement, puisque ces derniers peuvent difficilement se déplacer pour rencontrer un étudiant, nous avons accepté de nous entretenir avec eux dans leur milieu de travail, mais dans un endroit calme et retiré. Idéalement, nous aurions préféré réaliser nos entretiens dans un environnement « neutre » de manière à influencer le moins possible leur discours. Deuxièmement, certains interviewés ont été pressés dans le temps lors de l'entretien et cela a nécessairement limité l'ampleur de l'information qu'ils nous ont communiquée.

Ces entretiens ont été réalisés en français et ont une durée moyenne d'une heure trente minutes. Bien que tous les interviewés aient accepté d'être enregistrés, nous avons également pris des notes afin d'être en mesure d'intervenir adéquatement pendant l'entretien. Les policiers rencontrés n'ont pas été réticents à l'idée de s'entretenir avec nous. Ils nous ont même donné les noms et coordonnées de collègues et membres d'autres corps policiers.

Consignes de prise de contact

Afin d'être en mesure de comparer les propos de nos interviewés, nous avons utilisé la consigne de prise de contact suivante avec chacun d'eux :

« Bonjour, mon nom est Stéphane Lapointe, je réalise présentement ma maîtrise à l'École de criminologie de l'Université de Montréal. Ma recherche porte sur le processus d'organisation des corps policiers, canadiens et québécois, par rapport à Internet. J'aimerais m'entretenir avec vous de ce sujet. Cette entrevue sera confidentielle, anonyme et d'une durée d'environ une heure trente. »

Une fois la conversation amorcée, nous mentionnions également que l'entretien devait se tenir dans un endroit calme et qu'il ne s'agissait pas d'un questionnaire, mais plutôt d'un entretien où certains thèmes allaient être abordés de manière ouverte et chronologique.

Consigne de départ

Nous avons adapté notre protocole d'entretien de façon à couvrir l'ensemble de nos objectifs et sous-objectifs de recherche. Chaque entretien débutait par l'énoncé général suivant :

« Avant tout, je vous remercie de bien vouloir participer à cette entrevue. Comme je vous l'ai mentionné au téléphone, cette recherche a pour but de connaître le processus d'organisation des corps policiers, au Canada ainsi qu'au Québec, par rapport à

Internet. Je vous rappelle que l'entrevue est anonyme et confidentielle. J'aimerais vous demander l'autorisation d'enregistrer l'entrevue. Cela facilite mon travail et me permet de rester plus près de vos propos. Les cassettes seront détruites après l'analyse. Nous allons procéder de la manière suivante ; nous aborderons un certain nombre de thèmes de manière ouverte et chronologique. »

Deux autres énoncés ont été utilisés par la suite. Le premier visait l'atteinte de notre sous-objectif relatif à l'opinion qu'ont ces policiers d'Internet. Nous estimions qu'il était préférable de recueillir cette opinion dès le début de l'entretien afin qu'elle ne soit pas influencée par les autres thèmes abordés. Pour ce faire, nous utilisons l'énoncé suivant :

« Tout d'abord, j'aimerais que vous me donniez votre opinion d'Internet ? »

Une fois les propos de l'interviewé saturés quant à son opinion d'Internet, nous utilisions un second énoncé qui nous permettait, cette fois, d'atteindre nos autres objectifs uniformisés, c'est-à-dire, d'en apprendre davantage sur l'aspect organisationnel du processus qui nous intéresse ainsi que sur les expériences, points de vue et pratiques des interviewés. Il s'agit de cet énoncé :

« Vous travaillez dans (nom de l'unité) de la (nom du corps policier), j'aimerais que vous me parliez de votre expérience par rapport à Internet ? »

3.2.4 Observation participante

Depuis septembre 1998, nous travaillons à la Direction des renseignements criminels de la Sûreté du Québec et nous intervenons occasionnellement dans des dossiers relatifs à Internet. Nous avons donc profité de notre implication dans ces dossiers pour réaliser une observation participante et recueillir des données utiles à l'atteinte de nos objectifs de recherche.

Cette observation participante nous permet notamment de compléter les informations recueillies au moyen des autres techniques et de dépasser ainsi le discours officiel des interviewés et de la littérature « grise ».

Selon Junker (1980, cité dans Peretz, 1998), il existe quatre formes d'observation participante. Puisque nos activités de chercheur et notre objet d'étude ont été dévoilés dès notre embauche à la Sûreté du Québec, nous étions dans la catégorie de « l'observateur qui participe ». Pour Spradley (1980), notre position s'apparenterait à celle de la « participation complète » puisque nous participions au processus d'organisation des corps policiers étudiés par rapport à Internet.

Notre observation participante, qui dura du mois de septembre 1998 au mois de mars 1999, nous a donné l'occasion de recueillir d'intéressantes données. Pendant cette période, nous avons réalisé d'autres entretiens, informels cette fois, avec les policiers antérieurement interviewés ainsi qu'avec d'autres policiers qui participent au processus d'organisation par rapport à Internet. Nous avons également participé directement à la réalisation de certaines enquêtes relatives à la distribution de pornographie juvénile sur Internet en plus d'assister à des colloques et conférences sur le thème de l'intervention policière sur Internet.

Les données recueillies par le biais de cette observation participante viennent donc enrichir celles obtenues par les entretiens.

Informés de notre désir d'intégrer certaines observations à nos données, nos superviseurs ont simplement demandé qu'aucune information confidentielle ne soit divulguée dans nos résultats de recherche. Les observations réalisées ont donc été notées et intégrées au matériel recueilli par les autres techniques de recherche pour être ensuite analysées.

3.3 Stratégie d'échantillonnage

Alors que les notions d'échantillon et de population sont relativement claires dans le cadre d'une recherche quantitative, elles s'obscurcissent et se complexifient dans la plupart des recherches dites qualitatives (Poupart et al.,1997). Nous allons donc définir avec précision la population à l'étude dans ce mémoire ainsi que la stratégie d'échantillonnage utilisée pour réaliser nos entretiens.

3.3.1 Sélection de la population à l'étude

Notre démarche de recherche vise la compréhension du processus d'organisation des corps policiers, canadiens et québécois, par rapport à Internet. Dans cet ordre d'idée, la population que nous étudions, et que Sjoberg et Nett qualifient « d'univers général » (cités dans Poupart et al., 1997 : 125), est composée de l'ensemble des corps policiers canadiens et québécois qui s'organisent par rapport à Internet.

Certains facteurs nous incitèrent toutefois à ne pas examiner cette population dans son entier. Notamment le fait que certaines organisations policières présentaient un niveau d'organisation relativement bas par rapport à Internet. Nous avons donc créé ce que Sjoberg et Nett appellent un « univers de travail. » Il s'agit de l'univers sur lequel un chercheur travaille ou qu'il a à sa portée (Poupart et al., 1997). Notre univers de travail est composé de corps policiers sélectionnés parce qu'ils présentaient le niveau d'organisation le plus élevé par rapport à Internet à l'époque où nous avons réalisé notre étude. Il s'agit des corps policiers suivants :

- Gendarmerie Royale du Canada (GRC) ;
- Service de Police de la Communauté urbaine de Montréal (SPCUM) ;
- Sûreté du Québec (SQ).

À partir de ces organisations, nous avons créé un échantillon de policiers afin de réaliser des entretiens.

3.3.2 Sélection des interviewés

Les policiers sélectionnés pour la réalisation des entretiens travaillent tous au sein de l'unité spécialisée en criminalité informatique de leur organisation. Ils ont été sélectionnés pour deux raisons. D'abord, ces policiers, de par leur spécialisation, sont les mieux placés pour nous fournir des informations sur le processus d'organisation de leur corps policier par rapport à Internet. Ensuite, leurs expériences, points de vue et pratiques nous intéressent parce qu'ils travaillent sur les dossiers liés à Internet.

Puisque ces policiers étaient relativement peu nombreux à l'époque où nous avons réalisé nos entretiens, nous avons été en mesure de les rencontrer tous, ce qui représente précisément une douzaine d'entretiens.

Les policiers interviewés ont travaillé dans différentes unités avant d'être affectés à une unité spécialisée en criminalité informatique. Ils n'étaient donc pas à leurs premières armes dans le domaine des enquêtes. Tous les interviewés sont des hommes et la moyenne d'âge des interviewés est de 39 ans. Il faut comprendre que les postes au sein des unités spécialisées sont convoités et qu'il faut donc un minimum d'ancienneté et d'expérience pour en obtenir un. Aucun d'eux n'a donc été assigné à son poste contre son gré.

Il nous est possible de généraliser les résultats de notre analyse à l'ensemble des corps policiers qui s'organisent sur le territoire québécois par rapport à Internet puisque nous avons interviewé tous les policiers actifs dans ce domaine. Par contre, face aux autres organisations policières canadiennes, les policiers rencontrés ne représentent qu'un échantillon non probabiliste de type intentionnel (Fortin et al., 1988).

3.3.3 Sélection des documents analysés

Les documents utilisés pour l'analyse documentaire proviennent des organisations policières que nous avons énumérées. De façon générale, nous avons sélectionné des documents qui portent sur notre premier objectif de recherche, c'est-à-dire sur l'aspect

organisationnel du processus que nous étudions. La littérature « grise » étudiée était constituée de divers rapports et études internes. Nous avons également analysé des documents publics qui ne faisaient pas partie de cette littérature, notamment, les sites Web des organisations examinées et quelques documents qui y étaient disponibles.

3.3.4 Sélection du corps policier observé

Nous n'avons pas réellement sélectionné le corps policier observé puisque aucune observation participante n'avait été planifiée au tout début de notre démarche de recherche. Il s'agit plutôt d'un concours de circonstances à l'issue duquel nous avons été engagé par la Direction des renseignements criminels de la Sûreté du Québec pour travailler spécifiquement sur la problématique de la pornographie juvénile sur Internet. Ce n'est qu'une fois au travail, que nous avons décidé de profiter de la situation pour réaliser une telle observation participante.

3.4 Analyse du matériel

Une fois les entretiens terminés, nous avons utilisé ces enregistrements pour effectuer une transcription « verbatim » de chaque entretien. Cette transcription, quoique longue et ardue, nous a donné l'occasion de prendre connaissance de notre matériel avant de débuter son analyse.

Une fois les transcriptions terminées, nous avons utilisé les verbatims pour réaliser une analyse horizontale du matériel qui consiste à analyser chaque entrevue de manière individuelle. Il s'agit d'une analyse pendant laquelle nous identifions les thèmes qui ressortent du discours des interviewés. Il va sans dire que deux de ces thèmes, en l'occurrence nos objectifs de recherche, ressortent directement du protocole de recherche. D'autres thèmes ont également émergé de cette analyse thématique. Ces thèmes et sous-thèmes furent regroupés et utilisés pour réaliser l'analyse verticale des données.

Les observations menées et les documents sélectionnés ont été analysés en utilisant la grille thématique qui s'était dégagée de l'analyse des entretiens. Les données obtenues par l'observation participante et les informations contenues dans les documents sélectionnés ont donc été classées sous les thèmes et sous-thèmes identifiés lors de l'analyse des entretiens et sont venues enrichir ces thèmes.

Lors de cette analyse verticale, nous avons comparé les propos des divers interviewés relativement aux thèmes qui ont émergé de l'analyse horizontale et ce sont les résultats de cette analyse verticale que nous présentons dans les deux prochains chapitres. Le premier de ces chapitres a trait à notre premier objectif de recherche : l'aspect organisationnel du processus d'organisation des corps policiers, canadiens et québécois, par rapport à Internet. Le second porte sur notre deuxième objectif de recherche et ses sous-objectifs et traite des expériences, points de vue et pratiques des policiers relatifs à ce processus d'organisation.

Toutes les démarches de recherche ont des limites et nous allons maintenant aborder celles de notre étude.

3.5 Limites de notre recherche

Peu importe le soin apporté à la préparation et à l'exécution d'un travail de recherche, chaque démarche méthodologique comporte des limites. La nôtre ne fait bien sûr pas exception à cette règle.

Deux problèmes relatifs au discours des interviewés risque de se poser. D'une part, parce que nous les informions de la tenue de nos rencontres avec les membres d'autres organisations policières, les policiers interviewés ont peut-être adopté un discours qui avantage leur organisation face aux autres. Il est probable qu'ils tentent de nous donner une image de leur organisation qui soit avantageuse par comparaison avec les autres organisations. D'autre part, les policiers que nous avons rencontrés sont également habitués à accorder des entretiens à divers médias et étudiants et il est donc possible

qu'ils aient adopté un discours officiel qui ne reflète que partiellement la réalité.

Notre démarche de recherche connaît une autre limite contre laquelle nous ne pouvons rien et qui est propre à notre domaine de recherche dont l'évolution est très rapide. Internet est un univers en perpétuelle évolution. Au vu de cette constante évolution, les organisations policières auront encore à s'organiser et à modifier leurs interventions pour demeurer efficaces dans leur travail sur le Net. Contrairement à des recherches réalisées face à des problématiques plus stables et moins changeantes, la réalité que nous décrivons dans notre recherche risque donc de ne plus être à jour à brève échéance.

Par contre, cette dernière limite ne s'applique pas à tous les aspects de notre étude. Par exemple, l'origine du processus d'organisation des corps policiers examinés ainsi que les points de vue des policiers que nous avons rencontrés sont des thèmes qui demeureront contemporains dans les années à venir.

Dans l'analyse du matériel obtenu par entrevues, nous devons également tenir compte du fait que les membres des différents corps policiers ne travaillent pas tous sur les mêmes problématiques et les organisations pour lesquelles ils travaillent n'ont pas toutes les même objectifs.

Ensuite, quoique nous ayons rencontré tous les membres de ces unités à l'époque où nous réalisions nos entretiens, de nouveaux membres ont maintenant intégré les rangs de ces équipes et nous n'avons pas eu l'occasion de les interviewer. Les opinions présentées dans ce document sont donc celles des membres des unités à l'époque où les entrevues ont été réalisées.

Finalement, notre observation participante ne porte que sur un seul corps policier, en l'occurrence la Sûreté du Québec, et par conséquent les observations réalisées ne s'appliquent pas forcément de façon intégrale aux autres corps policiers.

Processus d'organisation des corps policiers par rapport à Internet

4 Processus d'organisation des corps policiers par rapport à Internet

Les nombreuses données recueillies par le biais des entretiens, de l'observation participante et de l'analyse documentaire ont été analysées en fonction de nos deux objectifs de recherche.

Les fruits de cette analyse sont dévoilés dans deux chapitres distincts. Ce premier chapitre présente les résultats relatifs au processus d'organisation des corps policiers par rapport à Internet, tandis que le chapitre suivant contient les résultats propres aux expériences, points de vue et pratiques des policiers qui participent à ce processus.

Notre cueillette de données nous a permis d'obtenir des informations sur les thèmes suivants :

- les circonstances ayant mené à l'intervention policière sur Internet ;
- le mandat des unités spécialisées qui interviennent sur Internet ;
- les ressources affectées à ces unités ;
- la formation des membres de ces unités ;
- le processus de sélection des dossiers face auxquels ces unités interviennent ;
- les projets futurs relatifs à Internet ;
- les relations intra et extra-organisationnelles.

4.1 Circonstances ayant mené les organisations policières à intervenir sur Internet

Nos entretiens révèlent l'existence d'une étape importante qui a précédé et, en quelque sorte occasionné, l'intervention policière sur Internet. Il s'agit de l'intervention policière face à la criminalité informatique en général. Nous allons donc examiner cette première étape avant de jeter un coup d'œil du côté de l'intervention policière spécifique à Internet.

4.1.1 Intervention policière face à la criminalité informatique

Cette intervention débuta de façon similaire, quoique à des époques différentes, dans les trois corps policiers qui nous intéressent. Comme l'explique ce policier de la Sûreté du Québec, elle fut initiée par des membres des unités spécialisées en criminalité économique. Ces policiers, habitués à collaborer étroitement avec les entreprises du secteur privé, furent les premiers confrontés à des enquêtes criminelles impliquant des ordinateurs.

> D'abord pourquoi aux crimes économiques plutôt qu'ailleurs ? Parce qu'on a été la première escouade a être confrontée aux ordinateurs. Pourquoi ? Parce que dans le milieu commercial et dans le milieu des affaires on informatise de plus en plus la gestion des affaires (Pierre, SQ).

