

**Université de Montréal**

**La transformation des enquêtes policières due à l'influence des technologies :  
perspective d'une unité policière spécialisée en analyse judiciaire informatique**

**par David-Emmanuel Baril**

**École de criminologie, Faculté des études supérieures**

Rapport de stage présenté à la Faculté des études supérieures en vue de  
l'obtention du grade de M. Sc. en criminologie  
Option stage en analyse criminologique

Décembre, 2014

©, David-Emmanuel Baril, 2014

## **Résumé**

*La popularité des technologies de l'information et des communications entraîne l'augmentation de la preuve retrouvée sous forme numérique lors d'enquêtes policières. Les organisations policières doivent innover afin d'analyser, gérer et tirer profit de cette preuve numérique. En réponse, elles ont constitué des unités spécialisées en criminalité technologique et en analyse judiciaire informatique. La présente étude utilise les théories de l'innovation afin de déterminer comment l'évolution des technologies et des tendances en matière de criminalité technologique influencent les enquêtes et les organisations policières. Cette recherche vise à augmenter les connaissances sur ces unités spécialisées en quantifiant et en qualifiant leur travail quotidien. Avec la collaboration d'une unité policière canadienne spécialisée en analyse judiciaire informatique, une analyse détaillée des demandes d'expertise adressées à leur service a été effectuée. Les résultats indiquent une augmentation de la preuve numérique avec la prévalence de certaines formes de criminalité et de certains appareils électroniques. Les facteurs influençant le délai de traitement sont soulignés ainsi que les stratégies mises de l'avant afin de gérer efficacement l'accroissement des demandes de service. Finalement, des entrevues ont été menées avec certains membres de l'équipe afin de mettre en lumière les défis et les enjeux relatifs à l'implantation et au fonctionnement d'une telle unité. Les principaux enjeux soulevés concernent les environnements technologiques et juridiques, la formation du personnel, la gestion des ressources et les priorités organisationnelles.*

*Mots-clés : analyse judiciaire informatique, criminalité technologique, unité policière spécialisée, innovation, preuve numérique*

## **Abstract**

*The popularity of information and communication technologies resulted in an increase of the digital evidence found during police investigation. Police organizations must innovate in order to analyze, manage and benefit from those digital evidences. Accordingly, they formed highly specialised units dedicated to technological crime and computer forensic. This study uses innovation theories to determine how technology and technological crime trends influence crime investigations and police organizations. This research aims to increase knowledge of these specialized units by quantifying and qualifying their daily work. With the assistance of a Canadian computer forensic police unit, a detailed analysis of all requests for assistance directed to their service was performed. Results indicate an increase of digital evidence with the prevalence of certain types of crime and electronic devices. Factors influencing the backlog are underlined as well as strategies elaborated to effectively manage the caseload. Finally, interviews were conducted with members of the team to highlight the challenges and issues related to the implementation and operation of such unit. The main concerns raised by the unit's members were the technological and legal environments, staff training, resource management and organizational priorities.*

*Keywords: computer forensic analysis, technological crime, special police unit, innovation, digital evidence*

## **Table des matières**

Résumé.....	ii
Abstract.....	iii
Table des matières.....	iv
Liste des tableaux et des figures.....	vii
Remerciements.....	viii
Chapitre I - Introduction.....	9
Chapitre II - Recension de la littérature : Police et innovation.....	15
1. Les théories de la diffusion et de l'adoption des innovations.....	16
1.1. Les racines des théories de l'innovation.....	17
1.2. Les théories contemporaines de l'innovation.....	18
1.3. Qu'est-ce qu'une innovation ?.....	19
1.4. L'innovation : un processus cyclique.....	21
2. Les organisations et l'innovation.....	22
2.1. Le processus d'innovation dans une organisation.....	23
3. L'innovation et l'adoption des technologies dans les organisations policières.....	26
3.1. Historique des innovations adoptées par les organisations policières depuis les 150 dernières années.....	27
3.2. Les types d'innovations policières.....	32
3.3. Les facteurs favorisant l'innovation dans les organisations policières.....	32
3.4. Le cas particulier des unités spécialisées.....	35
3.5. Les conséquences de l'innovation et autres considérations.....	36
4. Résumé et application des éléments théoriques.....	38
5. Implications pour le présent projet de recherche.....	40
5.1. Caractériser le travail d'une unité spécialisée en criminalité informatique.....	42
5.2. Où se trouvent au Canada les unités spécialisées en criminalité technologique ?.....	45
5.3. Études connexes sur les unités spécialisées en analyse judiciaire informatique.....	47
5.4. Projet de stage.....	48
Chapitre III - Méthodologie.....	50
1. L'Unité spécialisée en criminalité technologique et en analyse judiciaire informatique.....	51
2. Constitution d'une base de données des demandes d'assistance.....	52
2.1. Nature et objectif de la base de données.....	52
2.2. Description générale de la base de données.....	53

2.3.	Constitution de la variable « Type de service effectué » et dérivés.....	54
2.4.	Constitution de la variable « Type d'incident ».....	56
2.5.	Constitution de la variable « La demande spécifiait-elle du matériel à analyser ? ».....	57
2.6.	Constitution de la variable « Différence entre la date de réception et de l'incident ».....	58
3.	Autres sources de données et considérations méthodologiques.....	59
3.1.	Limites et biais méthodologiques de la présente étude.....	60
Chapitre IV - Caractériser le travail d'une unité policière spécialisée en analyse judiciaire informatique.....		62
1.	Les analyses descriptives exploratoires.....	64
1.1.	Analyse générale du nombre de demandes de services adressées à l'Unité.....	64
1.2.	Analyse mensuelle du nombre de demandes adressées à l'Unité.....	68
1.3.	Analyse des types de services rendus par l'Unité.....	71
1.4.	Analyse du profil des départements adressant les demandes de service.....	74
1.5.	Analyses des demandes selon le type d'incident concerné.....	76
1.6.	Analyse du profil du matériel analysé par l'Unité.....	81
2.	Synthèse du chapitre et constatations préliminaires.....	86
Chapitre V - Les défis et les enjeux d'une unité policière spécialisée en analyse judiciaire informatique.....		88
1.	Le délai de traitement des dossiers.....	90
1.1.	Facteurs influençant le délai soulevés par les membres de l'Unité.....	90
1.2.	Analyse du délai entre la réception d'une demande et l'ouverture du dossier d'enquête.....	92
1.3.	Synthèse des facteurs influençant le délai de traitement.....	97
2.	Les facteurs exogènes : l'évolution rapide du cadre technologie et juridique.....	98
2.1.	L'évolution rapide des technologies.....	98
2.2.	La jurisprudence.....	100
3.	Les facteurs endogènes : une expertise méconnue et des ressources limitées.....	102
3.1.	La diffusion de l'expertise.....	103
3.2.	L'effet CSI.....	104
3.3.	La formation du personnel.....	105
3.4.	La gestion de ressources limitées.....	106
3.5.	Les priorités organisationnelles.....	107
4.	Synthèse du chapitre.....	108
Chapitre VI - Synthèse, réflexions et conclusion.....		110
1.	Résumé des faits saillants.....	111
1.1.	Le profil des clients de l'Unité.....	112
1.2.	La réalité d'une unité de soutien spécialisée en criminalité technologique.....	112
1.3.	La criminalité technologique.....	114

2.	L'implantation d'une unité policière spécialisée en analyse judiciaire informatique.....	115
2.1.	La redéfinition et la restructuration .....	115
2.2.	La clarification .....	117
2.3.	L'intégration aux activités routinières .....	117
2.4.	Implantation d'une unité spécialisée : un cas réel .....	118
3.	Implications pour les organisations policières et la recherche scientifique .....	119
	Références .....	124
	Annexe 1 - Présentation détaillée des variables de la base de données .....	ix
	Annexe 2 – Questionnaire destiné aux membres de l'Unité.....	xiii
	Annexe 3 – Questionnaire pour l'inspecteur d'une agence gouvernementale.....	xv

## Liste des tableaux et des figures

### Tableaux

Tableau 1 – Typologie des adeptes selon leur vitesse d'adoption des innovations .....	19
Tableau 2 – Nombre de demandes adressées par années à l'Unité selon le type de service effectué .....	71
Tableau 3 – Nombre de demandes de service par années par département demandeur .....	74
Tableau 4 – Nombre de demandes de service par années par types d'incident .....	77
Tableau 5 – Nombre et nature des périphériques traités par années .....	81
Tableau 6 – Tests bivariés non paramétriques entre le délai et six variables catégorielles .....	94

### Figures

Figure 1 – Courbe logistique normale du taux d'adoption en fonction du temps .....	18
Figure 2 – Le cycle de vie des technologies de l'information .....	21
Figure 3 – Les étapes du processus d'innovation dans une organisation .....	25
Figure 4 – Nombre de demandes de service adressées à l'Unité par année de 2004 à 2013 .....	64
Figure 5 – Nombre de demandes de service adressées à l'Unité selon le mois .....	68
Figure 6 – Histogramme du nombre de demandes de service adressées par mois à l'Unité .....	70
Figure 7 – Nombre de demandes de service adressées par années à l'Unité selon le type de service effectué .....	71
Figure 8 – Nombre de demandes de service adressées par années à l'Unité selon le département effectuant la demande .....	74
Figure 9 – Histogrammes représentant le nombre de demandes adressées par années selon le type de crime .....	78
Figure 10 – Histogrammes représentant le nombre et la nature des périphériques traités par l'Unité par années .....	82
Figure 11 – Nombre de périphériques traités par années par l'Unité .....	93
Figure 12 – Nombre de jours écoulés entre la date de l'incident et la réception d'une demande de service .....	93

## Remerciements

*Je tiens à remercier l'organisation et les membres de l'unité spécialisée qui ont bien voulu participer à ce projet. Sans leur ouverture et leur collaboration le présent projet n'aurait pas été possible. Vous avez été très généreux de votre temps et votre apport au projet est considérable.*

*Je tiens aussi à remercier mon directeur pour ses bons conseils, son écoute et son soutien moral tout au long de cette entreprise.*

*Finalement, je veux remercier ma conjointe pour son dévouement : ton appui a réellement fait la différence! Merci d'avoir partagé les difficultés reliées à ce périple.*



---

## **Chapitre I**

### **Introduction**

---

### Mise en contexte

Depuis le début des années 1990, les nouvelles technologies de l'information et des communications se sont démocratisées et ont investi nos maisons. Aujourd'hui la majorité des foyers nord-américains possède un ordinateur personnel doté d'Internet. Selon l'enquête québécoise sur l'accès des ménages à Internet de l'Institut de la statistique du Québec (Lessard & Belleau, 2013), 81,6% des ménages québécois étaient branchés à Internet en 2012. Internet et les technologies de l'information et des communications font donc partie intégrante de la vie de nombreux Québécois et Canadiens depuis plusieurs années.

Le grand dictionnaire terminologique de l'Office québécois de la langue française (2007) définit les technologies de l'information comme étant : « L'ensemble des matériels, logiciels et services utilisés pour la collecte, le traitement et la transmission de l'information. ». Cette définition inclut une large variété d'appareils électroniques que nous utilisons quotidiennement; en effet, téléphones cellulaires, ordinateurs, consoles de jeu, tablettes électroniques, liseuses et téléviseurs ont maintenant tous la capacité de transmettre et de recevoir des données par le biais des technologies sans fil.

Ces périphériques, tous interconnectés, détiennent une grande quantité d'informations concernant nos habitudes de vie et la façon dont nous interagissons avec le monde. Qui plus est, nous stockons de plus en plus de renseignements personnels et bancaires sur ces appareils électroniques. Selon l'Association des banquiers canadiens (2014), 55% des Canadiens utilisent Internet comme le principal moyen d'effectuer des transactions bancaires, comparativement à 8% en 2000.

La grande majorité des foyers canadiens possèdent un réseau sans fil connecté à Internet. Selon l'enquête québécoise sur l'accès des ménages à Internet (Lessard & Belleau, 2013), 71,4% des ménages accèdent à Internet à partir d'un ordinateur portable, 52,8% le font à partir d'un téléphone intelligent ou d'un autre appareil de poche sans fil et 22,0% à partir d'une tablette numérique. Tous ces appareils nécessitent un réseau sans fil pour accéder à Internet. Toutefois, la sécurité de ces réseaux personnels est souvent limitée aux connaissances individuelles de l'utilisateur et à l'utilisation qu'il en fait. Insuffisamment protégés, ces réseaux

peuvent constituer des cibles intéressantes pour des individus mal intentionnés (Dunham, 2005; Grabosky, 2007; Jewkes & Yar, 2013). En effet, de pair avec l'accessibilité grandissante des technologies, de plus en plus d'opportunités criminelles se présentent sur ces nouveaux médiums pour les délinquants capables de les saisir (Bossler & al., 2009; Choi, 2008; Gundenon & al., 2000; Hutchings & al., 2008; Pratt & al., 2010; Willison, 2004; Yar, 2005). Les données contenues dans nos appareils électroniques, mais aussi celles que nous confions à des organisations privées et publiques, peuvent constituer un attrait pécuniaire considérable (Baker & al., 2011; Hengst & Warnier, 2013).

Cette forme émergente de criminalité est appelée criminalité technologique, criminalité informatique ou encore cybercriminalité. Pour les besoins de ce rapport nous utiliserons le terme criminalité technologique car il revête un caractère plus général. Selon David Wall (2007) la criminalité technologique peut prendre trois (3) grandes formes : les crimes contre l'intégrité des systèmes informatiques (par exemple : le piratage informatique), les crimes assistés par ordinateur (par exemple : le vol d'identité sur Internet) et les crimes de contenu illicite (par exemple : la possession de matériel pornographique juvénile).

La criminalité technologique n'est donc pas seulement l'affaire du pirate informatique; de nos jours tous les délinquants sont susceptibles d'utiliser la technologie pour commettre un crime. Conséquemment, les enquêteurs ont maintenant un doute raisonnable que la preuve de la commission d'une acte criminel puisse se trouver en totalité ou en partie sur un appareil électronique. Le résultat de ce phénomène est une importante augmentation de la preuve numérique depuis les dix dernières années (McMillan & al., 2013; Quick & Choo, 2014; Turnbull & al., 2009); mais aussi une diversification des appareils électroniques retrouvés dans les enquêtes policières (Turnbull & al., 2009).

Une conséquence de l'augmentation de cette preuve numérique est de transformer progressivement les enquêtes policières. Les organisations policières doivent faire face à cette réalité en développant de nouvelles stratégies d'analyse et de gestion afin de présenter cette preuve, parfois très volumineuse, en Cour (Quick & Choo, 2014). Par contre, ce n'est pas la première fois que les organisations policières font face à ce genre de changement. De toutes

époques, les forces de l'ordre ont dû s'adapter à l'évolution de la criminalité et aux changements des mœurs de la société (McQuade, 2001; Seaskate, 1998; Soullière, 1999; Weisburd, 2006). En effet, des forces exogènes, provenant des environnements politiques, sociaux, économiques, technologiques et juridiques ainsi que des forces endogènes, issues de l'organisation elle-même et de ses membres, poussent les organisations policières à innover.