Quelques membres de ces unités ont donc développé, officieusement et de leur propre chef, une expertise en matière d'intervention policière face à certains crimes informatiques.

> Donc, à l'interne, des gens intéressés à l'informatique ont commencé à développer des méthodes et à intervenir sur les lieux pour saisir les données comptables (Pierre, SQ).

Alors que cette expertise s'est développée approximativement vers 1990 à la SQ et au SPCUM, c'est en 1986 que des policiers spécialisés en crimes économiques de la GRC se sont intéressés pour la première fois à ce champ d'intervention.

> C'est cette unité-là qui a constaté, il y a 12 ou 15 ans, que l'informatique était de plus en plus implantée dans le milieu des affaires. On a réalisé qu'on avait besoin d'une personne ressource à l'intérieur de l'unité pour l'aspect informatique. Donc on a créé une position et on a placé du personnel en pour donner le support informatique aux autres enquêteurs (Luc, GRC).

En 1990, la GRC retira quelques-uns de ses policiers des enquêtes pour les assigner exclusivement au support informatique. Ceux-ci étaient tellement accaparés par les

demandes d'assistance de plus en plus nombreuses, qu'ils n'étaient plus en mesure de travailler sur leurs propres enquêtes de crimes économiques « conventionnels ».

> On supportait les enquêteurs à temps partiel, mais on était souvent sollicités et on avait pas le temps de faire nos propres enquêtes de crimes économiques (Martin, SQ).

Quant à la Sûreté du Québec et au Service de police de la Communauté urbaine de Montréal, c'est en 1997 qu'ils ont assigné des policiers au support informatique.

Selon ce policier de la Sûreté du Québec, la décision de la GRC et du SPCUM d'assigner des effectifs au support informatique aurait incité la Sûreté du Québec à faire de même afin de ne pas être désavantagée face à ces corps policiers.

> Il y avait une demande qui était telle qu'il fallait que la Sûreté du Québec bouge et si elle ne bougeait pas, j'imagine que les gens auraient été voir la GRC ou le SPCUM (Martin, SQ).

Les interviewés sont d'ailleurs partagés quant à l'expérience de chaque organisation en matière d'intervention sur Internet. Un policier de la Gendarmerie royale du Canada estime que son unité est plus avancée que les autres dans ce domaine.

> La première section ailleurs a commencé en 1997. Alors on est en avance de 7 ans (Serge, GRC).

De leur côté, les membres des unités de la Sûreté du Québec et du SPCUM considèrent que la différence d'expérience entre les diverses unités est minime puisque tous les policiers qui travaillent dans ce domaine ont la même source de formation.

> Ils (GRC) ont peut-être une expérience un peu plus développée, mais on a tous la même source de formation, qui est le Collège canadien de police (Pierre, SQ).

Indépendamment du corps policier examiné, un membre de la GRC croit que le Québec, comparativement aux autres provinces canadiennes, fait figure de pionnier en matière d'intervention policière face aux crimes technologiques.

> Je vais te dire qu'à Montréal on est en avance parce qu'il y a plusieurs provinces où ça n'existe même pas une unité des crimes technologiques (François, GRC).

Cette situation tend cependant à changer. De nombreuses provinces possèdent maintenant une ou plusieurs équipes spécialisées en criminalité informatique qui interviennent également sur Internet. Mentionnons, à titre d'exemple, l'équipe du « Projet P »[17] de « l'Ontario Provincial Police » qui se spécialise dans la lutte contre la pornographie juvénile sur Internet.

Ainsi, le développement d'équipes spécialisées en criminalité informatique à jeté les bases de l'intervention policière sur Internet car, comme nous allons le constater, ce sont ces mêmes équipes qui ont été chargées d'intervenir sur Internet.

4.1.2 Intervention policière sur Internet

L'intervention policière sur Internet débuta en 1995, suite au dépôt de plaintes par des citoyens et des entreprises. Par la suite, des demandes d'assistance pour des dossiers liés à Internet furent également formulées par des corps policiers sans expertise.

Dès la réception de ces premières plaintes et demandes d'assistance, les corps policiers eurent le réflexe de transmettre celles-ci à leur unité spécialisée en criminalité informatique.

> Par la suite des gens ont commencé à nous appeler pour nous dire qu'ils étaient sur Internet et qu'ils avaient rencontré tel ou tel problème (Sébastien, SQ).

---

[17] Site Web : http://www.gov.on.ca/OPP/projp/english/default.htm

Toutefois, le commentaire de cet interviewé laisse croire que les unités ne sont pas toutes en mesure d'enquêter n'importe quel crime réalisé sur Internet.

> La plainte nous a été signalée, mais au niveau technique on n'a pas les ressources pour remonter ça. La GRC a quelques expériences de ce côté-là (Pierre, SQ).

Contrairement à la Sûreté du Québec et au SPCUM, la GRC a été appelée à enquêter des crimes qui impliquent l'utilisation illégale de réseaux téléphoniques par les premiers pirates informatiques. Il est probable que cette expérience a avantagé la GRC face aux autres corps policiers lorsque les premières plaintes relatives à Internet ont été déposées.

> Ce que les pirates voulaient avoir à cette époque c'était une ligne téléphonique pour rejoindre les babillards électroniques d'élite. Les choses ont beaucoup changé depuis 1995. Le nombre de nos dossiers de hackers ou de pirates a diminué un peu. Parce que le besoin d'avoir une ligne téléphonique est de moins en moins important depuis l'arrivée d'Internet (Serge, GRC).

Nous savons quand et dans quel contexte s'est développée l'intervention policière face à la criminalité informatique et sur Internet. Regardons le mandat de chacune des unités spécialisées.

4.2 Mandat des unités spécialisées en criminalité informatique

Ce mandat est relativement simple puisqu'il comporte un ou deux volets selon l'unité en question. Chacune d'elles offre du support dans les enquêtes liées à Internet et certaines enquêtent également quelques crimes particuliers.

4.2.1 Le support intra et extra-organisationnel

Les unités de la GRC, de la Sûreté du Québec et celle du SPCUM supportent les enquêteurs de leur organisation aux prises avec des dossiers qui impliquent l'informatique.

> Ce n'est pas nous autres qui allons enquêter douze types de crimes différents. Par contre, on fait le bout qui touche à l'aspect informatique de la preuve. Ils font leur enquête et le bout informatique on est là pour s'en occuper (André, SQ).

Comme le souligne un membre de la Sûreté du Québec, ce support est également offert aux enquêteurs d'autres corps policiers qui en font la demande au même titre que les autres services spécialisés.

> Souvent c'est le service de police municipal qui entre en contact avec nous. - On a une plainte et on ne sait pas quoi faire avec- (Pierre, SQ).

Ce support peut prendre différentes formes selon la nature de l'enquête et les besoins des requérants. Il peut s'agir par exemple :

- d'assister les enquêteurs dans la rédaction des mandats ;
- de procéder à la perquisition électronique d'un ou de plusieurs ordinateurs ;
- d'analyser le contenu de ces ordinateurs ;
- de préparer les éléments de preuve pour leur présentation à la cour ;
- de faire le lien entre les représentants de l'organisation et les experts du privé ;
- de conseiller l'organisation face à certaines problématiques liées à l'informatique (« bogue de l'an 2000 », équipement à se procurer, etc.).

4.2.2 Les enquêtes de crimes informatiques

En plus d'offrir du support, les unités de la GRC enquêtent également sur certains crimes informatiques qui, pour la plupart, impliquent Internet.

> Lorsqu'on parle de crimes informatiques ou technologiques, c'est notre unité qui va procéder aux enquêtes. Mais c'est bien spécifique aux hackers, aux méfaits aux données ou aux vols de télécommunications (François, GRC).

Parmi les crimes que cette unité est appelée à enquêter, on trouve :

- l'accès à des systèmes informatiques ou leur utilisation sans autorisation ;

- les méfaits contre des données ;
- la fraude en matière de télécommunications.

L'unité de la GRC en place dans la ville de Québec, contrairement à celle de Montréal, enquête également sur des crimes liés au respect des droits d'auteur sur Internet.

> Contrairement à mes collègues de Montréal, on a un aspect d'enquête supplémentaire ici. On met en application, à notre unité, la loi sur les droits d'auteur. L'aspect informatique de cette loi (Luc, GRC).

Le mandat de chaque unité respecte bien sûr le mandat général, donc la juridiction du corps policier auquel elle appartient. Mais lorsqu'on parle d'intervention policière sur Internet, le respect du mandat et de la juridiction des différents corps policiers s'avère plus difficile puisque la plupart des enquêtes impliquent des pays étrangers. Cette situation semble avantager la GRC puisque, comme le mentionne un de ses policiers, elle est théoriquement en mesure de s'approprier la plupart des enquêtes liées à Internet.

> Tu ne peux pas parler d'Internet sans parler d'international. Alors on a toujours la possibilité de prendre une enquête si on veut la prendre, mais on a toujours la possibilité de la refuser si on ne peut pas la faire (Yan, GRC).

Le commentaire d'un autre membre de la GRC laisse toutefois croire que le respect de la juridiction des divers corps policiers ne pose pas de problème.

> Ce n'est pas notre territoire et on laisse ça au SPCUM parce que ce sont eux qui s'occupent de ça (Serge, GRC).

La plupart des corps policiers traversent actuellement une période de coupures budgétaires. Or, pour être en mesure d'assurer le respect de son mandat, chaque unité a besoin de ressources humaines, monétaires et matérielles importantes.

4.3 Ressources affectées à ces unités

Notre participation à certaines enquêtes liées à Internet nous a permis de constater que l'intervention policière sur Internet nécessite d'importantes ressources humaines, monétaires et matérielles.

4.3.1 Ressources humaines

Voici, pour chaque unité, les effectifs actuellement en place ainsi que le processus de sélection des membres qui les composent.

- Gendarmerie royale du Canada

La GRC dispose de deux unités spécialisées en criminalité informatique. La première est située à Montréal et la seconde dans la ville de Québec. Tout récemment, de nouveaux postes ont été autorisés pour ces deux unités ce qui devrait augmenter leur taille jusqu'à 13 membres dans le cas de l'unité montréalaise et à 5 pour l'unité de Québec. Parmi ces 18 membres, un seul employé civil est affecté à l'unité montréalaise.

- Sûreté du Québec

La nouvelle structure mise en place par la Sûreté du Québec à l'automne 1999 comporte une unité située à Montréal ainsi qu'une unité dans la ville de Québec. La première compte six policiers et deux techniciens civils, la seconde trois policiers.

- Service de police de la Communauté urbaine de Montréal

L'unité du SPCUM est composée de quatre policiers et d'un analyste.

Toutes ces unités sont composées de policiers et d'un ou plusieurs superviseurs administratifs qui s'occupent de la gestion de l'équipe et qui participent occasionnellement aux enquêtes.

> On a aussi un sergent mais il est plus ou moins dans les enquêtes. Il enquête de temps en temps mais il est surtout occupé avec la supervision du groupe (Serge, GRC).

Sélection des membres des unités spécialisées en criminalité informatique

Les premiers membres ont été recrutés parmi ceux qui travaillaient aux crimes économiques et qui ont supporté leurs collègues dans les dossiers liés à l'informatique.

Les unités emploient maintenant un processus plus formel pour sélectionner les nouveaux membres. Elles utilisent le même processus que les autres unités spécialisées et, en collaboration avec les responsables des ressources humaines, annoncent officiellement les postes disponibles, déterminent les qualifications requises pour y postuler, organisent des entrevues, etc. Néanmoins, on accorde toujours autant d'importance à la motivation des candidats qui désirent se joindre à ces unités.

> On demandait un minimum d'éducation, c'est-à-dire un baccalauréat, et un intérêt marqué pour ce genre de travail (François, GRC).

Certains policiers ont d'ailleurs déployé d'importants efforts personnels pour obtenir un poste au sein de l'une de ces unités.

Lors de notre observation participante, nous avons été à même de constater que la plupart de ces policiers sont des passionnés d'informatique tout comme les délinquants et criminels auxquels ils sont confrontés. Ce sont des individus qui ont un intérêt marqué pour l'informatique et donc, qui s'y intéressent également lorsqu'ils sont hors du milieu de travail.

Mis à part l'intérêt pour l'informatique, un membre de la GRC explique que les qualités d'enquêteur sont également très importantes pour travailler dans une telle unité.

> On ne mettra plus un nombre d'années minimal au sein de la GRC, mais on va peut-être mettre un nombre d'années minimal au sein d'unités opérationnelles. Quelqu'un qui a travaillé au niveau administratif depuis les deux dernières années, bien il y a beaucoup de choses qui ont changées pendant ce temps-là (François, GRC).

Notre observation participante nous porte effectivement à croire que l'expérience d'un policier au niveau des enquêtes peut grandement augmenter les chances de réussite d'une enquête liée à l'informatique. Par exemple, la préparation de la preuve dans une enquête qui implique Internet est particulièrement ardue et demande des habiletés de communicateur et de vulgarisateur afin de bien faire comprendre les éléments techniques au juge ou aux membres du jury. Il est parfois difficile d'obtenir un simple mandat de perquisition chez le fournisseur Internet lorsque le juge de paix n'est pas familier avec l'informatique et Internet.

Nous avons constaté un fait relativement étonnant lors de nos entretiens avec les gestionnaires de ces unités. Ceux-ci estiment que les policiers ayant une formation académique en informatique ne sont pas forcément les meilleurs candidats pour travailler dans ces unités. Il semble que le travail que doit accomplir le membre d'une unité spécialisée en criminalité informatique est fort différent de ce pour quoi sont formés les informaticiens.

> J'ai demandé à la section formation de me sortir les dossiers de tous les policiers qui avaient une formation en informatique. Là j'ai regardé ça et après avoir interviewé des gens, j'ai constaté que c'est pas parce que tu as une formation en informatique que tu sais de quoi tu parles. [...] Ce n'est pas de l'informatique pour dire comment un réseau devrait être monté mais c'est de l'informatique pour la criminalité et c'est pas du tout la même chose (Dominique, SPCUM).

Bien que cette opinion soit partagée par l'ensemble des gestionnaires d'unités spécialisées en criminalité informatique, elle est toutefois contradictoire avec le désir que ceux-ci manifestent d'avoir au sein de leur équipe des informaticiens civils qui aident les policiers dans les dossiers très techniques.

Les ressources monétaires accordées à ces unités influencent aussi directement plusieurs aspects de leur fonctionnement. Alors que ces corps policiers traversent une période de

vache maigre, il est intéressant d'analyser l'opinion des interviewés au sujet des ressources monétaires accordées à leur unité.

4.3.2 Ressources monétaires

Bien qu'il nous soit impossible d'obtenir des informations sur les budgets passés, actuels ou futurs des unités spécialisées en criminalité informatique, plusieurs interviewés estiment que leur unité est privilégiée au niveau budgétaire et ce, même si leur corps policier subit d'importantes compressions budgétaires.

> Si je parle de mon unité à moi je dois dire qu'on a été choyé. Par contre si tu parles à mon patron, lui il a été coupé (François, GRC).

Les sommes nécessaires au fonctionnement de chacune de ces unités sont prélevées à même le budget de l'unité des crimes économiques de chaque corps policier. Or, deux problèmes découlent du fait que ces unités ne disposent pas de budget distinct.

D'abord, comme le souligne ce membre de la Sûreté du Québec, cela complexifie l'achat d'équipements par ces unités.

> Alors ça pose des problèmes parce que les budgets pour acheter cet équipement on prend encore ça sur les budgets de l'escouade ou sur le budget du district, parce que ce n'est pas encore distinct. Il n'y a pas encore de structure financière propre. Donc il faut constamment convaincre les autorités d'enlever de l'argent à quelque part pour le mettre là (Sébastien, SQ).

Ensuite, nous avons mentionné que les membres de ces unités spécialisées offrent du support à l'ensemble des enquêteurs de leur organisation. Or, le gestionnaire de l'unité des crimes économiques, qui utilise son budget pour payer le salaire de ces policiers spécialisés, n'est pas très heureux de voir son budget utilisé pour payer des ressources qui travaillent plus souvent qu'autrement pour d'autres unités.