Innover signifie l'introduction d'un élément nouveau à un système déjà établi. Un créneau relativement récent et en rapide expansion des sciences humaines se spécialise dans l'étude de l'innovation et des processus en découlant. De par sa versatilité, de nombreuses autres disciplines telles que l'éducation, la gestion, la sociologie et la géographie ont incorporé des aspects de ce champ d'étude (Rogers, 2003). Similairement, nous croyons que ces théories permettent de mieux comprendre comment les organisations policières se comportent face au changement en examinant leur processus d'innovation. Les théories de l'innovation s'avèrent donc un outil utile à la compréhension des transformations imposées par l'avènement des technologies de l'information et des communications.

À cet effet, les corps policiers n'ont pas eu le choix d'innover face à la présence de la preuve numérique afin d'être en mesure d'enquêter la criminalité technologique et de rester compétitif avec les délinquants. Conséquemment, ils se sont dotés d'outils sophistiqués et ils ont formé des experts en informatique capables de récupérer, préserver et analyser les données contenues dans ces appareils électroniques. Des unités spécialisées en analyse judiciaire informatique ont donc été créées afin de faire face à la demande grandissante pour cette expertise (Hinduja, 2007; McMillan & al., 2013; Quick & Choo, 2014; Turnbull & al., 2009; Yesilyurt, 2011).

### **Le présent projet de recherche**

La présente étude vise à étudier la transformation des enquêtes policières induite par l'évolution des technologies numériques. Pour se faire, la perspective d'une unité spécialisée en criminalité technologique et en analyse judiciaire informatique sera utilisée. Nous croyons qu'en augmentant les connaissances scientifiques sur ces unités spécialisées, il sera également possible d'avoir une meilleure idée de ce qu'est la criminalité technologique et de comment elle a poussé les organisations policières à innover afin de faire face à cette réalité.

Contrairement aux études portant spécifiquement sur l'adoption ou la diffusion des innovations, le présent projet de recherche vise plutôt une meilleure compréhension du processus d'innovation propre à ces unités spécialisées. Plus particulièrement, nous examinerons comment l'implantation d'une telle unité se réalise et quels sont les défis et les enjeux relatifs à son fonctionnement.

L'étude actuelle comporte donc deux principaux objectifs. Premièrement, caractériser le travail d'une unité spécialisée en criminalité technologique et en analyse judiciaire informatique en qualifiant et en quantifiant leurs activités. Deuxièmement, déceler les enjeux et les défis relatifs à l'implantation et au fonctionnement d'une telle unité. Nous croyons que ces deux objectifs contribueront à augmenter les connaissances scientifiques concernant ces groupes spécialisés. De plus, puisque la grande majorité des services d'enquête ont recours à cette expertise, le travail de ces unités reflète l'ensemble des dossiers traités par un corps policier donné. Ultimement, nous croyons que l'atteinte de ces deux objectifs permettra d'offrir une meilleure compréhension du processus d'innovation inhérent à ces unités ainsi qu'une idée plus claire de leur fonctionnement interne. Dans une perspective plus large, cela permettra également de mieux comprendre l'impact des technologies et de la preuve numérique sur les enquêtes policières.

### **Structure du rapport**

Ce rapport sera divisé en cinq parties. Dans un premier temps, le chapitre II a pour objectif d'examiner le lien entre les organisations policières et l'innovation. Pour ce faire, l'origine des théories de l'innovation sera abordée, suivie d'une présentation des théories plus contemporaines. Par la suite, l'application de ces théories de l'innovation aux organisations en général sera discutée. Finalement, un bref historique des innovations technologiques policières des 150 dernières années ainsi que l'application de ces théories aux organisations policières seront présentés.

Le chapitre III traite du projet de stage réalisé dans une unité spécialisée en criminalité technologique et en analyse judiciaire informatique. Premièrement, une présentation détaillée de l'unité sera effectuée. Deuxièmement, il sera question de la méthodologie utilisée lors de la

collecte de données. Les étapes de la création d'une base de données regroupant l'ensemble des demandes de service adressées à cette unité seront détaillées ainsi que les analyses en découlant. Des entrevues ont également été réalisées avec des membres de cette équipe afin d'approfondir certains aspects et de valider les analyses effectuées.

Le chapitre IV présente des analyses permettant de caractériser le travail d'une unité effectuant des analyses judiciaires informatiques. Il sera principalement question du volume de travail d'une telle unité, des types de services offerts, de ses principaux clients, des formes de criminalité enquêtées et de la nature du matériel expertisé.

Le chapitre V explore les défis et les enjeux spécifiques à une unité spécialisée en criminalité technologique. Les thèmes et les éléments abordés par les intervenants rencontrés permettent de souligner les contraintes les plus importantes pour leur unité. Notamment, il sera question des délais de traitement relatifs à l'analyse des pièces à conviction et des autres facteurs exogènes et endogènes exerçant une pression sur l'unité.

Finalement, le chapitre VI résume l'ensemble des éléments importants abordés dans la présente étude. Il vise également à distiller les informations colligées afin de les généraliser à toutes les organisations souhaitant implanter une unité spécialisée en criminalité technologique. Finalement, les implications de ce projet de recherche pour les milieux policier et académique seront discutées. Des constatations et des réflexions seront partagées quant à l'avenir de ces unités et à l'orientation de la recherche scientifique sur le sujet.

---

## **Chapitre II**

### **Recension de la littérature : Police et innovation**

---

Les organisations policières ont toujours entretenu un lien étroit avec les innovations technologiques, ces dernières pouvant potentiellement leur procurer un avantage dans l'exercice de leurs fonctions. Toutefois, le processus d'innovation semble affecté par de nombreux facteurs. Pourquoi certaines innovations sont adoptées dès leur invention et d'autres, tout aussi pertinentes, tombent dans l'oubli ou sont adoptées des années plus tard ?

Dans ce chapitre, il sera question de la relation entre les organisations policières et l'innovation. Nous tenterons de déterminer, à l'aide de théories existantes, quels sont les éléments-clefs articulant le processus d'innovation et comment ces éléments s'appliquent à la réalité des organisations policières.

Afin de remplir ce mandat, les théories traitant de l'innovation seront tout d'abord introduites. Il sera question de leur origine, du développement de ce courant scientifique ainsi que de leur état actuel. De plus, des concepts centraux à l'innovation, tels que la diffusion et le processus décisionnel, seront abordés. Deuxièmement, l'application des théories de l'innovation aux organisations en général sera traitée. Les mécanismes articulant l'innovation dans les organisations seront abordés ainsi que l'impact de l'innovation sur la structure organisationnelle. Troisièmement, la question spécifique de l'innovation dans les organisations policières sera discutée. Un bref historique de l'évolution technologique dans les organisations policières nord-américaines sera d'abord présenté. Il sera ensuite question des types d'innovations policières, des facteurs favorisant l'innovation dans les organisations policières et du cas particulier des unités spécialisées. Finalement, nous discuterons de l'implication et de l'utilité des théories présentées dans le cadre du présent projet de recherche.

## **1. Les théories de la diffusion et de l'adoption des innovations**

Un champ de la sociologie s'intéresse à comment s'opèrent la diffusion et l'adoption des innovations au sein d'un environnement donné. À titre d'exemple, cet environnement peut être un groupe d'individu, une population ou une organisation. Ces théories de l'innovation permettront de mieux comprendre quels processus et quels mécanismes articulent les évolutions technologiques au sein des organisations policières.



Dans cette première section, il sera question de l'origine des théories de l'innovation. Suivra une présentation détaillée de la théorie de la diffusion des innovations telle que popularisée par Everett M. Rogers (2003), l'un des plus éminents chercheurs en la matière. Il sera notamment question de la définition de l'innovation, de ses caractéristiques, de la diffusion des innovations et du processus d'innovation. Finalement, une particularité des technologies de l'information et des communications en tant qu'innovation sera abordée; c'est-à-dire le processus cyclique d'innovation.

### **1.1. Les racines des théories de l'innovation**

La deuxième moitié du 19<sup>e</sup> siècle voit la formalisation de la sociologie en tant que discipline académique. La théorie de l'innovation telle que nous la connaissons aujourd'hui remonte à cette période d'importante effervescence intellectuelle. Gabriel Tarde, sociologue, juriste et criminologue Français de renom, est un précurseur de cette théorie (Carof, 2007; Rogers, 2003). En 1890, il publie un ouvrage intitulé « *Les lois de l'imitation* » où il explique les mouvements sociaux par le processus d'imitation et d'invention. Pour Gabriel Tarde, les individus vivent en société de par l'imitation d'un même modèle; l'imitation est donc le fondement du lien social pour lui (Rogers, 2003; Touret, 1999). Les individus, de par leur nature, cherchent toujours à imiter ce qui leur est supérieur; ceci constitue le fondement du progrès. De plus, non seulement les individus, mais aussi les groupes sociaux, les organisations et les sociétés s'imitent et donc évoluent ainsi (Touret, 1999).

Les innovations et les découvertes technologiques sont le fruit d'une imitation, si faible soit-elle. Ces innovations se propagent d'individu en individu, telle une onde, par le processus de réinvention du modèle initial (Touret, 1999). En d'autres termes, chaque individu faisant l'adoption d'une innovation est susceptible de la modifier partiellement afin de mieux servir ses besoins. Par contre, l'imitation ne se fait pas sans résistance, il y a nécessité d'une adaptation (Carof, 2007; Rogers, 2003; Touret, 1999). La résistance est proportionnelle à l'écart entre le modèle de référence et l'innovation projetée.

En résumé, le modèle de Tarde comporte trois phases : l'imitation, la résistance et l'adaptation. Ce processus est cyclique et s'opère en continu; l'innovation, après la phase

d'adaptation, deviendra le modèle de référence et une autre innovation sera éventuellement introduite au système.

## 1.2. Les théories contemporaines de l'innovation

Ce n'est que dans les années 1940 que les recherches contemporaines sur l'innovation débiteront. Initialement, ces dernières se concentraient sur l'adoption de technologies agricoles chez des groupes d'agriculteurs américains (voir : Ryan & Gross, 1943). Le principal constat de cette première série d'études est le suivant : la distribution des innovations, dans un environnement donné, s'effectue selon la forme d'une courbe en « S » (Rogers, 2003), aussi appelée fonction logistique (voir Figure 1 ci-dessous). En d'autres termes, cela signifie que la diffusion d'une innovation dans le temps ne se répartit pas de façon uniforme.

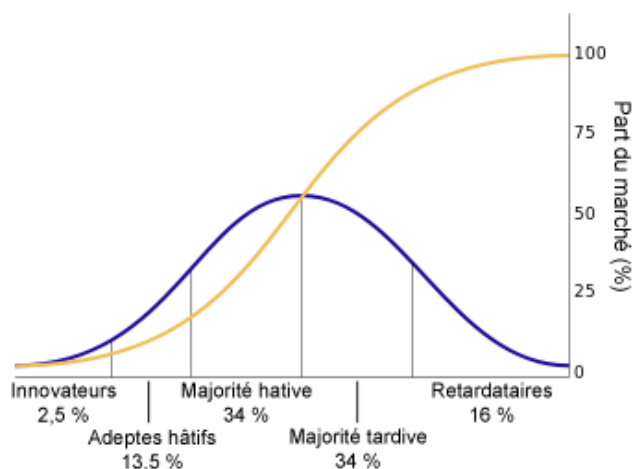


Figure 1. Courbe logistique normale du taux d'adoption en fonction du temps.

En effet, il semble qu'initialement un relativement petit nombre d'individus adoptent une innovation donnée. Ce nombre croîtra tranquillement jusqu'à ce qu'une masse critique soit atteinte. À ce moment, la majorité des membres de l'environnement feront l'adoption de l'innovation. Finalement, une certaine portion des individus sera récalcitrante à adopter l'innovation et ne le fera qu'en tout dernier. De ce constat découle une typologie popularisée en 1962<sup>1</sup> par Everett M. Rogers (2003) classant les adeptes (*adopters*) d'une innovation selon leur vitesse relative d'adoption. Le tableau 1 à la page suivante résume cette typologie.

---

<sup>1</sup> Date coïncidant avec la première édition de l'ouvrage *Diffusion of Innovations*. Everett M. Rogers en est à sa cinquième édition parue en 2003.

Tableau 1

*Typologie des adeptes selon leur vitesse d'adoption des innovations*

Type d'adeptes	Pourcentage de la distribution	Caractéristiques des individus
Innovateurs	2,5	Audacieux, gèrent le risque, possèdent un réseau interpersonnel développé, cosmopolites, ingénieux, nantis
Adeptes hâtifs	13,5	Avant-gardistes, respect des pairs, charismatiques, leadership au sein du système de référence
Majorité hâtive	34	Intégrés au système social de référence
Majorité tardive	34	Sceptiques, conservateurs
Retardataires	16	Isolés du système social de référence, résistes au changement, situation économique précaire

Suite à cette vague de recherche, un engouement pour les théories de l'innovation s'en suivra. Plusieurs autres disciplines académiques telles que la communication, le marketing et la géographie intégreront ces concepts à leur champ d'étude respectif. Malgré les disparités entre ces écoles de pensées, il y a naissance d'une nouvelle tradition de recherche : l'innovation (Rogers, 2003; Sonis, 2009).

L'étude de l'innovation comprend de nombreuses facettes, notamment : la vitesse d'adoption des innovations, la capacité à innover, les réseaux de diffusion, le processus entourant l'innovation, l'utilisation de différents canaux de communication dans le processus de diffusion et les conséquences de l'innovation (King, 2000; Rogers, 2003; Wolfe, 1994).

De façon générale, les recherches contemporaines sur l'innovation peuvent être divisées en trois grands courants : les études sur la diffusion, les études sur les facteurs favorisant l'innovation et les études sur le processus d'innovation (King, 2000; Sonis, 2009; Wolfe, 1994).

### **1.3. Qu'est-ce qu'une innovation ?**

Tracer les origines des théories de l'innovation mène à une question fondamentale : « *Qu'est-ce qu'une innovation ?* ». Une innovation est une idée, une pratique ou un objet perçu comme étant nouveau par un individu ou un autre système de référence; une organisation par exemple (Rogers, 2003). L'innovation peut prendre la forme d'une nouvelle technologie, d'une méthode novatrice, d'un processus industriel ou d'une stratégie de gestion.

Selon Rogers (2003) une innovation possède cinq (5) caractéristiques centrales : (1) son avantage relatif, (2) sa compatibilité, (3) sa complexité, (4) sa testabilité et (5) son observabilité. Ces caractéristiques, telles que perçues par le système ou l'unité de référence, déterminent la vitesse d'adoption d'une innovation.