Pour être en mesure de remplir adéquatement leur mandat, les unités spécialisées en criminalité informatique doivent également disposer de certains outils. Ces outils sont relativement dispendieux et, parce que le monde informatique évolue rapidement, doivent être remplacés fréquemment. L'analyse qui suit vise à identifier comment les corps policiers s'organisent face à cet autre besoin particulier.

4.3.3 Ressources matérielles

Deux motifs font en sorte que les membres des unités spécialisées qui interviennent sur Internet doivent avoir accès à de l'équipement informatique performant et donc coûteux. D'une part, comme le souligne ce membre de la Sûreté du Québec, ils doivent posséder des ordinateurs aussi puissants que ceux des criminels sur lesquels ils enquêtent.

> Donc il faut être à la fine pointe de la technologie pour dire que si on a un nouvel ordinateur à perquisitionner, on va être capable aussi (Martin, SQ).

D'autre part, comme l'explique cet interviewé, certains équipements dispendieux à l'achat, peuvent se révéler économiques à moyen et long terme. Par exemple, l'achat d'un ordinateur dernier cri peut permettre d'effectuer un travail d'analyse plus rapidement et donc rendre une unité plus productive.

> Un moment donné, pour que ce soit plus efficace, on va aller chercher des appareils plus performants puis ça va coûter moins cher en temps/hommes (Pierre, SQ).

Puisque les unités spécialisées en criminalité informatique ne sont pas autonomes au niveau budgétaire, leurs gestionnaires doivent justifier l'achat de certains équipements auprès de leurs supérieurs. Or, ceux-ci comprennent difficilement que les membres de ces unités ne puissent plus utiliser des équipements achetés il y a à peine deux ans alors que toutes les autres unités de l'organisation s'en accommodent très bien.

Néanmoins, plusieurs policiers rencontrés sont d'accord avec ce membre du SPCUM pour estimer que les ressources matérielles dont ils disposent se sont améliorées depuis la mise sur pied de leur unité.

> Bien moi je trouve qu'on a fait d'énormes progrès. Je ne sais pas si tu as examiné notre unité à ses débuts ? Au début, on avait un petit bureau, on était deux, on pouvait pas tirer nos deux chaises en même temps. Maintenant on a trois locaux, de l'équipement, on a un budget, on a de la formation (Dominique, SPCUM).

L'évolution rapide du monde informatique n'entraîne pas seulement la désuétude des équipements utilisés dans ces unités. Elle exige également d'eux qu'ils renouvellent constamment leurs connaissances. La prochaine section examine donc la question de la formation des policiers affectés aux interventions sur Internet.

4.4 Formation

Afin de bien situer la place qu'occupe la formation dans le travail de ces spécialistes, nous nous sommes attardés aux facteurs qui expliquent l'importance de la formation, aux types de formation, aux sources de formation, à la formation offerte au Collège canadien de police ainsi qu'aux problèmes liés à la formation.

Deux facteurs expliquent l'importance de la formation pour les policiers spécialisés en criminalité informatique. Celui le plus fréquemment mentionné, est l'évolution de la technologie.

> On doit faire de la formation continue parce que les méthodes changent, la technologie change et ça évolue très rapidement (Yan, GRC).

Cette évolution est très rapide et force ces policiers spécialisés à constamment renouveler leur formation.

> Parce que si on dit que pendant six mois on ne fait pas de formation et qu'on fait juste des enquêtes, dans six mois ça change beaucoup. Il va y avoir tellement de choses à reprendre que l'on n'arrivera pas. (Yan, GRC).

Un membre de la Sûreté du Québec croit d'ailleurs que les policiers qui travaillent dans ce domaine doivent retourner au Collège canadien de police annuellement pour mettre à jour leurs connaissances.

> [...] ce que nous leur demandons actuellement (aux enquêteurs), c'est de retourner au collège au moins une fois par année. Parce que tu suis ces cours mais ça évolue tellement que ce qu'ils nous ont dit il y a deux ans, tu peux oublier ça, c'est démodé. (André, SQ).

Le second facteur s'avère être la grande diversité des équipements et des logiciels que ces policiers rencontrent dans le cadre de leur travail. Ces derniers doivent posséder les connaissances nécessaires pour remplir leur mandat peu importe l'équipement ou le logiciel auquel ils sont confrontés.

> Que ce soit en matière d'enquête ou en matière de support, on rencontre des systèmes informatiques différents à chaque fois qu'on va à quelque part (Yan, GRC).

Examinons les divers types de formation offerts aux policiers des unités qui interviennent sur Internet.

4.4.1 Types de formation

Nous distinguons deux types de formation qui se complètent. D'abord, une formation que nous appelons « personnelle » et qui est acquise par l'enquêteur dans ses temps libres et habituellement à ses frais. Les faiblesses et la rareté de la formation officielle viennent augmenter l'importance de ce type de formation. Le superviseur d'une unité considère d'ailleurs que ses policiers doivent investir des efforts dans la formation « personnelle » s'ils veulent bien fonctionner au sein de leur équipe.

> Oui, puis je vais te dire une chose, s'il y en avait un qui ne faisait pas ça, il ne suivrait pas. Premièrement il aurait la pression de ses pairs. (...) Ce n'est pas parce que tu veux le mettre à la porte, c'est parce qu'un moment donné il va être dépassé. Il va se retirer de lui-même (François, GRC).

Ensuite, une formation que nous qualifions de « professionnelle. ». Il s'agit de la formation offerte à l'enquêteur dans le cadre de son travail, aux frais de l'organisation et le plus souvent pendant ses heures de travail.

4.4.2 Sources de formation personnelle

Les policiers interviewés mentionnent deux sources de formation personnelle. Les cours collégiaux et universitaires ainsi que les lectures et l'expérimentation personnelle.

Cours collégiaux/universitaires

Pratiquement tous les enquêteurs rencontrés, à un moment ou à un autre de leur cheminement professionnel, ont réalisé des études collégiales ou universitaires en informatique. Deux enquêteurs de la GRC ont cependant souligné qu'il était difficile de concilier de telles études avec le travail et la vie familiale.

> Moi j'ai fait des cours de programmation au cégep Vanier et des cours dans l'électro-technologie au cégep Vanier aussi. Mais là je suis démotivé. J'ai fait toute mon université le soir et je suis retourné pour mes cours d'informatique et d'électro-technologie et je voulais juste en faire un peu. Mais j'ai pas le temps. J'ai deux enfants à la maison et chaque fois que je me préparais à étudier, ils venaient me déranger (Serge, GRC).

> Suivre des cours à l'université, avec la famille et le travail c'est plus difficile. Il faut y aller à petit pas et non à grands pas. Donc l'expertise et l'expérience sont plus longues à acquérir (Luc, GRC).

Lectures et expérimentations personnelles

Plusieurs enquêteurs lisent des ouvrages spécialisés en informatique et expérimentent ce qu'ils y apprennent à la maison dans leurs temps libres.

> Comme moi je reçois des magazines à la maison. C'est comme ça que je m'informe des nouvelles choses qui sortent, des problèmes reliés à Windows et à Windows NT, les réseaux (François, GRC).

> Les gars ont beaucoup d'initiative. Ils achètent leurs volumes et ils se montent des systèmes informatiques à la maison. Parce que je vais te dire ; si on se met à faire ça ici on n'aura pas le temps de faire des enquêtes (François, GRC).

4.4.3 Sources de formation professionnelle

Nous identifions quatre sources de formation professionnelle : le Collège canadien de police (CCP), la formation donnée au sein des organisations policières, la formation disponible dans le secteur privé et l'apprentissage au travail.

1. La formation donnée au Collège canadien de police (CCP)

Le CCP est la seule source de formation professionnelle systématiquement utilisée par tous les policiers que nous avons rencontrés. On y offre des cours pour les policiers qui interviennent face aux crimes informatiques et sur Internet. Nous détaillons les caractéristiques du CCP dans une section ultérieure.

2. La formation donnée au sein des organisations policières

Certains corps policiers, notamment la GRC, offrent des cours en informatique à leurs membres. Ces cours peuvent porter sur l'utilisation de systèmes d'exploitation (Windows, Linux) ou sur l'utilisation de logiciels de bureautique. Ils s'adressent habituellement aux utilisateurs débutants et ne répondent que partiellement aux besoins des policiers spécialisés en criminalité informatique qui doivent connaître les «dessous» de ces systèmes et logiciels.

3. La formation disponible dans le secteur privé

Cette formation peut prendre deux formes différentes. La première est une formation offerte à l'ensemble de la population et qui, tout comme celle donnée au sein des

organisations policières, convient davantage à l'utilisateur débutant ou intermédiaire qu'à l'enquêteur informatique.

La seconde est une formation donnée par le secteur privé, à la demande d'un ou de plusieurs corps policiers et qui, quoique plus dispendieuse, est beaucoup plus adaptée aux besoins des policiers qui interviennent sur Internet.

Face aux coûts élevés de cette formation, un membre de la Sûreté du Québec suggère que les unités spécialisées se regroupent pour commander, financer et recevoir cette formation.

> On a déjà discuté de se former nous-mêmes le groupe de la GRC, SPCUM et Sûreté du Québec. Par exemple identifier un besoin spécifique et l'exprimer au Centre de recherche informatique de Montréal ou à d'autres personnes compétentes qui peuvent répondre à nos questions et organiser une session de formation (Pierre, SQ).

4. Apprentissage en cours de travail

Des enquêteurs affirment, tout comme ce membre de la Sûreté du Québec, que le fait d'être régulièrement confrontés à des problèmes et à des défis permet de développer de nouvelles techniques et d'approfondir ses connaissances en informatique.

> C'est une formation sur le tas, mais c'est une formation quand même. C'est à force de perquisitionner, de faire des tests, d'essayer des choses (Martin, SQ).

Un policier de la GRC abonde dans le même sens.

> Mais dans le domaine de l'informatique, le meilleur apprentissage c'est d'embarquer sur l'ordinateur. Tu comprends un peu et tu y vas. C'est ça qu'on fait (Serge, GRC).

Selon un enquêteur de la Sûreté du Québec, le principal problème de la formation « professionnelle » ne serait pas sa qualité mais plutôt le nombre restreint de sources.

> [...] on a tous les même sources d'informations, la même source de formation, qui est le Collège canadien de la police. Il y a pas une grande panoplie, on n'a pas beaucoup le choix au niveau de la formation. (...) Actuellement le problème qu'on a au niveau de la formation c'est qu'on a atteint un espèce de plateau, un niveau de saturation (Pierre, SQ).

Parce qu'il occupe un rôle important dans la formation des policiers qui interviennent sur Internet, le Collège canadien de police mérite d'être examiné de plus près.

4.4.4 Le Collège canadien de police (CCP)

Voici la mission officielle du Collège canadien de police (Collège canadien de police, Page consultée le 11 décembre 1999) :

> « [. . .] être le chef de file dans le développement professionnel de la communauté policière en définissant et en établissant, en collaboration avec nos clients, des normes nationales d'excellence dans le secteur de la formation policière et des services d'information. »

Le CCP offre donc une gamme importante de cours spécifiquement destinés à la communauté policière. Parmi ceux-ci, on trouve des cours qui traitent de l'intervention policière face aux crimes informatiques et de l'intervention policière sur Internet :

- perquisition électronique ;
- perquisition électronique d'un système Macintosh ;
- principes d'un réseau et techniques d'enquête ;
- techniques d'enquête sur les fraudes en télécommunication.

Ces cours durent en moyenne 10 jours et sont donnés à une quinzaine d'élèves à la fois. Les participants sont sélectionnés et évalués une fois la formation terminée.

Selon un policier de la Sûreté du Québec, les cours qu'offre le CCP en matière de criminalité informatique sont très réputés et attirent des participants de partout au Canada et même de l'étranger.

> Nous autres on n'a pas de diplôme universitaire, mais on a des diplômes du Collège canadien de police qui a une bonne réputation. Pour te donner un exemple, sur un des cours que j'ai fait il y avait des gens d'un peu partout et ils considéraient que le cours comme étant de meilleure qualité que ceux du FBI (André, SQ).

Il semble que le CCP ait d'ailleurs toujours été très avant-gardiste en matière de formation policière à caractère technologique.

> La première fois que j'ai entendu parler de ce cours c'est en 1979. Mais c'était bien différent d'aujourd'hui. Mais en 1979, c'était pas mal d'avant-garde d'avoir des cours comme ça (Serge, GRC).

Toutefois, il importe de mentionner que le CCP ne s'intéresse à Internet que depuis 1995.

> En mars 1995, je suivais un cours au Collège canadien de police à Ottawa et le CCP avait deux ou trois ordinateurs reliés à Internet. On jouait avec ça mais c'était pas vraiment quelque chose qui nous préoccupait à cette époque. C'était plus pour s'amuser (Serge, GRC).

Bien que le CCP soit administré par la GRC, cela n'avantage en rien les membres de ce corps policier qui sont sélectionnés et traités de la même façon que les autres participants.

> Par exemple la GRC va payer pour envoyer un gars au CCP. Ce n'est pas gratuit pour la GRC. C'est la même chose que pour les gens de la CUM. Le CCP ne peut pas donner seulement un cours sur le hacking et le vol de télécommunication parce que le GRC ne fait que ça. Si tu fais ça le gars de la CUM n'ira pas parce que lui il travaille sur la pédophilie, la pornographie, la fraude, etc (Yan, GRC).

Problèmes reliés à la formation offerte au CCP

Quoique les policiers rencontrés apprécient et reconnaissent la qualité de la formation offerte au CCP en matière de criminalité informatique, ils identifient néanmoins quelques problèmes associés à celle-ci et notamment à son accessibilité.

On reproche entre autres au CCP de ne pas être en mesure de répondre à la demande de formation des corps policiers. Un informateur-clé nous confirme d'ailleurs que le CCP n'est pas en mesure de répondre à cette demande, ni même à celle qu'il considère comme étant prioritaire.

> Présentement, on satisfait 50% de la demande totale. De la demande totale, on a une demande prioritaire et on rencontre à peu près 80% de la demande prioritaire (Julie, CCP).

Indirectement, cette situation complique la formation de la relève puisqu'il est difficile pour les enquêteurs d'autres domaines de recevoir de la formation du CCP. En effet, puisque les places dans les classes sont limitées, le CCP favorise les policiers qui travaillent déjà dans le domaine de l'informatique.

Il est également probable que l'adoption récente, par le CCP, d'une politique de recouvrement des coûts, limite de plus en plus l'accès des petits corps policiers à la formation offerte au Collège.

> Mais je te parlais un peu plus tôt de « cost recovery ». Ça va devenir un peu plus difficile pour les petits corps policiers qui n'ont pas beaucoup d'argent de prendre 1 000$ ou 1 500$ pour venir à un cours au Collège canadien de police (Julie, CCP).

Si c'est effectivement le cas, cette situation renforcera la centralisation actuelle des unités spécialisées en criminalité informatique dans les grands centres urbains et les grands corps policiers.

Comme le dit cet interviewé, l'accessibilité à la formation offerte au CCP est également limitée pour les policiers qui ne maîtrisent pas suffisamment l'anglais.

> Le problème que l'on a c'est que tous les cours sont en anglais alors on a besoin d'un gars qui est bilingue (Sébastien, SQ).

Finalement, et dans un autre ordre d'idée, un enquêteur de la Sûreté du Québec reproche au CCP d'afficher un léger retard face à certaines innovations technologiques.

> Même le CCP prend du retard face à certaines choses et parfois on doit lui dire de bouger parce qu'il est en arrière sur certains points (André, SQ).

De l'avis d'un informateur-clé impliqué dans la gestion des programmes de formation du CCP, ce retard est en partie lié aux lourdeurs administratives du Collège qui empêchent de modifier et d'adapter rapidement le contenu des cours.

Peu importe le type ou la source de formation que l'on examine, il semble qu'il sera toujours difficile de former un policier sans expérience antérieure dans le domaine.