D'autres facteurs importants peuvent influencer l'adoption d'une innovation (Shayo, 2009) : le type de processus décisionnel (est-ce que l'innovation est adoptée de façon volontaire ou est imposée par une autorité), la nature des canaux de communication (est-ce que l'innovation est diffusée par des médias de masse ou de façon plus personnalisée), la nature du système social (les caractéristiques et les normes en place dans le groupe de référence) et les efforts des agents du changement (à quel point les défenseurs de l'innovation mettent de l'avant les avantages relatifs de l'innovation et supportent sa diffusion).

Dans ses analyses, Rogers (2003) tente de déterminer les facteurs favorisant l'adoption d'une innovation. Il élabore ainsi sa théorie de la diffusion des innovations. La diffusion est le processus par lequel une innovation est communiquée, via différents canaux de communication, aux membres d'un même système social, et ce pour une période donnée. La diffusion est un type particulier de communication qui est caractérisée par la nouveauté de l'idée ou du concept véhiculé. Cette nouveauté est souvent accompagnée d'une incertitude que les individus ou des organisations souhaitent réduire en s'informant. En réduisant l'incertitude relative à une innovation il est plus facile d'en faire d'adoption. Ce qui est perçu comme étant nouveau dépend du référentiel en question, il est donc essentiel de définir adéquatement l'entité étudiée et de l'inscrire dans une certaine temporalité.

Finalement, selon Rogers (2003), le processus décisionnel d'adopter ou de rejeter une innovation peut être divisé en plusieurs étapes : (1) la connaissance, (2) la persuasion, (3) la décision, (4) l'implantation et (5) la confirmation.

#### 1.4. L'innovation : un processus cyclique

Selon Shayo (2009), il est de l'intérêt des individus et des organisations de développer des stratégies systémiques afin d'identifier, de se procurer, de comprendre et d'implémenter de nouvelles technologies. Ceci est particulièrement vrai puisque, selon l'auteur, les technologies (particulièrement les technologies de l'information et des communications) se renouvellent continuellement. De plus, ce « cycle » semble s'accélérer de plus en plus rapidement.

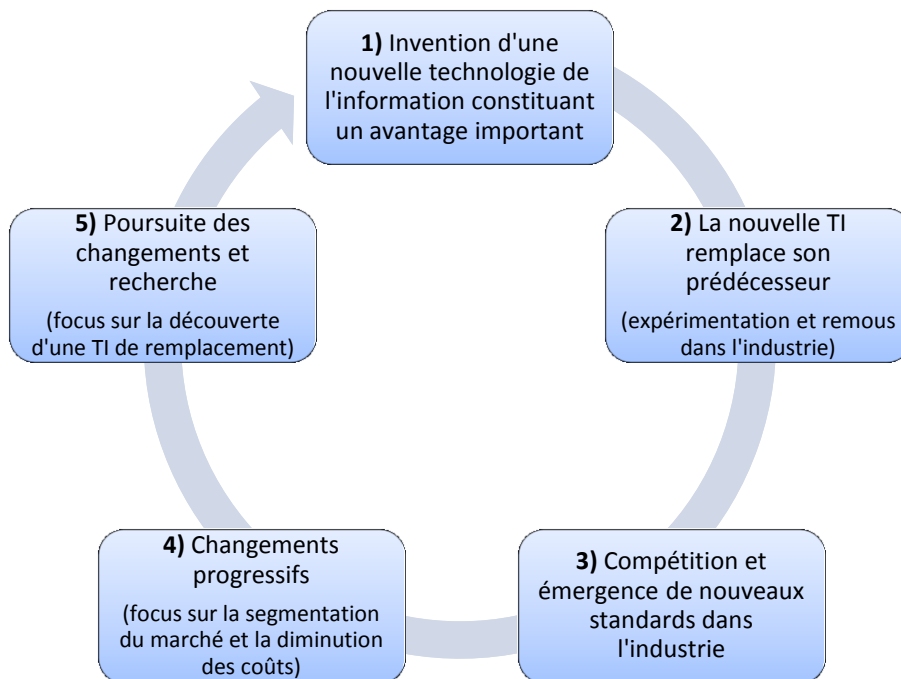


Figure 2. Le cycle de vie des technologies de l'information. Inspiré de Shayo (2009), Figure 1, page 2654.

Une illustration populaire de cette réalité est la constatation effectuée en 1965 par Gordon E. Moore le cofondateur d'*Intel Corporation*. Selon la prédiction de Moore (1965), le nombre de transistors par circuit intégré doublera au deux ans. Cette progression exponentielle, mieux connue sous le nom de « loi de Moore », s'est avérée exacte jusqu'à présent (Quick & Choo, 2014). De plus, selon Walter (2005) l'augmentation de la capacité de stockage des disques durs est encore plus effrénée, doublant chaque année depuis 1995. Il est hasardeux de prédire l'avenir, mais il est raisonnable de croire que si ce rythme ne s'accélère pas dans le futur, il gardera néanmoins sa vitesse de croisière.

Les avancées rapides de la science couplée à l'effervescence des technologies de l'information et des communications contribuent à un environnement technologique en grande mouvance. Les individus, tout comme les organisations, doivent être bien informés et rester à l'affût de leur environnement afin d'être au fait de tous ces changements.

## **2. Les organisations et l'innovation**

Quelques décennies après les premières études sur l'innovation, certains chercheurs ont tenté de transposer aux organisations les modèles théoriques développés initialement pour les individus. Ces premières études considéraient l'organisation en entier en tant qu'unité de référence (Rogers, 2003). Le principal objectif de ces études était de déterminer quelles étaient les caractéristiques menant à l'adoption ou à la non-adoption d'une innovation dans une organisation donnée (Rogers, 2003; Zaltman & al., 1973).

Rapidement, les chercheurs ont réalisé qu'une organisation est complexe et qu'elle ne constitue pas un tout homogène; le modèle utilisé était donc trop simpliste et ne reflétait pas les multiples facettes d'une organisation (Van de Ven & Rogers, 1988; Zaltman & al., 1973). En effet, pour une organisation donnée, une même innovation ne sera pas adoptée de façon uniforme par tous les membres de l'institution. Qui plus est, la manière dont une innovation est adoptée et utilisée est également susceptible de varier d'une organisation à l'autre.

À cet effet, Gerald Zaltman et ses collègues, dans l'ouvrage « *Innovations and Organizations* » (1973), apportent des distinctions importantes qui devraient être prises en compte lors de l'étude de l'innovation dans les organisations. Ils sont dans les premiers à considérer, en tant que variable dépendante, l'implantation (l'intégration d'une innovation spécifique au sein d'une organisation) plutôt que l'adoption. L'adoption ou non d'une innovation peut être vue comme la finalité d'un processus; il est beaucoup plus instructif de comprendre le processus préalable à l'adoption. De plus, la façon dont est implantée une innovation sera garante de son utilisation future et de l'atteinte de son plein potentiel. Zaltman et ses collègues se concentrent donc sur le processus entourant la « pré-adoption », l'acquisition, l'implantation et l'utilisation d'une innovation donnée. Cette séquence d'événements est appelée processus d'innovation.

Lors de son introduction, ce courant de recherche visait l'étude des nouvelles technologies de l'information et des communications progressivement introduites dans les organisations au cours des années 1990. En effet, puisque plusieurs de ces implantations ont échoué, un intérêt accru a été porté afin de comprendre les mécanismes reliés au processus d'implantation (Rogers, 2003; Van de Ven & Rogers, 1988).