> [...] je suis dans le domaine depuis 1992 et je juge que j'ai encore beaucoup à apprendre. C'est sûr qu'un jeune de 14, 15, 16, 17, 18, qui est allé au cégep en informatique, qui est allé au cégep ou à l'université en informatique a un gros bagage de connaissances. Mais quelqu'un qui n'a jamais fait ça et qui commence dans l'informatique à 32 ou 35 ans ça va prendre des années avant qu'il ait autant de connaissances (Luc, GRC).

Bien qu'ils soient très motivés, on peut se demander si ces policiers, dont la moyenne d'âge est de 39 ans, ne sont pas désavantagés lorsque confrontés à un jeune délinquant passionné d'informatique.

Ces interviewés semblent affirmer que la formation ne suffit pas à rendre un policier efficace dans son travail. Celui-ci doit acquérir de l'expérience sur le terrain.

> Il y a une formation de base avant de pouvoir dire que j'ai assez d'expérience. L'expérience entre en ligne de compte par la suite (Luc, GRC).

> Tu vois, il y a un policier qui s'en vient bientôt, il est recruté et il a tous les cours qu'il faut. Quand il va venir, c'est l'expérience qu'il va lui manquer (Martin, SQ).

Mentionnons qu'Internet n'est abordé que dans un seul des 5 cours donnés au CCP. La plupart des cours ou séminaires auxquels participent les enquêteurs portent plutôt sur des notions relatives à l'informatique en général. Toutefois, puisque l'intervention sur Internet est une forme spécialisée d'intervention face à la criminalité informatique, les interviewés estiment qu'il est normal qu'on leur enseigne des notions générales d'informatique. Il est également probable, dans un avenir rapproché, que l'augmentation de la criminalité sur Internet entraîne l'apparition d'autres cours orientés vers les usages problématiques de ce réseau informatique.

Finalement, un interviewé explique que le travail des enquêteurs spécialisés en criminalité informatique serait grandement facilité si l'on enseignait aux autres policiers les attitudes à adopter face aux dossiers liés à l'informatique. On éviterait notamment qu'ils endommagent des éléments de preuve en manipulant un ordinateur sur la scène d'un crime.

Regardons comment ces unités s'y prennent pour sélectionner les dossiers dans lesquels elles interviennent.

4.5 Sélection des dossiers ou ces unités interviennent

Puisque leur personnel est restreint et que leur charge de travail augmente continuellement, les unités spécialisées en criminalité informatique doivent sélectionner les dossiers où elles interviennent.

Les unités qui offrent du support ne sont habituellement consultées qu'une fois l'enquête initiée. Leur capacité à sélectionner les dossiers dans lesquels elles interviennent est donc limitée. Elles peuvent néanmoins donner leur opinion sur les chances de réussite d'une enquête et ainsi influencer la décision d'entreprendre ou non l'enquête.

De plus, parce que les unités spécialisées en criminalité informatique sont souvent le point de chute des plaintes relatives à Internet, elles peuvent examiner celles-ci et

sélectionner celles qui seront traitées par leur organisation et celles qui seront ignorées ou référées à un autre corps policier.

> On est dans ce milieu là, donc on reçoit des plaintes par Internet. Souvent ce sont des demandes d'information qui vont devenir des plaintes. Souvent ce sont des plaintes qui vont simplement être des informations transmises. À ce moment-là on fait une première filtration. Est-ce que ça concerne la police oui ou non ? Est-ce qu'on redirige les gens vers un autre organisme ? (Dominique, SPCUM).

Quant aux unités de la GRC, celles-ci peuvent également sélectionner les enquêtes qu'elles vont initier. Ce pouvoir de sélection est même très grand puisque, comme nous l'avons souligné lorsque nous avons abordé le mandat de chacune des unités, la plupart des enquêtes sur Internet sont de nature internationale et la GRC est mandatée pour enquêter les crimes internationaux..

Aucune de ces unités n'utilise une procédure systématique et méthodique pour sélectionner les dossiers face auxquels elle intervient. Il s'agit plutôt d'une évaluation basée sur certains critères officieux énumérés par les interviewés.

La nature du litige

Évidemment, on s'assure, avant d'intervenir, qu'il s'agit bel et bien d'un acte criminel et non d'un litige civil.

> On a des demandes par des gens qui sont offusqués de la nature subversive, haineuse ou raciste des messages. Au niveau criminel on a aucun pouvoir d'intervention (Pierre, SQ).

Le mandat et la juridiction de l'unité

Le mandat et la juridiction des corps policiers sont les deux principaux critères à la base de la sélection des dossiers. La GRC enquête habituellement sur les crimes inter-provinciaux et internationaux, tandis que la Sûreté du Québec s'intéresse aux crimes

perpétrés au Québec, exception faite de ceux qui surviennent sur le territoire de la Communauté urbaine de Montréal puisqu'ils sont traités par le SPCUM.

Même si toutes les unités affirment respecter la juridiction des autres corps policiers, les propos d'un membre de la GRC laissent croire que cela n'est pas toujours le cas.

La collaboration de la victime

Dans certains dossiers, la collaboration de la victime est particulièrement importante pour la réussite de l'enquête. Par exemple, il arrive à l'occasion que l'on demande à une victime de laisser son système informatique vulnérable quelques jours, afin d'accumuler les éléments de preuve nécessaires à l'identification du criminel. Comme le mentionne ce membre de la GRC, certaines victimes n'acceptent pas de prendre ce risque.

> La probabilité que l'on attrape un pirate informatique est parfois très faible. Si on lui permet de se brancher à nouveau au système, on peut peut-être l'attraper. Si la compagnie qui est victime n'est pas prête à faire ça, on leur explique que les chances de l'attraper sont très minces. Selon ce que la victime va nous dire c'est nous qui allons décider si on va entreprendre l'enquête ou pas (Yan, GRC).

Les répercussions à long terme de l'acte criminel

Même si l'évaluation de ces répercussions est subjective, elle sert tout de même à sélectionner les dossiers à traiter.

> On évalue les répercussions à long terme, si on prend action ou si on ne prend pas action (François, GRC).

Le nombre de victimes touchées

Pour ce policier de la GRC, le statut social de la ou des victimes est moins important que le nombre total de victimes touchées par l'acte criminel.

> C'est pas parce que c'est une organisation en particulier, comme Bell Canada, qu'on va le faire. Mais si ça touche 25% de la population c'est pas la même chose (François, GRC).

Toutefois, les propos d'un autre policier de la GRC laissent croire que lorsqu'il s'agit d'un cas isolé, les pertes financières liées à l'acte criminel peuvent influencer la décision d'amorcer ou non l'enquête.

> C'est évident que c'est dommage pour le monsieur dont le site Web personnel a été vandalisé mais il s'agit habituellement de données sans grande valeur. C'est pas comme une compagnie qui va devoir payer pour remettre son système en ligne (Vincent, GRC).

Chances de réussite du dossier

Ces policiers désirent entreprendre des enquêtes susceptibles d'être fructueuses à la cour et qui, éventuellement, donneront lieu à une jurisprudence qui les appuiera dans leurs enquêtes futures.

> À la cour, on va amener des dossiers qui peuvent nous donner, pas une jurisprudence, mais au moins un genre de barème. [...] On va prendre des cas qu'on va réussir à la cour (Serge, GRC).

Impact dissuasif

Pour ce policier de la GRC, il importe de concentrer les efforts des unités sur les délinquants les plus habiles afin d'envoyer un message dissuasif efficace aux autres délinquants.

> Tu as un meilleur impact si tu attrapes des bons délinquants. Si c'est juste des petits ça va presque renforcer les gros. Ils vont dire qu'on passe notre temps à attraper des petits (Vincent, GRC).

Certains policiers disent être agacés de ne pas pouvoir travailler sur toutes les plaintes formulées par la population. Mais ils admettent tous que leur charge de travail et les ressources limitées dont ils disposent les forcent à effectuer cette sélection.

Le processus d'organisation des corps policiers canadiens et québécois par rapport à Internet ne sera jamais terminé. Le caractère changeant d'Internet forcera les organisations policières à constamment s'adapter à la nouvelle réalité d'Internet et c'est pourquoi nous désirons évaluer leur vision de l'évolution d'Internet et de la criminalité qui s'y trouve.

4.6 Évolution future d'Internet et de la criminalité qu'on y trouve

Les policiers et gestionnaires des unités estiment que les usages problématiques et criminels d'Internet seront de plus en plus nombreux puisque Internet est de plus en plus facile à utiliser et, comme l'explique un interviewé, de plus en plus abordable.

> Le jeune pirate informatique, ça ne lui tente peut-être pas de payer 35$ par mois pour aller sur Internet, mais peut-être que quand ça va être à 10$ par mois (Luc, GRC).

Plusieurs, dont ce membre de la Sûreté du Québec, craignent que le crime organisé utilise de plus en plus Internet pour communiquer de façon sécuritaire et à l'abri de l'écoute électronique.

> Il est possible que les bandes criminalisées utilisent de plus en plus Internet pour communiquer. Par exemple dans des transactions de drogue. [...] Elles peuvent encrypter leurs messages et communiquer via Internet. Moi je pense, mais je peux me tromper, qu'il va en avoir de plus en plus (Martin, SQ).

Deux policiers, de la Sûreté du Québec et de la GRC, estiment que le commerce électronique va connaître un essor considérable à court et à moyen terme.

> Donc il y a beaucoup de changements à l'horizon. Un autre changement, qui est lent à démarrer à cause de la sécurité, ce sont les transactions internationales sur Internet. Les banques commencent là, mais on se rend compte que les systèmes de sécurité sont peut-être encore jeunes et pas efficaces à 100% (André, SQ).

> Les gens hésitent pour le moment à faire du commerce, mais je pense que ça va être la prochaine grosse vague (Vincent, GRC).

Un membre de la Sûreté du Québec va même plus loin en affirmant qu'éventuellement, Internet et d'autres médias tels la télévision, la radio et le téléphone, seront appelés à se fondre l'un dans l'autre.

> Dans quelques années, l'ordinateur, la télévision, les DVDs et le téléphone seront tous intégrés dans ton ordinateur et ton ordinateur va faire des tâches de toutes sortes dans la maison (André, SQ).

Il est également probable que l'essor que connaîtra le commerce électronique dans les années à venir entraînera une hausse de la criminalité économique dans le cyberespace.

Évidemment, puisqu'ils pensent que les usages problématiques et criminels d'Internet vont prendre de l'ampleur, les policiers interviewés croient également qu'ils seront de plus en plus nombreux à travailler dans ce champ d'intervention.

> On a maintenant trois locaux sur l'étage. On est quatre et probablement bientôt 5 ou 6 personnes. Ça va bien. Bientôt on va mettre en fonction, si on a le temps, notre propre réseau interne pour partager nos ressources et faire des tests. Tu ne peux pas évoluer dans ce milieu si tu ne fais pas de tests et si tu n'expérimentes pas (Dominique, SPCUM).

Il semble que l'analyse de ces policiers s'est avérée juste. Nous avons observé, depuis la réalisation des entretiens, la croissance des unités de deux des trois corps policiers examinés. Malgré cela, les policiers qui composent ces unités sont encore relativement peu nombreux. Nous avons constaté, lors de la réalisation des entretiens, que la plupart

d'entre eux se connaissent et qu'ils connaissent également plusieurs acteurs du secteur privé. Les relations qu'ils entretiennent entre eux ainsi qu'avec les acteurs du secteur privé sont examinées et font l'objet du thème suivant.

4.7 Les relations intra et extra-organisationnelles

Les acteurs avec lesquels les membres des unités spécialisées en criminalité informatique entretiennent des relations sont de trois types :

- les unités spécialisées en criminalité informatique d'autres corps policiers
- le secteur privé
- la population

4.7.1 Les relations avec les unités spécialisées d'autres corps policiers

Les interviewés affirment que ces relations sont très bonnes. Comme en témoignent les propos de ce membre de la Sûreté du Québec, il semble exister un esprit de camaraderie et de solidarité entre les membres des différentes unités.

> Ils (membres des autres unités) ont autant besoin de nous autres comme on a besoin d'eux. On est tous sur le même pied. On ne peut pas dire qu'il y en a un qui est plus avancé que nous autres. Certains ont peut-être plus de moyens financiers que nous, mais au point de vue des connaissances c'est équivalent (Martin, SQ).

Un policier nous fait remarquer que les membres des unités collaborent entre eux afin de standardiser les méthodes, les procédures et les équipements utilisés dans les interventions sur Internet afin de faciliter la tâche aux acteurs du système judiciaire avec qui ils travaillent. De plus, cette collaboration évite à chaque unité de chercher la solution à un problème déjà résolu par une autre unité.

Les unités spécialisées en criminalité informatique collaborent également entre elles pour pallier au manque de ressources matérielles et humaines.

> Quelquefois c'est au niveau du matériel. Quand tu as besoin de Jazz à 150$ la copie, et que tu dois en avoir 10 tu contournes le problème des coupures budgétaires en empruntant de l'équipement (Pierre, SQ).

> Tu ne peux pas être spécialiste de tout. Donc à un moment donné il y en a qui ont plus de facilité dans un domaine et d'autres dans un autre. Il y en a qui sont plus familiers avec les réseaux ou bien avec d'autres types d'interventions (Pierre, SQ).

Pour ce policier de la Sûreté du Québec, il est important que les unités se regroupent et échangent tout comme le font les délinquants auxquels ils sont confrontés.

> De toute façon on n'a pas le choix, il faut échanger. Les bandits l'ont compris. Le crime organisé s'organise et celui qui n'a pas sa place dans le groupe ne demeure pas longtemps dans le groupe. La police doit s'organiser et les guerres de clocher doivent cesser (André, SQ).

Même les policiers qui se considèrent les plus expérimentés, comme ce membre de la GRC, se disent prêts à partager leur expérience avec les membres des autres unités.

> Nous sommes les pionniers dans ce domaine. Les autres sont nouveaux dans ce domaine et ils ont moins d'expérience. Nous autres on est prêt à partager notre expérience avec eux, la Sûreté du Québec et le SPCUM (Serge, GRC).

Il existe même des associations internationales de policiers spécialisés en criminalité informatique et en intervention sur Internet.

> Il y a aussi l'organisation américaine HTCIA (High Technology Crime Investigator Association) qui devient tranquillement internationale. Il y a beaucoup de procureurs là-dedans mais il y aussi des enquêteurs et des intervenants en informatique. HTCIA c'est un organisme structuré avec des chapitres dans différents coins des États-Unis. À l'automne, les enquêteurs du SPCUM sont allés à une convention de cet organisme en Californie et ils ont obtenu l'autorisation d'ouvrir un chapitre au Québec (André, SQ).

Il existe également une certaine collaboration entre les unités de divers pays et celle-ci permet à chaque organisation de mener plus aisément des enquêtes qui impliquent des individus ou des organisations situés dans un autre pays :

> Puisque « America Online » est situé aux États-Unis, ton mandat ou ton autorisation légale qui est valide ici, te permet pas de perquisitionner là-bas. Il faut alors demander l'assistance d'un corps policier là-bas. Mais le crime est ici, alors ça prend des interrogatoires, des contre-interrogatoires. Ça demande une commission rogatoire, mais c'est long. C'est pour ça qu'il y a beaucoup d'échanges entre les services de police (Pierre, SQ).

Comme le souligne ce policier de la Sûreté du Québec, un corps policier peut difficilement mener à terme une enquête liée à Internet sans interagir avec une autre organisation policière.

> De toute façon ça s'en vient de plus en plus comme ça parce que tu vas commencer une enquête et elle va se finir en Colombie-Britannique, en Europe ou ailleurs dans le monde. C'est pas évident que c'est toi qui va arrêter le gars (André, SQ).

Il n'en demeure pas moins que la plupart des unités examinées doivent constamment justifier leur existence et les budgets qui leurs sont accordés en présentant des statistiques sur le nombre d'enquêtes entreprises et terminées. Cela n'encourage pas forcément le partage des informations ou la remise d'un dossier à un autre corps policier afin que celui-ci termine l'enquête.

4.7.2 Les relations avec le secteur privé

Comme en témoigne le commentaire de ce policier, il est crucial que les unités qui interviennent sur Internet aient de bonnes relations avec le secteur privé.

> Il faut se fier sur les compagnies téléphoniques parce que tout passe sur les lignes téléphoniques. Sans eux, nos chances sont réduites. Mais on a de très bonnes ententes et relations avec elles alors ça aide (Serge, GRC).

Même s'ils peuvent obtenir certaines informations à l'aide d'un mandat de perquisition, ces policiers apprécient de pouvoir contacter un expert du secteur privé qu'ils connaissent et obtenir rapidement une information particulière.

Les relations avec les acteurs du secteur privé et des policiers situés à l'étranger facilitent également le travail des unités canadiennes et québécoises.

> Quand on a contacté les gens de la Californie pour obtenir des renseignements, ils ont été très surpris d'apprendre ce qui se passait sur leur serveur et ont offert leur entière coopération. Ils ont même fermé le site Web et coupé l'accès à cet individu (Luc, GRC).

À l'heure actuelle, ce sont les acteurs du secteur privé qui font de la recherche et du développement. Les corps policiers doivent donc entretenir des relations avec ceux-ci pour être au fait des dernières nouveautés. Malheureusement, le secteur policier ne semble pas être un marché très intéressant pour ces entreprises puisqu'il est encore très petit.

> Il y a le Centre de recherche informatique de Montréal qui fait des recherches de ce côté-là et l'entreprise privée. Et jusqu'à quel point ça devient rentable pour l'entreprise privée de développer des logiciels spécialisés pour ça. C'est bien beau, tu développes quelque chose, mais tu ne peux pas le vendre nulle part ailleurs (Pierre, SQ).

Finalement, lorsque les membres de ces unités se heurtent à des problèmes techniques qui dépassent leurs compétences, ils font appel aux services d'informaticiens du secteur privé.

4.7.3 Les relations avec la population

Les relations qu'entretiennent ces corps policiers avec la population sont limitées. Bien sûr, ces organisations policières possèdent un site Web que les internautes peuvent consulter et une adresse de courrier électronique qu'ils peuvent utiliser pour les rejoindre. Les unités spécialisées en criminalité informatique accordent également de

nombreux entretiens aux médias et réalisent des conférences dans des écoles, des entreprises et des associations d'individus impliqués dans le milieu informatique.

Ces policiers gagneraient cependant à utiliser des stratégies plus interactives et innovatrices pour rejoindre les internautes et les informer de leurs activités. Ils pourraient par exemple échanger avec les membres de diverses communautés virtuelles ou tenir des séances d'information thématiques dans certains canaux du service de bavardage Internet.[18]

4.8 Sommaire

L'analyse des thèmes abordés dans ce chapitre permet de replacer le processus d'organisation de ces corps policiers par rapport à Internet à l'intérieur d'un processus d'organisation encore plus vaste, celui par rapport à l'informatique en général. Pour tous les corps policiers examinés, ces deux processus furent initiés par les unités spécialisées en criminalité économique et reposent presque entièrement sur les épaules de quelques policiers.

Ceux-ci sont regroupés dans des unités spécialisées en criminalité informatique qui sont mandatées pour offrir du support dans les dossiers qui impliquent l'informatique ou Internet. Certaines de ces unités ont également le mandat d'enquêter sur quelques crimes relatifs à Internet.

Parce qu'elles disposent de ressources limitées et qu'elles ont une charge de travail considérable, ces unités doivent sélectionner les enquêtes dans lesquelles elles interviennent et celles qu'elles initient. Pour ce faire, elles se basent principalement sur leur mandat et leur juridiction mais également sur des facteurs tels que la nature du

---

[18] Service de bavardage-clavier permettant aux internautes dotés du logiciel client approprié, de participer, en temps réel, à des forums de bavardage accessibles au moyen d'un réseau de serveurs spécialisés. **Note(s):** Le terme générique anglais « chat » est très souvent utilisé pour désigner le service de bavardage IRC. (Source : OLF, Page consultée le 15 avril 2000).

litige, le nombre de victimes, la collaboration de la victime et les chances de réussite de l'enquête.

Pour fonctionner et être en mesure de remplir leur mandat, ces unités requièrent des ressources humaines, matérielles et monétaires importantes. Bien que ces unités puissent s'accommoder du manque de personnel ou d'équipements qui ne sont pas à la fine pointe de la technologie, elles peuvent difficilement se passer de formation. Leurs membres sont confrontés à une grande variété de logiciels et d'équipements ainsi qu'à l'évolution rapide de la technologie. C'est pourquoi ils doivent posséder de bonnes connaissances en informatique ainsi que sur le fonctionnement d'Internet.

Nous avons également constaté qu'il existe une certaine solidarité entre les membres des différents corps policiers qui s'organisent par rapport à Internet. Ceux-ci, peut-être parce qu'ils sont peu nombreux et qu'ils font face aux même défis, échangent des informations et se prêtent main forte pour surmonter les obstacles. Contrairement à d'autres champs d'intervention policière, l'intervention face aux crimes liés à Internet exigent également de ces policiers qu'ils entretiennent de bonnes relations avec certains acteurs du secteur privé.

Nous allons maintenant examiner les résultats de nos analyses en regard à notre second objectif de recherche qui porte sur l'examen des pratiques des policiers qui sont au cœur de ce processus d'organisation par rapport à Internet.

Expériences, points de vue et pratiques des policiers

5 Expériences, points de vue et pratiques des policiers

Ce chapitre porte sur l'examen des expériences, points de vue et pratiques des policiers au cœur du processus d'organisation dont nous avons relaté le développement dans le chapitre précédent.

Comme nous l'avons précisé dans le chapitre sur la problématique et la méthodologie, nous avons jugé utile d'explorer l'opinion générale qu'ont les policiers d'Internet et ceci afin de mieux comprendre leur points de vue, expériences et pratiques professionnelles.

L'analyse de notre matériel met en évidence les cinq thèmes suivants:

- l'opinion qu'ont les policiers d'Internet ;
- les obstacles à l'intervention policière sur Internet ;
- la charge de travail des unités spécialisées en criminalité informatique ;
- l'utilisation d'Internet par les policiers ;
- le point de vue des policiers sur leur travail.

5.1 Opinion qu'ont les policiers d'Internet

Même si des aspects positifs d'Internet sont mentionnés par quelques interviewés, l'opinion générale d'Internet est plutôt négative. Ceux-ci énumèrent brièvement quelques aspects positifs d'Internet, puis dressent une longue liste de ses facettes négatives.

Toutefois, certains interviewés, tel ce policier de la Sûreté du Québec, sont plus nuancés et estiment qu'Internet n'est ni bon, ni mauvais en soi mais que ce sont les internautes qui en font un bon ou un mauvais usage.

> Moi je compare embarquer sur Internet, à quelqu'un qui va visiter une grande ville n'importe où dans le monde. Il y en a qui vont visiter les cathédrales et les musées. Et il y en a d'autres qui vont aller au bordel. Ça dépend de qui tu es et sur Internet c'est exactement la même chose (André, SQ).

Nous croyons que le travail qu'exercent les policiers interviewés est en partie responsable de leur vision négative d'Internet et c'est également l'opinion de ce membre de la GRC :

> Mais nous autres, dans notre travail, on voit l'aspect noir. Parce que quand tout va bien, personne nous appelle. On entre en action quand il y a des problèmes (Serge, GRC).

Les pages qui suivent présentent les points de vue positifs puis négatifs qui ressortent de l'opinion qu'ont les interviewés d'Internet.

5.1.1 Les points de vue positifs

Les policiers rencontrés ont soulevé trois aspects positifs d'Internet.

Internet est un outil de communication efficace

Tous les interviewés estiment qu'Internet est un outil de communication efficace. Ils utilisent d'ailleurs fréquemment le courrier électronique pour communiquer dans le cadre de leurs activités professionnelles et personnelles.

Internet permet des relations interpersonnelles sans discrimination

Pour ce policier du SPCUM, Internet permet à chacun de vivre des relations interpersonnelles enrichissantes et épanouissantes, indépendamment de ses caractéristiques sociales ou physiques.

> On va abolir les frontières, on donne de l'accessibilité et la possibilité à des gens d'interagir entre eux même s'ils sont informes ou paraplégiques. Tu peux quand même être quelqu'un toute la journée dans ce monde virtuel qui ne tient pas compte de ton enveloppe, de tes besoins ou de tes ressources financières (Dominique, SPCUM).

Internet libéralise et universalise la connaissance

Un interviewé, membre de la Sûreté du Québec, croit qu'Internet libéralise et universalise la connaissance humaine en rendant accessible à tous des informations autrefois réservées à une élite intellectuelle.

> Tu places une masse de connaissances à la portée de tous. Tu libéralises la connaissance plutôt que de l'enfermer dans des universités (André, SQ).

Il croit également que cette libéralisation de la connaissance risque de ne pas plaire à tous les gouvernements et donne l'exemple du gouvernement chinois.

> Présentement, la Chine recense tous les gens qui ont accès à Internet. Tous les gens qui ont accès à Internet dans le pays sont recensés. Et ils voudraient bien censurer certaines choses (André, SQ).

5.1.2 Les points de vue négatifs

La vision générale d'Internet est plutôt négative et est partagée par la majorité des policiers que nous avons rencontrés.

Internet est un nouvel outil pour réaliser des crimes

Plusieurs interviewés partagent l'opinion de ce membre de la Sûreté du Québec et considèrent qu'Internet est un nouvel outil pour commettre des crimes autrefois réalisés d'une autre façon.

> Avant la fausse représentation se faisait par courrier et maintenant elle se fait par Internet. [...] Plutôt que de prendre une enveloppe et un timbre, on va l'envoyer par email (Pierre, SQ).

Un policier de la GRC abonde dans le même sens :

> Parce que comme vous savez, les crimes changent. Les mêmes crimes se font, mais la façon de faire les crimes change et Internet c'est une façon (Serge, GRC).

Au yeux des policiers, il s'agit d'un nouvel outil très avantageux pour les criminels.

> Avant c'était plus difficile parce que le pédophile devait se déplacer physiquement dans des lieux que les jeunes fréquentaient. Maintenant il n'a plus besoin. Il ne se fait pas voir, on ne voit pas son visage, on ne sait pas son nom, on ne connaît pas son identité (Luc, GRC).

Un membre de la GRC explique que la distribution de pornographie juvénile est un crime beaucoup plus avantageux à commettre via Internet.

> Ça fait longtemps qu'il y a de la pornographie juvénile mais avant Internet c'était moins connu et plus discret et cette pornographie était distribuée par courrier ou de main en main. Avec Internet, plus besoin de ça. C'est facilement accessible sur Internet et on s'échange des fichiers de pornographie juvénile (Luc, GRC).

Internet permet la réalisation de nouveaux crimes

L'apparition d'Internet a également rendu possible la réalisation de nouveaux crimes, tels les intrusions dans des systèmes informatiques.

> Par contre l'intrusion dans un système informatique c'est un nouveau crime. Ça n'existait pas avant parce que les ordinateurs ne communiquaient pas entre eux (Dominique, SPCUM).

On peut difficilement contrôler les dires et les activités des internautes

Plusieurs facteurs font en sorte qu'il est difficile de contrôler Internet. Par exemple, on peut difficilement vérifier la véracité des informations qui circulent sur Internet et il est pratiquement impossible de contrôler les activités des gens qui y naviguent.

> Donc non seulement il n'y a pas de contrôle sur le contenu, mais il n'y a pas de contrôle sur les personnes qui vont expédier ou qui vont mettre des choses, donc sur les utilisateurs (Pierre, SQ).

L'inadaptation de nombreuses lois criminelles et civiles complique également le contrôle d'Internet et profite aux criminels qui évitent ainsi les accusations ou obtiennent des sentences plus clémentes.

> Donc n'importe qui peut dire n'importe quoi et non seulement on n'a pas de contrôle là-dessus mais puisque le réseau existe dans un espace virtuel, la législation ne s'est pas encore adaptée à cette réalité (Pierre, SQ).

Finalement, comme l'explique ce membre du SPCUM, les parents moins familiers avec Internet éprouvent des difficultés à superviser et contrôler les activités de leur(s) enfant(s) sur Internet.

> Et la plupart des parents vont mettre une protection pour que l'enfant ne visite pas des sites problématiques. La plupart des enfants sont plus brillants que les parents en informatique et ils peuvent facilement déverrouiller une protection ou un mot de passe (Dominique, SPCUM).

Les relations personnelles vécues sur Internet sont fausses

Un policier de la Sûreté du Québec croît que la plupart des internautes profitent du fait que leur interlocuteur ne peut vérifier la véracité de leurs propos pour mentir. Notamment face à leurs caractéristiques physiques. Il estime également que les relations vécues sur Internet sont, pour la plupart, basées uniquement sur le charme et le « flirt », tout comme celles vécues par le biais du *Minitel* français.

Internet facilite l'accès à des contenus problématiques

Parmi les contenus problématiques auxquelles les internautes ont accès, on trouve des «recettes» pour fabriquer des bombes, des propos haineux et des outils de piratage informatique disponibles gratuitement. La présence de ces contenus problématiques sur Internet fait dire à un policier de la GRC que les enfants ne doivent pas naviguer sur Internet sans supervision parentale.

> Ils (parents) achètent un ordinateur ou ils disent à leurs enfants de s'occuper et ceux-ci passent des heures et des heures sur l'ordinateur. Je pense que ce

> n'est peut-être pas une erreur des parents, mais une méconnaissance des dangers d'Internet si les enfants naviguent aux mauvais endroits (Serge, GRC).

Cet interviewé considère même que certains contenus présents sur Internet sont parfois plus problématiques que ceux que l'on trouve dans les autres médias.

> Les sujets comme le sexe et la pornographie. Ça a toujours existé, mais là ce sont des affaires plus bizarres que tu vois sur Internet. [...] Des enfants, des animaux, des actes indécents que tu ne vois jamais ailleurs (Serge, GRC).

Les internautes ne savent pas encore comment se protéger sur Internet

Ces derniers n'ont pas encore développé les réflexes nécessaires pour être en mesure de se protéger adéquatement lorsqu'ils naviguent sur Internet.

> En fait ce ne sont pas tellement les habiletés mais c'est les attitudes sociales appropriées. Si tu marches dans la rue et tu vois huit membres d'un gang de rue qui semblent des durs et ils veulent t'intercepter pour te parler. Tu vas peut-être être craintif, hésitant, méfiant, tu vas peut-être mettre la main sur ton portefeuille, tu vas peut-être regarder s'il y a du monde dans les environs. S'ils te demandent ton nom, où tu demeures, ta date de naissance et ce que tu aimes, comment s'appelle ta mère, tu vas être un peu hésitant à leur donner ces informations et un tas de renseignements sur toi. Sur Internet est-ce que tu vas te méfier ? Non ! Les gens ne se méfient pas (Dominique, SPCUM).

On peut développer une dépendance envers Internet

Cet interviewé affirme que des internautes prennent goût à la navigation sur Internet, au point de négliger d'autres aspects de leur vie et que des psychologues offrent désormais des traitements spécialement adaptés aux « cyber-dépendants ».

> Je voyais, dans une revue, qu'ils ont même développé une discipline en psychologie pour la dépendance à Internet. Comme il y en a qui sont dépendants au jeu et à la boisson (Pierre, SQ).

S'il est vrai que des psychologues ont offert de tels traitements, il faut également mentionner que d'autres spécialistes de la psychologie affirment que la dépendance à

Internet n'est pas différente des autres formes de dépendance (ex. jeu, alcool, sexe) et qu'il n'y a pas lieu de la traiter différemment (Abitbol, E., Faucon, B., Page consultée le 11 décembre 1999).

La navigation sur Internet est une perte de temps

Un interviewé estime qu'on ne peut utiliser Internet sans se laisser distraire de son objectif initial et perdre du temps.

> Je regarde les gens utiliser Internet et c'est censé être plus rapide et efficace et ça prend plus de temps parce que tu dévies toujours de ton sujet. Tu es censé partir d'un entonnoir et réduire, mais finalement c'est le contraire qui se passe (Martin, SQ).

L'opinion qu'ont ces policiers d'Internet est plutôt négative. Bien que quelques-uns de ces policiers naviguent sur le Net à la maison, la plupart sont en contact avec Internet dans le cadre de leur travail. Or, il semble qu'ils font face à de nombreux obstacles dans leurs interventions. Ces obstacles sont présentés dans la prochaine section.