L'analyse du processus d'innovation semble l'approche la plus appropriée pour traiter le présent sujet d'étude, c'est-à-dire l'influence des technologies de l'information et des communications sur les enquêtes policières. En effet, selon Willis (2011) cette approche est probablement la plus révélatrice pour les gestionnaires œuvrant dans les organisations policières, celle-ci leur permettant de mieux comprendre les contextes dynamiques, politiques et sociaux dans lesquels s'inscrit une innovation. Qui plus est, cette approche permet de disséquer les étapes de ce processus et de déterminer quels facteurs, à quels moments, ont mené au succès ou à l'échec de l'implantation d'une innovation donnée.

### **2.1. Le processus d'innovation dans une organisation**

Selon Rogers (2003), Une organisation peut être définie comme le regroupement d'individus en un système stable, travaillant ensemble afin d'atteindre des objectifs communs, et ce, au travers d'une hiérarchie et d'une division du travail déterminée. De plus, une organisation possède cinq (5) principales caractéristiques : (1) des buts prédéterminés, (2) des rôles prescrits, (3) une structure autoritaire, (4) des règles et des réglementations et (5) des pratiques informelles.

Ces caractéristiques organisationnelles viendront pondérer chacune des étapes du processus d'innovation. Ce dernier peut être décrit comme étant la principale séquence de décisions, d'actions et d'événements nécessaires à l'adoption d'une innovation dans une organisation donnée. Selon la modélisation de Rogers (2003) le processus d'innovation dans les organisations se découpe en deux phases principales, elles-mêmes subdivisées en cinq (5) étapes distinctes. Voici un résumé de ces étapes et de leurs principaux aspects :

## **Phase I - L'initiation :**

1. La détermination de l'agenda est l'étape à laquelle l'avènement d'une problématique engendre un besoin, tel que perçu par l'organisation, pouvant être comblé par une innovation. Toute organisation maintient un agenda permettant de déterminer les priorités, les embûches potentielles, les besoins et les solutions mises de l'avant. L'étape de la détermination de l'agenda consiste donc dans un premier temps à identifier les embûches et les besoins et à les prioriser. Par la suite, l'organisation cherche dans son environnement immédiat pour des solutions pouvant combler ces besoins et endiguer les problèmes. L'adéquation entre la performance réelle d'une entreprise et la performance potentielle perçue est un solide moteur à l'innovation. De plus, la majorité des organisations adoptent une attitude proactive afin de déceler des innovations dans leur environnement. Dans ce cas de figure, il est possible que la découverte d'une innovation soit l'initiateur du processus d'innovation organisationnel; il y a donc création d'un besoin.
2. L'appariement est l'étape à laquelle on associe une problématique présente à l'agenda de l'organisation à une innovation précise. On évalue plus concrètement à quel point l'innovation choisie répond au problème identifié par l'organisation. De plus, on examine et on planifie la faisabilité du projet. Lors de cette étape, on s'affaire donc à trouver plus d'information sur l'innovation en cause et on s'assure qu'elle répond précisément à nos réels besoins.

Une fois ces deux premières étapes franchies, il y a formulation d'une décision quant à l'intégration ou non de l'innovation à l'organisation. Si la décision est positive le processus se continue et la phase suivante est entamée; si la décision est négative le processus se termine ici pour l'innovation en question. Ceci n'exclut pas qu'une nouvelle solution soit examinée afin de régler la problématique décelée précédemment. Dans ce cas, le processus recommence avec la nouvelle innovation retenue.



## Phase II - L'implantation :

3. La redéfinition et la restructuration constituent l'étape où l'organisation se familiarise progressivement avec l'innovation choisie et l'intègre à son environnement. La redéfinition s'opère lorsque l'organisation transforme ou réinvente l'innovation afin de servir plus exactement les besoins de l'organisation. À cette étape, autant l'innovation que l'organisation sont susceptibles de changer. Cette adaptation permet de calibrer l'innovation avant que cette dernière soit complètement intégrée aux activités routinières de l'organisation.
4. La clarification survient lorsque l'utilisation de l'innovation est plus largement diffusée au sein de l'organisation. Les membres de l'organisation ont une vision plus claire du rôle de l'innovation dans le cadre des activités. Escamoter cette étape essentielle peut mener à de la résistance et même au rejet d'une innovation. Cette étape consiste donc à donner un sens clair à l'innovation, apprivoiser son fonctionnement et comprendre ses avantages.
5. L'intégration aux activités routinières se produit lorsqu'une innovation est finalement partie intégrante des activités de l'organisation et qu'elle a perdu son caractère exogène. À cette étape le processus d'innovation est complété. Toutefois, l'adoption et l'intégration d'une innovation aux activités de l'organisation n'assurent pas sa pérennité. La durabilité affecte la période durant laquelle une innovation sera utilisée par l'organisation suite au processus d'implantation. Deux facteurs sont déterminant à la durabilité d'une innovation : 1) le niveau de participation des membres lors de l'implantation et 2) le niveau de réinvention effectué par les adeptes de l'innovation.

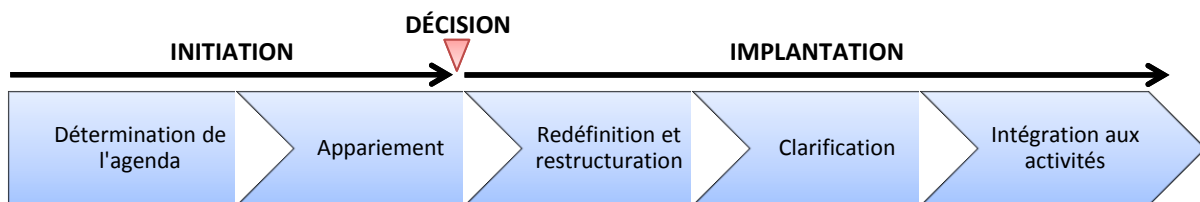


Figure 3. Les étapes du processus d'innovation dans une organisation tel que théorisé par Everett M. Rogers. Figure inspirée de Rogers (2003), *Figure 10-3*, page 421.

Le processus d'innovation en soi peut avoir des conséquences sur l'organisation car il pousse cette dernière à effectuer une série d'analyse de ses besoins et de ses objectifs. Cette introspection peut mener une organisation à se questionner sur sa raison d'être et même à redéfinir sa mission.

#### *2.1.1. Innovation et structure organisationnelle*

Innover, pour une organisation, peut également signifier l'altération de sa structure interne. Cela peut se traduire par la création d'une nouvelle branche ou d'une nouvelle unité s'ajoutant à la structure hiérarchique déjà en place (Rogers, 2003; Zaltman & al., 1973). À titre d'exemple, les avancées scientifiques en identification judiciaire ont donné accès à de nouvelles formes de preuves matérielles (comme l'ADN) qui avant étaient inaccessibles. Ceci a mené à l'introduction de laboratoires de sciences judiciaires et médico-légales aux organisations policières (Seaskate, 1998; Soullière, 1999).

De plus, certaines innovations sont susceptibles d'affecter l'entièreté de l'organisation en changeant profondément les méthodes et les façons de faire. Par exemple, l'adoption de l'approche communautaire a grandement transformé la façon dont les organisations policières interviennent en décentralisant leur structure (Weisburd, 2006). Les innovations ne font donc pas seulement se greffer à la structure organisationnelle; ils la changent.