5.2 Obstacles à l'intervention policière sur Internet

L'intervention policière sur Internet est très complexe et ils doivent surmonter plusieurs obstacles. Nous avons regroupé ces obstacles à l'intérieur de trois principaux groupes, soit :

- les obstacles liés au système judiciaire et/ou d'ordre législatif ;
- les obstacles inhérents aux organisations policières ;
- les obstacles liés aux caractéristiques du monde informatique.

5.2.1 Obstacles liés au système judiciaire et/ou d'ordre législatif

Ces obstacles démontrent que le système judiciaire n'est pas encore complètement adapté à la réalité et aux particularités des crimes liés aux réseaux informatiques.

Sentences rares et peu sévères

De l'avis des policiers, les sentences pour les crimes réalisés sur Internet sont rares et peu sévères parce qu'il s'agit de crimes non-violents, qui n'inspirent pas la crainte dans l'opinion publique et qui sont souvent réalisés par des individus sans antécédent judiciaire.

Absence de jurisprudence relative aux crimes informatiques

L'absence de jurisprudence rend les procureurs de la couronne nerveux à l'idée de présenter de telles causes en cour et ceux-ci n'entament donc des procédures que si les policiers leur remettent des dossiers très étoffés.

> Beaucoup d'entre eux (juges, avocats, procureurs) ont peur de ces causes et ne veulent pas y toucher. Je pense que c'est juste la peur de faire une gaffe au niveau des causes. Donc ils ne veulent que des super bonnes causes où on est entré et le gars était là puis il vient de rentrer dans le système (Vincent, GRC).

Obtention et préparation de la preuve

Les problèmes liés à la preuve sont multiples. Tout d'abord, certains éléments de preuve détenus par les fournisseurs Internet, tels les registres d'activité des internautes, doivent être récupérés rapidement par les policiers puisqu'ils ne sont conservés que quelques jours.

Ensuite, la présentation d'éléments de preuve techniques à la cour exige des policiers un important travail de vulgarisation. Ce ne sont pas tous les acteurs du système judiciaire qui sont familiers avec Internet et ses aspects techniques.

> C'est difficile de préparer un dossier pour les tribunaux ou pour un procureur parce que c'est un domaine avec des termes techniques et complexes qu'ils ne connaissent pas. Il faut vulgariser beaucoup (Yan, GRC).

Nous avons constaté, par le biais de notre observation participante, qu'il est parfois difficile d'identifier un individu qui a posé un geste problématique sur Internet. Dans

certains cas, même lorsque les policiers trouvent l'ordinateur utilisé pour commettre le crime, ils doivent encore identifier son utilisateur. C'est le cas lorsque l'ordinateur se trouve dans une demeure où habitent plusieurs internautes ou dans une bibliothèque municipale ou un « cyber-café ».

Crimes sans victime immédiate

La distribution de pornographie juvénile et la vente ou l'échange de logiciels piratés sur Internet sont des exemples de crimes sans victime immédiate, difficiles à détecter pour les corps policiers. Internet est tellement vaste que ces activités se déroulent souvent sans attirer l'attention des forces de l'ordre.

Relativité des normes

Une activité impliquant des internautes de différents pays, peut être considérée comme illicite dans l'un de ces pays et licite dans l'autre. Prenons l'exemple de la distribution de pornographie juvénile. Puisque l'âge de la majorité diffère d'un pays à l'autre, un individu peut offrir de la pornographie légale dans son pays, à un autre individu qui demeure dans un pays où ce matériel est illégal. Dans une telle situation, comment déterminer les normes qui ont préséance ? À l'heure actuelle, les organisations policières canadiennes prennent pour acquis que si la victime ou le(s) criminel(s) sont au Canada, alors le droit criminel canadien s'applique.

Définition du crime informatique

Les législateurs de différents pays ont de la difficulté à s'entendre sur la définition même du crime informatique. Une définition reconnue par ceux-ci est pourtant importante puisqu'elle offre une base pour l'encadrement de l'intervention policière face aux crimes commis via l'informatique et Internet.

5.2.2 Obstacles inhérents aux organisations policières

Nous avons regroupé ici les obstacles inhérents aux organisations policières sans distinction entre les organisations policières concernées. Ces obstacles se retrouvent dans une ou plusieurs des organisations examinées.

La juridiction policière

Une organisation policière tient compte de sa juridiction pour sélectionner les actes criminels sur lesquels elle enquête. Or, lorsqu'il est question des crimes liés à Internet, cette façon de faire s'avère problématique à deux égards.

Premièrement, la juridiction d'une organisation policière se limite à une zone géographique bien précise alors que la plupart des gestes posés sur Internet peuvent difficilement être situés dans le temps et l'espace. Par conséquent, il est difficile d'identifier le corps policier censé intervenir face à un crime réalisé sur Internet.

> On reçoit souvent des plaintes face à des crimes mais on est confronté à l'aspect de la juridiction (Pierre, SQ).

Deuxièmement, une activité réalisée via Internet implique souvent des équipements informatiques situés à l'étranger et peut donc être considérée comme une activité à caractère international. Est-ce que la GRC doit donc enquêter tous les crimes liés à Internet parce qu'ils sont de nature internationale ? En théorie, la GRC peut s'approprier la plupart de ces enquêtes puisqu'elle est mandatée pour enquêter les crimes internationaux.

Présence policière modeste et prévisible

Nous avons observé l'existence d'un décalage entre la présence des policiers et celle des « cyber-délinquants » sur Internet. Alors qu'on trouve des délinquants informatiques d'une même région sur Internet à toute heure du jour et de la nuit et ce, tous les jours de la semaine, les policiers qui naviguent sur Internet sont peu nombreux et y naviguent habituellement les jours de la semaine entre 7h00 et 17h00. C'est donc dire que la

présence policière sur Internet, contrairement à celle des « cyber-délinquants », est actuellement modeste et prévisible.

Inexpérience des gestionnaires policiers face aux enquêtes sur Internet

Les interviewés estiment que les gestionnaires, parce qu'ils ignorent la nature d'Internet et le travail des unités spécialisées en criminalité informatique, comprennent mal leurs besoins. Notamment en matière de formation et de ressources matérielles.

> Ils ne comprennent pas que l'on soit souvent en formation et que l'on ait besoin de formations supplémentaires (Yan, GRC).

De plus, les policiers de ces unités éprouvent parfois plus de difficulté que ceux d'autres unités spécialisées lorsqu'ils doivent convaincre leurs gestionnaires du bien-fondé de certaines de leurs enquêtes.

> Mais tu peux dire qu'est-ce que c'est prendre la ligne d'un modem. Ça fait quoi dans la vie ça ? À qui ça fait mal. Oui, mais si ce propriétaire là ainsi que ses 50 employés qui génèrent 200 000$ de revenu par semaine ne peut plus opérer son commerce pendant une semaine (Luc, GRC).

Toutefois, leur gestionnaire immédiat, le sous-officier en charge de leur unité, connaît mieux leur travail et leurs besoins. C'est d'ailleurs lui qui tente habituellement de convaincre les gestionnaires supérieurs du bien-fondé de leurs requêtes.

Selon ce membre du SPCUM, cette situation s'explique par le fait qu'il s'agit d'une nouvelle criminalité contre laquelle les corps policiers ne sont pas encore habitués à lutter.

> Il y a des milliers d'années que la première tape dans le visage a été donnée. On a eu le temps d'analyser le phénomène, d'analyser les comportements et de mettre en place une structure pour réagir à cette situation et la prévenir. En trois ans on n'a pas eu le temps de cerner tous les problèmes reliés à Internet (Dominique, SPCUM).

Inexpérience des collègues de travail

Les autres policiers de l'organisation peuvent également, par inadvertance, compliquer la tâche des interviewés.

> Tu as des policiers qui arrivent sur une scène de crime et qui ne savent pas quoi faire. Il y en a d'autres qui pensent connaître ça parce qu'ils ont un ordinateur à la maison. Mais je tente de faire comprendre à tous que l'ordinateur fait partie de la scène de crime et qu'il ne faut pas y toucher (André, SQ).

Manque de collaboration et de coordination entre les organisations policières

De façon générale, les délinquants informatiques s'échangent des informations sur leurs activités par le biais de sites Web, de forums de discussion ou encore de bavardoirs dédiés à la piraterie informatique. De leur côté, les interviewés, quoiqu'ils collaborent entre eux, s'échangent tout de même moins d'informations que ne le font les pirates informatiques.

De plus, les unités doivent constamment justifier leurs budgets par le biais de statistiques sur leurs activités. Cette situation n'incite pas leurs membres à partager des information de peur que d'autres unités n'utilisent ces informations à leur avantage.

Manque de standardisation dans les enquêtes de crimes informatiques

L'absence de standard, notamment au niveau des connaissances techniques, des procédures et des outils utilisés complexifie la collaboration avec les autres unités, les acteurs du secteur privé et ceux du système judiciaire. Les policiers interviewés tentent d'établir de tels standards.

> On tente de standardiser les équipements que les unités des divers corps policiers utilisent. On voudrait utiliser des méthodes d'opération identiques pour qu'on arrive à la cour et qu'un gars du SPCUM, un gars de la Sûreté du Québec ou un gars de la GRC procède de la même façon (François, GRC).

Ressources humaines, monétaires et matérielles

Les enquêtes sur le Net exigent des ressources humaines, monétaires et matérielles importantes. Or, les corps policiers subissent d'importantes compressions budgétaires qui forcent les gestionnaires de ces unités à faire des choix difficiles quant à l'allocation des ressources.

> Les budgets sont serrés et il n'y a pas d'argent et il n'y en aura pas pour bientôt. Alors il faut identifier la priorité. Tu as du matériel à acheter mais tu as aussi des opérations à effectuer (François, GRC).

De plus, aucun budget n'est alloué directement aux unités spécialisées en criminalité informatique. Celles-ci doivent donc justifier leurs besoins auprès des instances qui les chapeautent et qui contrôlent les budgets.

> On n'a aucun budget pour acheter du matériel. L'argent est centralisé à la section de l'informatique et je dois leur soumettre mes besoins (section des achats informatiques) et les justifier (François, GRC).

Un interviewé souligne qu'à l'inverse des corps policiers, les groupes criminels organisés n'ont aucun problème de ressources.

> C'est important parce que les criminels ont les moyens de se payer les meilleurs experts et d'acheter le meilleur équipement (Dominique, SPCUM).

Augmentation constante de la charge de travail de ces policiers

Notre observation participante de quelques mois à la Sûreté du Québec confirme l'augmentation de la charge de travail de l'unité spécialisée en criminalité informatique de ce corps policier. Nos entretiens avec les membres d'autres unités révèlent que le phénomène se réalise dans les trois organisations examinées.

Les membres des unités sont fréquemment affectés à d'autres tâches

Dans ce champ d'intervention, il est particulièrement important de préserver l'expertise en maintenant chaque enquêteur en place le plus longtemps possible. Ainsi il y a un

problème avec le système actuel de promotion dans les corps policiers examinés puisqu'il incite le policier de carrière à changer fréquemment de poste et d'unité.

Les unités investissent peu dans la recherche et le développement

Les ressources humaines et monétaires limitées ainsi que la charge de travail importante, empêchent ces policiers de se familiariser avec de nouveaux outils et de nouvelles méthodes de travail.

> On a pas le temps de regarder les nouvelles choses qui apparaissent sur Internet et de faire de la recherche et du développement (Yan, GRC).

La coopération avec le secteur privé est limitée

Les unités examinées ont des besoins particuliers auxquels les spécialistes du secteur privé peuvent difficilement répondre.

> Il faut pouvoir régler les problèmes techniques qu'on rencontre nous-même, car on téléphone aux techniciens et ils disent qu'ils n'ont jamais rencontré quelqu'un qui veut faire ça de la façon dont on veut faire les choses (Luc, GRC).

Ajoutons à cela que le secteur privé hésite à investir dans la recherche et le développement de techniques et d'outils pour ces unités spécialisées puisqu'il s'agit d'un marché restreint et donc peu lucratif.

Les organisations policières s'adaptent lentement

À certains égards, les organisations policières réagissent lentement. Notamment lorsqu'il est question d'acheter des équipements et lorsqu'il faut communiquer avec une autre organisation policière par les voies officielles.

> J'ai commencé mon enquête de deux façons. Par la voie hiérarchique normale, via Interpol, et par une autre source qui m'a donné le nom de l'enquêteur en charge du dossier en moins de 24 heures. Par la voie hiérarchique j'ai attendu 15 jours pour avoir la même information (André, SQ).

Finalement, parmi l'ensemble des obstacles auxquels sont confrontés les policiers qui interviennent sur Internet, certains sont liés aux caractéristiques du monde informatique.

5.2.3 Obstacles liés aux caractéristiques du monde informatique

Cette catégorie regroupe les obstacles qui découlent directement des caractéristiques du monde informatique ou des caractéristiques d'Internet.

L'évolution rapide du monde informatique

Comme nous l'avons mentionné, l'évolution rapide de l'informatique exige le renouvellement fréquent des équipements et des connaissances des policiers.

> C'est frustrant de voir que la technologie évolue si rapidement. Tu n'as pas le temps de capitaliser les connaissances que tu viens d'acquérir que tu dois en acquérir de nouvelles (Dominique, SPCUM).

En plus de maîtriser les nouvelles technologies, les policiers doivent intervenir sur les vieux équipements qu'ils rencontrent occasionnellement dans leurs interventions.

> Tu ne peux pas te débarrasser de tes vieux équipements. Je fais une perquisition et je trouve un ordinateur récent et j'en fais une autre ailleurs et je trouve un bon vieux 8088 XT avec des disquettes 5"¼ (Pierre, SQ).

Certains dossiers exigent la combinaison de plusieurs techniques d'enquête

Une intervention liée à Internet peut nécessiter l'utilisation de techniques d'enquête spéciales, propres à Internet, en plus de techniques d'enquête traditionnelles ce qui complexifie le travail des policiers.

> Dans des opérations, la ligne téléphonique est écoutée et quand il y a un transfert de matériel pornographique, simultanément, des policiers, enfoncent la porte ou observent les lieux et prouvent que la personne est toute seule. On revient aux méthodes traditionnelles (Pierre, SQ).

Internet est trop vaste pour être patrouillé de façon proactive

Internet est un immense réseau informatique qui offre plusieurs services et où des centaines de millions d'internautes s'échangent des informations et s'adonnent à des activités variées. Les policiers peuvent difficilement être proactifs dans un univers si vaste et se contentent donc, la plupart du temps, de réagir aux plaintes formulées.

Les enquêtes liées à Internet sont généralement longues

Certaines étapes de ces enquêtes, comme l'analyse du contenu d'un ordinateur, sont longues à compléter.

> Aujourd'hui, les disques durs contiennent tous trois gigabytes d'informations. Le grand monument à Washington, l'espèce de pyramide de 300 à 400 pieds de haut, bien trois gigabytes d'informations, en feuilles de papier ça donne la hauteur de ce monument (Yan, GRC).

Chaque nouvelle génération d'ordinateurs permet d'ailleurs d'emmagasiner de plus en plus d'informations.

> Les ordinateurs deviennent de plus en plus gros et on peut y entreposer un nombre extraordinaire d'informations. C'est astronomique (Pierre, SQ) !

De plus, il appert qu'il est difficile d'identifier l'ampleur d'une enquête lorsqu'elle débute et cela complique la tâche des gestionnaires au niveau de la planification des dossiers et de l'allocation des ressources humaines.

Les entreprises hésitent à rapporter leur victimisation

Les entreprises hésitent à porter plainte de peur de perdre la confiance de leurs clients et actionnaires ou d'attirer l'attention d'autres délinquants.

> Si tu sais que ta banque est victime d'un pirate informatique, tu vas te demander pourquoi tu laisserais ton argent à cette banque (Pierre, SQ).

Ce membre de la GRC abonde dans le même sens :

> Souvent la victime ne peut pas porter plainte [...] Ça va causer des préjudices parce que la banque cherche à établir une distance entre elle et les clients en offrant des services à distance. Elle peut ainsi engager moins de personnel et ses succursales sont moins achalandées. Alors si les pirates entrent là-dedans et font de la magouille, les banques vont perdre leur réputation (Serge, GRC).

Bien sûr, on tente d'inciter les entreprises victimes à porter plainte.

> C'est un énorme problème, parce que dans notre système de justice, quand il n'y a pas de victime, il n'y a pas de crime et il n'y a pas de cause. On fait notre possible pour convaincre les gens que c'est un devoir civique de porter plainte. Comme un bon citoyen corporatif ou un autre citoyen (Serge, GRC).

La dénonciation des criminels informatiques est importante pour ces unités puisque l'intervention policière sur Internet est essentiellement réactive et qu'elle dépend donc des plaintes formulées par les organisations et internautes.

Les délinquants peuvent demeurer anonymes sur Internet

Il peut être ardu d'identifier un individu qui s'adonne à une activité illicite sur Internet.

> On le voit du côté de la criminalité et du commerce de la pornographie infantile. C'est possible d'identifier le contenu mais ce n'est pas toujours évident d'identifier l'expéditeur et le récepteur (Pierre, SQ).

Des sites Web et des logiciels spécialisés, accessibles gratuitement, permettent même de naviguer sur Internet tout en demeurant anonyme.

> Il y a des sites Web comme Hotmail.com où tu t'enregistres et ton courrier électronique est acheminé sous n'importe quel faux nom sans dévoiler ta véritable identité (Luc, GRC).

Un criminel soucieux de demeurer anonyme ou dont les activités délinquantes actuelles ou passées l'empêchent de s'abonner chez un fournisseur Internet peut devenir son propre fournisseur.

> Tu peux avoir ton serveur dans le sous-sol de ta maison et avoir ton lien direct avec Internet sans passer chez un fournisseur Internet (Luc, GRC).

Les corps policiers éprouvent de la difficulté à obtenir la coopération de ces petits fournisseurs Internet puisqu'ils n'ont pas beaucoup de personnel ou simplement parce qu'ils ne désirent pas coopérer.

L'encryptage et la stéganographie

Les criminels utilisent des logiciels d'encryptage et de stéganographie, distribués gratuitement sur Internet, pour rendre illisibles ou invisibles les messages et fichiers qu'ils s'échangent.

> La stéganographie permet d'envoyer un message à l'intérieur d'un autre médium. Ton message est caché à l'intérieur d'un fichier image ou d'un autre médium. [...] Les bandits commencent à se servir de ça (André, SQ).

Internet est difficilement contrôlable

Internet est beaucoup plus difficile à contrôler que les moyens de communication traditionnels.

> Le gros problème avec le contrôle d'Internet c'est de savoir qui va l'exercer ! On peut contrôler la presse écrite. On peut contrôler ce qui est imprimé à Montréal. C'est facile à contrôler ça se passe ici. Mais sur Internet c'est quoi la juridiction ? (Pierre, SQ)

Ce sont la structure et le fonctionnement d'Internet qui rendent difficile le contrôle des informations qui y circulent.

> C'est bien beau d'empêcher ça en Allemagne mais les Allemands, avec Internet, ils vont aller chercher ça ailleurs. Pas besoin de passer par un fournisseur Internet en particulier. Il n'y a aucune frontière sur Internet et si une personne ne peut pas t'en fournir, tu vas en voir une autre (Serge, GRC).

Le contrôle d'Internet est actuellement laissé au bon vouloir de chacun.

> Internet c'est laissé au bon vouloir de chacun. C'est laissé à la bonne volonté de ceux qui offrent le service (Pierre, SQ).

Face à cette situation, un interviewé propose deux solutions. D'abord, la mise en place d'une législation internationale spécifique à Internet :

> Il faudrait peut-être penser à un système de contrôle qui soit international à ce moment-là. Ça serait une législation internationale comme il y en existe ailleurs. Comme par exemple les lois au niveau de la circulation aérienne (Pierre, SQ).

Ensuite, l'adoption volontaire, par les acteurs impliqués dans la gestion et le développement d'Internet, d'un code d'éthique :

> Oui, mais ce qui pourrait être fait d'abord ce serait un code moral ou d'éthique de base. Si le code d'éthique est respecté par les fournisseurs de services c'est déjà quelque chose (Pierre, SQ).

Ce membre de la GRC estime que le secteur privé craint la mise en place d'une réglementation gouvernementale et que, pour l'éviter, il tente de s'auto-réglementer.

> Ils (fournisseurs Internet) ne veulent pas que le gouvernement réglementent Internet. Donc ils se sont auto-réglementés pour montrer au public qu'ils faisaient quelque chose et pour démontrer leur bonne foi (Luc, GRC).

Cette auto-réglementation consiste principalement en la mise sur pied et l'adoption volontaire, par certains acteurs du secteur privé, notamment les fournisseurs de services Internet, de code d'éthique corporatif.

Tout au long des entretiens, les policiers mentionnent à plusieurs reprises que leur charge de travail est élevée. Notre observation participante confirme cette réalité et nous approfondissons ce thème dans la section suivante.

5.3 Charge de travail

Les enquêteurs affirment tous que leur charge de travail n'a cessé d'augmenter depuis la mise sur pied de leur unité.

> Au tout début, on avait un nombre raisonnable de dossiers. Il n'y en avait pas beaucoup. Mais avec la venue d'Internet on réalise que l'informatique occupe un rôle de plus en plus grand dans la société et ce, tant auprès des particuliers que des compagnies. Alors il y a beaucoup plus d'enquêtes et le volume du support n'a pas cessé de croître parce que maintenant ce ne sont pas seulement 20, 30, ou 50% des compagnies qui ont des ordinateurs, mais presque 100% (Luc, GRC).

La charge de travail actuelle est telle que certains policiers de la GRC et de la Sûreté du Québec affirment qu'ils ne font que répondre aux urgences.

> Depuis septembre, on est trois enquêteurs avec un sergent et on est encore débordé. Alors ce n'est pas le manque d'ouvrage qu'on a ici, c'est le manque de personnes (Serge, GRC).

> Il y a assez d'ouvrage pour libérer des gens à temps plein sur ça. On a beaucoup d'ouvrage et ça va aller en augmentant. C'est pour ça que je te dis que l'équipe ne peut que grossir. Elle ne pourra pas être enlevée (Martin, SQ).

Cet enquêteur de la GRC estime d'ailleurs qu'Internet joue un rôle important dans l'accroissement de cette charge de travail.

> On enquête des crimes informatiques et le nombre d'enquêtes ne fait qu'augmenter et s'accroître. Et Internet est un facteur important dans ça (Luc, GRC).

Environ 50% du travail effectué par l'unité du SPCUM est lié à Internet.

> C'est difficile de te donner un pourcentage mais je dirais qu'environ 50% de notre travail touche Internet d''une façon ou d'une autre (Dominique, SPCUM).

Toujours au SPCUM, près de la moitié des dossiers relatifs à Internet portent sur les activités à caractère pédophile sur le Net.

> On a environ 27% de notre travail qui tourne alentours de la pédophilie parce que c'est un problème (Dominique, SPCUM).

La charge de travail des unités de la GRC diffère puisqu'elle se partage entre le support aux enquêteurs et les enquêtes informatiques.

> Le support représente environ 70% de notre travail et le 30% restant va aux enquêtes. À Montréal ça semble être différent, parce qu'eux ils font l'inverse. Environ 30% pour le support et 70% pour les enquêtes (Luc, GRC).

Parce qu'ils sont débordés, les interviewés sont à la merci des imprévus qui bouleversent leur planification et, par conséquent, celle des enquêteurs qui requièrent leur assistance.

> Je travaillais sur un dossier et un enquêteur qui travaille aux crimes contre la personne m'a donné un dossier urgent parce que l'accusé est en dedans et il y a des procédures en marche. Son dossier est devenu prioritaire et j'ai laissé l'autre de côté. Mais il peut en arriver un autre et un autre (Martin, SQ).

Par exemple, une perquisition inattendue peut ajouter plusieurs jours de travail à un horaire déjà chargé.

> Une perquisition peut générer une semaine de travail. Donc si j'en fais trois ou quatre en ligne [...] (Luc, GRC).

Cette charge de travail élevée force les unités à sélectionner soigneusement les dossiers qu'elles traitent.

> Je suis forcé de dire à mon superviseur que je ne peux pas faire certains dossiers. Parce que je ne peux pas faire huit dossiers à la fois (Vincent, GRC).

Cette charge de travail amène également les unités de différents corps policiers à se prêter occasionnellement main-forte dans les dossiers d'envergure.

Finalement, parce qu'ils sont surchargés, les policiers n'ont pas le temps d'assurer un suivi des dossiers. Une fois une enquête terminée, ils ne peuvent se permettre de vérifier, quelques mois plus tard, si les individus appréhendés sont à nouveau actifs.

> Maintenant les babillards existent encore, mais on a tellement de travail qui s'est ajouté que je ne suis pas retourné voir au niveau des babillards (Luc, GRC).

Les pages suivantes détaillent comment les interviewés utilisent Internet au travail.

5.4 Utilisation d'Internet

Nous n'avons pas recueilli beaucoup d'informations quant à l'utilisation personnelle que ces policiers font d'Internet. Comme nous l'avons mentionné, les entretiens ont été réalisés dans le milieu de travail des interviewés. Cette situation semble avoir orienté le discours des interviewés vers leur utilisation professionnelle d'Internet. On peut toutefois croire, si l'on se base sur leur opinion d'Internet, que la plupart d'entre eux ne naviguent pas beaucoup dans le cyberespace à la maison.

Au travail, les interviewés utilisent Internet comme outil de communication ainsi que comme source d'informations.

5.4.1 Internet comme outil de communication

Pour ces policiers, il ne fait aucun doute qu'Internet est un excellent outil de communication qui leur permet notamment de correspondre avec des collègues partout dans le monde.

> On ne s'aventure pas beaucoup sur Internet mais on l'utilise beaucoup pour communiquer avec d'autres corps policiers à travers le monde (André, SQ).

5.4.2 Internet comme source d'informations

Il n'est pas rare que ces policiers réalisent des recherches sur Internet pour trouver la solution à un problème technique auquel ils sont confrontés.

Parmi les thèmes examinés dans le cadre de notre sous-objectif sur les expériences, points de vue et pratiques des interviewés, nous trouvons l'opinion qu'ont ceux-ci de leur travail.

5.5 Points de vue sur leur travail

La majorité des interviewés ont un intérêt marqué pour l'informatique.

> Je suis une personne qui a tendance à être logique dans ses pensées et l'informatique c'est très logique, donc j'avais ça dans mes affinités et j'ai développé ça (Luc, GRC).

Par conséquent, ils se considèrent chanceux de pouvoir travailler dans ce domaine. La plupart ont d'ailleurs réalisé des sacrifices pour obtenir ou conserver un poste dans ce champ d'intervention.

> Je suis chanceux car je peux joindre l'utile à l'agréable puisque je suis payé pour faire ça et c'est mon travail. J'ai laissé tomber bien des choses pour continuer mon travail, dont deux promotions à Montréal. J'ai laissé passer ces promotions parce que j'aime bien mon travail (Luc, GRC).

Ces policiers sont également fiers d'être des « pionniers » dans un champ d'intervention encore jeune.

> À la GRC, on ouvre un nouveau champ d'intervention, un nouveau chemin. Il y a à peine quelques années, l'informatique ça n'était pas beaucoup exploré (Luc, GRC).

Malgré les ressources limitées et les autres irritants, les interviewés estiment que leur travail est apprécié à sa juste valeur par les gestionnaires.

> C'est plaisant parce que tu travailles et tes supérieurs sont conscients de tes besoins et ils font ce qu'ils peuvent avec ce qu'ils ont. Donc c'est encourageant dans le travail qu'on fait. Au moins l'avenir est intéressant (Martin, SQ).

Ces policiers ne se perçoivent pas comme des spécialistes en informatique mais plutôt comme de simples policiers qui ont des connaissances plus approfondies en informatique.

> Je ne suis pas un expert en informatique mais une personne ressource en informatique. Ça fait peut-être 8 ou 10 ans que je suis en informatique. J'ai 40 ans donc ça veut dire que j'ai commencé à l'âge de 30 ans. Il y a des gens qui s'intéressent à l'informatique depuis l'âge de 12 ans (Luc, GRC).

Parmi les insatisfactions énoncées par les interviewés face à leur travail, on trouve les sentences données aux individus qu'ils appréhendent.

> Mon travail c'est d'amener des causes à la cour. Je ne peux pas me fâcher contre le jugement. Parce que quelqu'un n'aura jamais la sentence que tu penses mais ce n'est pas ma faute. Toi tu es la première ligne du front. Tu vois tout circuler et tu vois que le petit gars c'est un vaurien mais on ne peut pas le juger sur ça (Serge, GRC).

Un policier de la Sûreté du Québec souligne également cette frustration.

> On ne peut pas être enquêteur, procureur et juge. On ne peut pas prendre la Justice dans nos mains comme ils disent. Reste que la justice je trouve qu'elle a de la difficulté parfois (André, SQ).

5.6 Sommaire

Même si quelques interviewés ont une opinion positive d'Internet, ce n'est pas le cas de la majorité d'entre eux. Pour ceux-ci, Internet est un univers où les criminels peuvent à la fois réaliser des crimes « conventionnels » et des crimes d'un nouveau genre. Ils considèrent Internet comme un univers difficilement contrôlable où circulent des informations problématiques et estiment que les relations interpersonnelles vécues sur le Net sont « fausses » et superficielles.

Ces policiers spécialisés sont confrontés à plusieurs obstacles lors dans leurs interventions sur Internet. Ceux-ci peuvent être classés à l'intérieur de trois groupes distincts : les obstacles liés au système judiciaire et/ou d'ordre législatif, les obstacles inhérents aux organisations policières ainsi que les obstacles liés aux caractéristiques du monde informatique.

Parmi les obstacles inhérents aux organisations policières, on mentionne la charge de travail élevée des unités spécialisées en criminalité informatique. La charge de travail actuelle de certaines d'entre elles est telle qu'elles ne peuvent répondre qu'aux urgences. Certains interviewés croient qu'Internet est le principal responsable de cette charge de travail élevée et tous estiment qu'elle augmentera encore dans les années à venir.

Les policiers interviewés utilisent le courrier électronique pour communiquer avec des amis et des collègues de travail et naviguent sur Internet pour obtenir des informations et des solutions à des problèmes techniques qu'ils rencontrent au travail. Bien que ces policiers semblent utiliser plus fréquemment Internet au travail qu'à la maison, il est possible que la réalisation des entretiens dans le milieu de travail ait indirectement orienté leur discours l'utilisation professionnelle d'Internet.

Même s'ils ne sont pas de fervents internautes, la plupart des membres de ces unités spécialisées ont un intérêt marqué pour l'informatique en général. C'est pourquoi ils se considèrent tous chanceux de travailler dans ce domaine. Cette vision positive de leur travail semble d'ailleurs leur permettre de faire face plus aisément aux obstacles qu'ils rencontrent. Ils se considèrent également comme des pionniers puisqu'ils sont parmi les premiers policiers à œuvrer dans ces unités spécialisées.

Conclusion

6 Conclusion

En utilisant une méthodologie qualitative, nous avons tenté d'appréhender le processus d'organisation des corps policiers canadiens et québécois par rapport à Internet. Les techniques de recherche utilisées, c'est-à-dire les entretiens semi-directifs, l'observation participante et l'analyse documentaire, nous ont procuré des informations sur ce processus ainsi que sur les expériences, points de vue et pratiques des policiers qui en sont les principaux maîtres d'œuvre.

La quasi-absence de littérature sur notre objet d'étude confère à notre démarche un caractère exploratoire et rend d'autant plus intéressantes les conclusions de nos analyses.

Pour tous les corps policiers examinés, l'organisation face à Internet s'inscrit à l'intérieur d'un processus d'organisation encore plus vaste, qui porte sur la criminalité informatique. À l'heure actuelle, ce double processus repose principalement entre les mains des quelques policiers qui œuvrent dans les unités spécialisées en criminalité informatique.