Tel que mentionné précédemment, de puissantes forces endogènes et exogènes sont susceptibles de transformer les corps policiers. Ces forces poussent au changement; une évolution qui est souvent pour le meilleur, mais aussi parfois pour le pire. Ces changements technologiques et organisationnels sont incarnés par l'adoption d'innovations, vecteurs de ces transformations.

### **3. L'innovation et l'adoption des technologies dans les organisations policières**

Dans cette section il sera spécifiquement question des organisations policières et de comment les théories vues précédemment aident à comprendre le phénomène de l'innovation dans ce contexte précis. Vers la fin des années 1990 et le début des années 2000, plusieurs chercheurs ont tenté de mieux comprendre comment s'articule l'innovation dans les organisations

policières. Le développement de ce créneau spécialisé a mené à de nombreuses études pointues. Parmi les thématiques les plus souvent abordées, nous retrouvons les études sur l'adoption de stratégies policières d'envergure tels que : la police communautaire (Morabito, 2008b; Weisburd, 2006), l'approche par résolution de problèmes (Weisburd, 2006), la cartographie et l'analyse des « *points chauds* »<sup>2</sup> de la criminalité (Manning, 2008; Weisburd, 2006) ainsi que l'analyse comparative des statistiques de la criminalité<sup>3</sup> (Manning, 2008; Moore, 2003; Skogan, 2005; Weisburd, 2003; Weisburd, 2006; Willis, 2007). Ces innovations organisationnelles majeures réorientent les activités policières et concordent souvent avec d'importants changements de paradigme.

D'autres chercheurs se sont concentrés sur les facteurs influençant le degré d'innovation dans les organisations policières (King, 2000; Morabito, 2008 A; Weiss, 1997) ainsi que le processus entourant l'adoption des innovations (Klinger, 2003; Willis, 2011). Finalement, des études traitent de l'introduction de groupes spécialisés aux organisations policières tels que les unités d'intervention tactiques (Klinger, 2003; Kraska 1997) ou l'apparition des équipes d'analyses judiciaires spécialisées (Yesilyurt, 2011).

Les sous-sections suivantes aborderont différentes facettes de l'innovation dans les organisations policières. Plus précisément, il sera question des types d'innovations policières, des facteurs favorisant l'innovation dans les organisations policières ainsi que des unités spécialisées.

### **3.1. Historique des innovations adoptées par les organisations policières depuis les 150 dernières années**

L'évolution rapide des technologies a transformé nos vies et la façon dont nous interagissons en société. Les organisations sont également affectées par ces changements technologiques et doivent adopter ces nouvelles technologies afin de rester compétitives et actuelles. Il en va de même pour les organisations policières qui ont, depuis leur existence, maintenu un lien étroit

---

<sup>2</sup> De l'anglais : « *Hot spots policing* ».

<sup>3</sup> Connu très souvent sous le nom de « *Compstat* », abréviation de « *Complaint Statistics* ».

avec les innovations technologiques (Seaskate, 1998; Soullière, 1999); Soullière (1999) parle même d'une dépendance à la technologie. En effet, les organisations policières subissent de nombreuses pressions extérieures les poussant à se réformer en adoptant de nouvelles façons de faire.

Avec du recul, il est possible de percevoir des tendances et des phases dans l'évolution technologique des organisations policières. Kelling et Moore (1988) découpent l'évolution technologique de la police nord-américaine en trois périodes distinctes : l'ère politique, l'ère de la réforme (aussi présentée sous le nom de « l'ère du modèle professionnel » par Seaskate, 1998) et finalement l'ère de la police communautaire et de l'approche par résolution de problème. Plus récemment, les technologies de l'information et des communications ont poussées les organisations policières vers un nouveau modèle basé sur le renseignement (Manning, 2008; Oliver, 2006; Ratcliffe, 2012; Weisburd, 2006). Oliver (2006) a qualifié cette période « d'ère de la sécurité intérieure ». Chacune de ces époques est donc caractérisée par un modèle policier et des stratégies qui lui sont propres.

### *3.1.1. L'ère politique*

L'ère politique, comprise entre 1840 et 1920, est ainsi nommée car à cette époque les organisations policières américaines et les politiciens entretenaient des relations étroites et intéressées (Kelling & Moore, 1988; Soullière, 1999). En effet, la police relevait de l'autorité municipale locale qui lui donnait sa légitimité ainsi que les ressources nécessaires à ses opérations<sup>4</sup>. La police avait principalement comme rôle le maintien de l'ordre, mais offrait également une variété de services à la communauté. Afin de faire respecter la loi et protéger les honnêtes citoyens, les agents patrouillaient les rues en utilisant des technologies rudimentaires – de simples outils – tels que la matraque et la lanterne (McQuade, 2001). D'un point de vue technologique, cette période est caractérisée par l'adoption de technologies coercitives : l'arme à feu, la matraque et les menottes en sont des exemples. Également, il y a apparition de technologies de communication telles que le télégraphe, les cabines

---

<sup>4</sup> Le modèle américain contraste beaucoup avec les Britanniques qui à cette époque ont une police centralisée très puissante sous l'autorité de la Couronne (Kelling & Moore, 1988).

téléphoniques policières ainsi que le développement des premiers laboratoires<sup>5</sup> de sciences judiciaires. Le policier sur le terrain est extrêmement isolé et les technologies de communication vont progressivement briser cet isolement (Soullière, 1999) en favorisant le flux de l'information. Finalement, au cours des années 1920 une autre technologie importante fera progressivement son apparition dans les organisations policières : l'automobile.

### *3.1.2. L'ère de la réforme*

L'ère de la réforme ou de la professionnalisation, comprise entre 1920 et 1970, est caractérisée par la bureaucratisation (Soullière, 1999) et le développement d'un modèle policier plus indépendant, basé sur la discipline et la formation et mettant l'emphase sur la lutte contre la criminalité (Kelling & Moore, 1988). Les laboratoires de sciences judiciaires deviennent plus communs et sont mieux équipés. Durant les années 30 et 40, les véhicules de patrouilles deviennent largement utilisés et sont progressivement équipés de radios possédant un émetteur-récepteur (Seaskate, 1998; Soullière, 1999). Ceci change le modèle policier en promettant une réponse plus rapide et efficace aux citoyens. Ultimement, à la fin des années 60, l'Amérique du Nord voit l'apparition du système « 911 », un numéro unique centralisant les appels d'urgence (Kelling & Moore, 1988; Seaskate, 1998).

### *3.1.3. L'ère de la police communautaire*

Dans les années 1960, le taux de criminalité<sup>6</sup> et la peur des citoyens sont à la hausse malgré les efforts déployés par les forces de l'ordre (Kelling et Moore, 1988). Le modèle réformiste, très réactif, devient de moins en moins adapté aux valeurs sociales et au contexte de cette époque. Une des principales causes de ces changements sociaux est l'opposition grandissante des Américains face à la guerre du Vietnam. Les manifestations causent de nombreux affrontements entre les policiers d'un côté et la jeunesse et les minorités visibles de l'autre (Weisburd, 2006). De plus, le rapport<sup>7</sup> de 1967 de la Commission présidentielle sur le

---

<sup>5</sup> Les premiers laboratoires de sciences judiciaires furent créés à Paris en 1868, à Lyon en 1910 and à Montréal en 1914 (Soullière, 1999).

<sup>6</sup> Le fait que le taux de criminalité aux États-Unis ait doublé entre 1940 et 1965 est largement publicisé (Seaskate, 1998).