Le processus d'organisation par rapport à Internet en est encore à ses premiers pas dans les corps policiers que nous avons examinés et prend actuellement deux formes. D'une part il y a la mise sur pied de sites Web corporatifs où l'on affiche des informations générales sur les organisations. D'autre part, des unités capables d'appuyer les policiers dans les enquêtes liées à l'informatique et à Internet sont créées. En plus de supporter les interventions policières sur Internet, certaines de ces unités enquêtent sur des crimes relatifs à Internet. Cependant, la charge de travail élevée de ces unités limite leur capacité à initier des enquêtes de leur propre chef ; elles doivent habituellement se contenter de donner suite aux plaintes qu'elles reçoivent.

Il s'agit donc d'un processus d'organisation par rapport à Internet qui, pour le moment, est essentiellement réactif et qui ne répond qu'aux besoins les plus pressants de ces organisations policières. Cette situation s'explique en partie par les ressources limitées

dont disposent les corps policiers. Pour aller de l'avant dans ce processus d'organisation, ceux-ci doivent investir d'importantes ressources humaines, monétaires et matérielles dans ces unités spécialisées. Or, les corps policiers traversent actuellement une période de compressions budgétaires et c'est peut-être ce qui explique qu'ils ne cherchent qu'à répondre aux besoins les plus pressants.

Les ressources limitées dont disposent ces unités ont également des répercussions sur leur fonctionnement. Parce qu'elles ont des effectifs modestes et qu'elles font face à une importante charge de travail, ces unités doivent sélectionner avec soin les enquêtes où elles interviennent et celles qu'elles initient tout évitant les faux pas au niveau juridique. À l'heure actuelle, cette sélection des dossiers ne repose sur aucun critère officiel, si ce n'est le mandat et la juridiction de chacune des organisations policières. Les membres de ces unités se basent plutôt sur des critères extralégaux pour effectuer cette sélection, par exemple, la collaboration de la victime, les chances de réussite de l'enquête ou l'ampleur des dommages causés.

L'analyse du discours des interviewés ainsi que les informations obtenues par le biais de notre observation participante, nous font croire que ce processus d'organisation par rapport à Internet ne sera jamais réellement terminé. Internet, tout comme un organisme vivant, évolue continuellement et les corps policiers seront, malgré eux, confrontés tant à de nouvelles problématiques qu'à de nouvelles possibilités d'utilisation du cyberespace. Lors des entretiens, les policiers ont mentionné le développement imminent du commerce électronique sur Internet et selon eux, cela laisse présager l'apparition prochaine de crimes liés à cette nouvelle activité commerciale. Non seulement les forces policières devront s'adapter à la criminalité conventionnelle traditionnellement associée au commerce mais elles devront en plus faire face à des formes de criminalité innovatrices et actuellement méconnues.

Les corps policiers examinés entretiennent de bonnes relations entre eux ainsi qu'avec les différents acteurs qu'ils côtoient dans leurs interventions sur Internet. Il existe une

certaine solidarité entre les différentes unités spécialisées en criminalité informatique. Elle permet parfois aux membres de ces unités de contourner des problèmes tels le manque de ressources ou d'expertise. Les relations avec les acteurs du secteur privé, sont également bonnes et il est primordial qu'elles le demeurent puisque la collaboration du secteur privé est essentielle à la réussite de la majorité des enquêtes liées à Internet.

Quant aux expériences, points de vue et pratiques des policiers au cœur de ce processus d'organisation, l'analyse des entretiens révèle que la plupart d'entre eux ont une opinion plutôt négative d'Internet. Ils admettent cependant que leur travail les expose aux facettes les plus sombres d'Internet et que cela influence probablement leur vision du cyberespace.

Tous ces policiers sont également confrontés à plusieurs obstacles qui compliquent considérablement leurs interventions sur Internet.

Ces obstacles sont liés au système judiciaire, aux organisations policières elles-mêmes ainsi qu'aux caractéristiques du monde informatique. Certains obstacles propres au système judiciaire pourraient être éliminés en sensibilisant ses acteurs face aux usages problématiques. Ceux-ci pourraient par exemple être initiés à la navigation sur Internet ou assister à une démonstration, en direct, de certaines activités problématiques réalisées sur le réseau Internet.

Bien que le travail de ces policiers soit exigeant, ceux-ci affirment aimer ce qu'ils font et tous travaillent dans ce domaine par choix. Certains ont même refusé des promotions afin de conserver leur travail. Ces policiers sont, pour la plupart, des amateurs d'informatique et se considèrent comme des pionniers de ce nouveau champ d'intervention policière.

Finalement, à la lumière des analyses réalisées dans le cadre de ce mémoire, deux commentaires s'imposent. D'une part, nous avons observé que les corps policiers qui

s'organisent par rapport à Internet, utilisent peu le réseau. Une telle situation a deux impacts, lesquels sont intimement reliés. Premièrement, les corps policiers ne tirent pas pleinement profit du potentiel d'Internet. Deuxièmement, puisqu'ils connaissent peu Internet, les policiers sont peu compétitifs dans la lutte aux usages problématiques de ce nouvel environnement.

À cet égard, les corps policiers gagneraient à explorer les multiples utilisations possibles d'Internet et à être proactifs dans le cyberespace. Pour ce faire, les gestionnaires policiers doivent promouvoir l'exploration et l'utilisation d'Internet en fournissant les ressources financières nécessaires à la formation. Les enquêteurs des autres escouades auraient aussi intérêt à se familiariser avec Internet puisque la criminalité traditionnelle est appelée à se déplacer vers cet univers virtuel.

D'autre part, il serait pertinent de réaliser une analyse descriptive approfondie des diverses activités criminelles présentes sur le réseau Internet. Les gestionnaires policiers, armés d'une telle analyse, pourraient mieux harmoniser les ressources affectées au processus d'organisation par rapport à Internet. En ce sens, une évaluation plus adéquate des coûts associés à cette criminalité permettrait une allocation adaptée des ressources humaines, monétaires et matérielles. Une telle analyse constituerait d'ailleurs un intéressant projet de recherche très actuel.

Bibliographie

7 Bibliographie

Abitbol, E., Faucon, B. (Page consultée le 11 décembre 1999). La cyberdépendance, mythe ou réalité ? [En ligne]. Http://www.planete.com/archives.html

Agence de presse Reuter. (31 août - dimanche 1er septembre 1996). Des « cyber-flics » aux trousses des pédophiles virtuels. Le Devoir, p. A9..

Barret, D., J. (1996) Bandits on the Information Superhighway. Bon Ger : O'Reilly & Associates.

Bissio, R. (1994). Nouvelles armes pour les démocrates. LE MONDE diplomatique, Manière de voir Hors-série : Internet, l'extase et l'effroi, 42-44.

Boutin, G., (1997). L'entretien de recherche qualitatif. Sainte-Foy : Presses de l'Université du Québec.

CAIP. (Page consultée le 28 octobre 1999). Canadian Association of Internet Providers, [En ligne]. http://www.caip.ca

CANARIE. (Page consultée le 28 octobre 1999). CANARIE, [En ligne]. http://www.canarie.ca/index_f.html

Carlander, I. (1996). Aux avant-postes du cybermonde. LE MONDE diplomatique, Manière de voir Hors-série : Internet, l'extase et l'effroi, 42-44.

Cassius de Linval, R. (7 novembre 1996) Profession : cybercop. Voir, p. 73.

Cassius de Linval, R. (24 octobre 1996). Vie privée et cookies : Des biscuits indigestes. Voir, p. 14.

Collège canadien de police. (Page consultée le 11 décembre 1999). Collège canadien de police, [En ligne]. http://www.cpc.gc.ca/

Colombain, J. (1996). Internet. Toulouse : MILAN.

Conseil de la radiodiffusion et des télécommunications canadiennes. (Page consultée le 9 décembre 1999). Bienvenue au CRTC, [En ligne]. http://www.crtc.gc.ca/

CRIM. (Page consultée le 4 mai 1999). Centre de recherche informatique de Montréal, [En ligne]. http://www.crim.ca

Denning, D., E. (1995). Crime and Crypto on the Information Superhighway. Journal of Criminal Justice Sciences, 6 (2) p. 323336.

Dufour, A. (1996). Internet. (2e éd). Paris : PUF.

Duncan, M. (novembre 1997) Lutte contre la criminalité sur l'inforoute. La Gazette de la GRC, 59 (10), p. 4-12.

École de criminologie. (Page consultée le 3 novembre 1999). Faculté des Arts et des Sciences, [En ligne]. http://www.fas.umontreal.ca/CRIM

Electronic Frontier Canada. (Page consultée le 17 septembre 1999). Electronic Frontier Canada, [En ligne]. http://insight.mcmaster.ca:80/org/efc/efc.html

Electronic Frontier Foundation. (Page consultée 12 septembre 1999). Electronic Frontier Foundation, [En ligne]. http://www.eff.org

Eudes, Y. (30 juin 1997). Vies privées à vendre sur le réseau. Le Devoir, p. B4

Forde, P., Patterson, A. (1998). Paedophile Internet Activity. Trends & Issues in crime and criminal justice, 97, p. 1-6.

Fortin, M., F., Taggart, M., E., Kérouac, S., Normand, S. (1988). Introduction à la recherche. Montréal : Décarie.

Francescon, O. (1996). Les nouvelles techniques d'information et de communication et leur exploitation à des fins illicites. Revue internationale de criminologie et de police technique, XLIX, p. 61-68.

Gingras, M. (14 novembre 1996). Zone X : De la personne au profil. Voir, p. 42 (?).

Gouvernement du Québec, Office de la langue française (1995). Vocabulaire d'Internet. Montréal: Office de la langue française.

Grabosky, P., Smith, R. G., Wright, P. (1998). Nouvelles technologies, nouveaux délits. Les cahiers de la sécurité intérieure, (34), 13-29.

GRC. (Page consultée le 28 octobre 1999). La criminalité informatique et en matière de télécommunications, [En ligne]. http://www.rcmp-grc.gc.ca/html/informat.htm

Griffin, M. (1998) Internet Gambling. Crime & Justice International, 14 (18 & 19).

Hannaford, C. (1995) La criminalité perpétrée sur l'autoroute de l'information. La Gazette de la GRC, 57 (10) p. 22-24.

IDC. (Page consultée le 21 octobre 1999). Hot New Research , [En ligne]. http://www.idcresearch.com

IETF. (Page consultée le 28 octobre 1999). The Internet Engineering Task Force, [En ligne]. http://www.ietf.cnri.reston.va.us

Innovation Ressources. (Page consultée le 28 octobre 1999). Electronic Commerce, [En ligne]. http://www.innovationresources.com

Internet Society. (Page consultée le 12 juillet 1999). Internet Society, [En ligne]. http://www.isoc.org

Johnson, D. (1989). The Public-Private Status of Transaction in Computer Networks. In Goulg, C. (éds). The Information Web. (pp. 37-57).Colorado: Westview Press.

Le Devoir (1 septembre 1996). Des « cyber-flics » aux trousses des pédophiles virtuels. A9.

Nations Unies. (Page consultée le 13 décembre 1999). Nations Unies, [En ligne]. http://www.un.org/french

Next Generation Internet Initiative. (Page consultée le 22 octobre 1999). NGI Initiative Home Page, [En ligne]. http://www.ngi.gov

Nua. (Page consultée le 25 octobre 1999). New Thinking for the Digital Age, [En ligne]. http://www.nua.ie

Office de la langue française. (Page consultée le 21 octobre 1999). Office de la langue française, [En ligne]. http://www.olf.gouv.qc.ca

Office de la langue française. (Page consultée le 15 avril 2000). Office de la langue française, [En ligne]. Http://www.olf.gouv.qc.ca

Peretz, H. (1998). Les méthodes en sociologie. Paris : Éditions La Découverte.

Piragoff, D., Holthuis, A. (Page consultée le 29 septembre 1999). Les nids-de-poule de l'autoroute électronique : crimes et abus, [En ligne]. http://canada2.justice.gc.ca/cgi-bin/repere/fr/repere.cgi?corpus=http%3A%2F%2Fcanada2.justice.gc.ca%2Fcgi-bin%2Frepere%2Ffr%2Frepere.cgi&tout=autoroute+%E9lectronique&language=fr&range=39&numdoc=65

Planète Internet. (Page consultée le 2 juillet 1997). La légende high tech de la guérilla zapatiste. [En ligne]. http://www.netpress.fr/interface/SendPage.exe?ID=274

Poupart, J., Groulx, L. H., Deslaurier, J. P., Laperrière, A., Mayer, R., Pires, A. P. (1997). La recherche qualitative : enjeux épistémologiques et méthodologiques. Montréal : Gaëtan Morin Éditeur ltée

Poupart, J., Groulx, L. H., Deslaurier, J. P., Laperrière, A., Mayer, R., Pires, A. P. (1998). La recherche qualitative : diversité des champs et des pratiques au Québec. Montréal : Gaëtan Morin Éditeur ltée.

Quéau, P. (1995). Internet, média du futur. LE MONDE diplomatique, Manière de voir Hors-série : Internet, l'extase et l'effroi, 20-21.

Québec Science (1996). Internet : Le guide pratique. Montréal : Québec Science.

Quivy, R., Campenhoudt, L., V. (1988). Manuel de recherche en sciences sociales. Paris : Dunod.

Ramonet, I. (1996). Changer d'ère. Le MONDE diplomatique, Manière de voir Hors-série : Internet, l'extase et l'effroi, 6-7.

Renaud, P., Torrès, A. (1995). Une chance pour le Sud. LE MONDE diplomatique, Manière de voir Hors-série : Internet, l'extase et l'effroi, 46-48.

Réseau interordinateurs scientifiques québécois. (Page consultée le 23 mars 1998). RISQ, [En ligne]. http://www.risq.qc.ca

Réseau interordinateurs scientifiques québécois. (Page consultée le 6 avril 1998). Le réseau mondial 1 : de 1957 à 1986, [En ligne]. http://www.risq.qc.ca/info/table/vue/vue_01.html

Réseau interordinateurs scientifiques québécois. (Page consultée le 4 décembre 1999). Résultats de la quatrième enquête du RISQ sur les internautes québécois [En ligne]. http://www.risq.qc.ca/enquete/4/

Rosé, P. (1992). La criminalité informatique à l'horizon 2005 : analyse prospective. Paris : L'Harmattan

Rosnay, J. (1996). La révolution informationnelle. LE MONDE diplomatique, Manière de voir Hors-série : Internet, l'extase et l'effroi, 33-34.

Schwartz, P. (Page consultée le 14 juillet 1998). Shock Wave (Anti) Warrior. [En ligne]. http://www.wired.com/wired/archive/people/alvin_toffler/

Service de police de la Communauté urbaine de Montréal. (Page consultée le 9 décembre 1999). Sommaire, [En ligne]. http://www.spcum.qc.ca./francais/menu_f.htm

SilverStone Sofware Corp. (Page consultée le 5 décembre 1999). Protect Your Children, [En ligne]. http://www.silverstone.net/

Software & Information Industry Association. (Page consultée le 4 décembre 1999). Software & Information Industry Association, [En ligne]. http://www.siia.net/

Sous-Direction de la Sécurité Technique. (Page consultée le 4 décembre 1999). Bienvenue à la Sous-Direction de la Sécurité Technique, [En ligne]. http://www.rcmp-grc.gc.ca/tsb/index_f.htm

Spradley, J. P. (1980). Participant observation. New York : Holt, Rinehart and Winston.

Sterling, B (1992). The Hacker Crackdown. New York : Bantam Books

Sûreté du Québec. (Page consultée le 9 décembre 1999). Bienvenue, [En ligne]. http://www.suretequebec.gouv.qc.ca

Sussman, V. (2 mars 1995). Les inforoutes du crime. Courrier international, 226.

Sussman, V. (22 octobre 1995). Hate, Murder and Mayhem on the Net. U.S. News & World Report, (pages inconnues).

Telcordia Technologies. (Page consultée le 14 octobre 1999). Telcordia Technologies, [En ligne]. http://www.netsizer.com

Thibaudeau, C. (2 septembre 1995). Faire la police sur le réseau Internet. La Presse, A14.

Toffler, A., (1982) La troisième vague. Paris : Gonthier

Voir. (Page consultée le 9 décembre 1997). Surveillance des employés : Netiquette monte la garde , [En ligne]. http://www.voir.ca

World Wide Web consortium. (Page consultée le 5 août 1999). Leading the Web to its Full Potential...., [En ligne]. http://www.w3.org