<sup>7</sup> Rapport intitulé : *“The Challenge of Crime in a Free Society”*.

maintien de l'ordre et l'administration de la justice<sup>8</sup> pose de sérieux doutes quant à l'efficacité du système de justice actuel (Seaskate, 1998; Weisburd, 2006). Ceci mènera, dans les années 1970, à un changement de paradigme au sein des forces de l'ordre : celui de la police communautaire. Il y a décentralisation des opérations et les interventions policières sont centrées sur la communauté et préconisent une approche par résolution de problèmes (Weisburd, 2006). Cette période est aussi caractérisée par l'introduction progressive de l'informatique dans les services policiers (Seaskate, 1998).

Avec l'informatisation des organisations policières, les actions posées sont de plus en plus dirigées par le renseignement. À cet effet, l'ordinateur devient un outil essentiel à l'analyse des informations colligées et à la planification des opérations. Éventuellement, l'ordinateur permettra également d'accéder à des renseignements tactiques directement du véhicule de patrouille.

L'informatique permet aussi la centralisation des informations (Soullière, 1999) et la création de bases de données contenant une grande variété de renseignements pertinents autant pour les patrouilleurs que les enquêteurs. À l'aide de ces instruments la police devient de plus en plus proactive et est en mesure d'élaborer des programmes de prévention en concentrant ses activités sur les points chauds de la criminalité. C'est donc l'avènement d'un modèle policier décentralisé, près des communautés et possédant de puissants nouveaux outils d'analyse.

#### 3.1.4. *L'ère de la sécurité intérieure*

Certains auteurs, comme Oliver (2006), croient que depuis les attentats terroristes du 11 septembre 2001, nous sommes entrés dans une quatrième et nouvelle ère policière : l'ère de la sécurité intérieure (*homeland security*). Cet événement a drastiquement accéléré une tendance qui existe depuis les années 1990, celle des activités policières fondées sur le renseignement – le « *intelligence-led policing* ». Ce modèle policier est articulé par la gestion du risque, l'analyse systématique de renseignements criminels à l'aide de logiciels spécialisés, la

---

<sup>8</sup> *President's Commission on Law Enforcement and Administration of Justice.*

géolocalisation des zones chaudes de la criminalité et le développement de solutions adaptées aux problématiques détectées (Ratcliffe, 2012; Weisburd, 2006). Ce processus d'analyse a été popularisé sous le nom de « *Compstat* », modèle adopté initialement par le *New-York Police Department* (NYPD) sous l'administration du maire Giuliani. Ce modèle, hautement encensé, a ensuite été reproduit partout aux États-Unis avec des résultats mitigés (Manning, 2008; Weisburd, 2006).

Selon Olivier (2006), cette nouvelle époque de la sécurité intérieure est spécifiquement caractérisée par la conscience d'une menace terroriste externe, l'adoption de lois permettant la suspension de certains droits civiques ainsi que la collecte systématique de renseignements stratégiques. La disponibilité de technologies d'interception de données couplée à de puissants systèmes d'analyse informatique permet d'assembler de vaste quantité d'informations afin de tenter de prévenir les attentats terroristes.

À cet égard, les technologies de l'information et des communications, dont Internet est probablement la plus emblématique, sont des outils de renseignement incroyablement puissants servant autant les forces de l'ordre que les organisations criminelles. Comme toute nouvelle innovation majeure, ces technologies offrent de nombreuses opportunités stratégiques pour l'individu ou l'organisation en faisant l'adoption.

Entre 2005 et 2009, le nombre et la valeur totale des commandes électroniques effectuées par les Canadiens ont doublé (Statistique Canada, 2010b). Le commerce électronique et les transactions financières sur Internet sont devenus une réalité incontournable. Une conséquence de ce phénomène est la prolifération des renseignements personnels (numéros de cartes de crédit, noms, adresses, dates de naissance, courriels, etc.) stockés sur les serveurs d'entreprises privées et publiques. Ces renseignements constituent des cibles très intéressantes pour des individus malintentionnés (Baker & al., 2011; Hengst & Warnier, 2013). Paradoxalement, selon l'étude de Statistique Canada (2010a) sur l'utilisation d'Internet par les individus, seulement un Canadien sur quatre est préoccupé par la protection de ses renseignements personnels.

Il appert donc que le développement technologique de la police au 21<sup>e</sup> siècle sera caractérisé par le besoin de rester à niveau avec les criminels et leurs utilisations des technologies de l'information et des communications (Seaskate, 1998). L'adaptation à cette nouvelle réalité passera certainement par l'adoption de technologies policières permettant d'enquêter et de contrer la criminalité technologique. Toutefois, l'adoption d'une innovation n'est pas systématique et plusieurs facteurs peuvent favoriser ou inhiber ce processus complexe.

### **3.2. Les types d'innovations policières**

Il est intéressant, d'un point de vue conceptuel, de catégoriser les innovations policières afin d'en distinguer les caractéristiques. Cet exercice permet également d'évaluer les facteurs favorisant spécifiquement l'adoption et l'implantation d'un type d'innovation donné. Une typologie populaire, élaborée par Moore & al. (1997) et reprise par plusieurs auteurs (King, 2000; Randol, 2013; Weisburd, 2006; Willis, 2011), se décline en quatre (4) volets :

- 1) Les innovations concernant de nouveaux programmes (*programmatic innovations*) visent la création d'unités spécialisées ou de tactiques opérationnelles ciblant un objectif ou une problématique spécifique;
- 2) Les innovations administratives touchent principalement la gestion d'une organisation;
- 3) Les innovations techniques visent à adopter une nouvelle pièce d'équipement; ces innovations possèdent des composantes matérielles et/ou logicielles;
- 4) Les innovations stratégiques changent globalement l'orientation d'une organisation ou d'une de ses missions. Elles peuvent avoir un impact drastique sur l'organisation qui en fait l'adoption.

Ces catégories permettent d'étiqueter facilement les innovations policières, mais la majorité de celles-ci sont susceptibles de recouper plusieurs catégories et de toucher plusieurs facettes de l'organisation policière. Il est donc judicieux de ne pas percevoir ces catégories comme étant automatiquement mutuellement exclusives.

### **3.3. Les facteurs favorisant l'innovation dans les organisations policières**

Les facteurs poussant les organisations policières à l'innovation sont multiples mais ils peuvent être découpés en deux grandes catégories : les facteurs exogènes et les facteurs endogènes. Les facteurs exogènes sont les pressions extérieures menant à l'innovation; ils sont principalement de nature politique, sociale et économique (Morabito, 2008 A; Randol, 2013;



Zhao, 1995). De plus, les organisations policières doivent faire face aux formes de criminalité émergentes comme la cybercriminalité et le piratage informatique (Wall, 2007). Les facteurs endogènes, quant à eux, constituent les caractéristiques inhérentes de l'organisation, telles que sa structure, sa hiérarchie, les méthodes de recrutement et les politiques internes (Randol, 2013; Rogers, 2003).

Randol (2013) a spécifiquement étudié l'importance relative des facteurs exogènes (via les théories de la contingence) et endogènes (via les théories de la structure organisationnelle) poussant les organisations policières à l'innovation. Pour ce faire, un échantillon de 380 organisations policières, provenant de trois principales sources de données<sup>9</sup>, a été utilisé. Les données utilisées s'échelonnent sur dix années, permettant ainsi une analyse longitudinale. La capacité à innover (variable dépendante) est mesurée par la quantité d'innovations techniques, programmatiques<sup>10</sup> et administratives<sup>11</sup> adoptées par les organisations policières ciblées.

Des indicateurs tels que le nombre de policiers dans l'organisation, le poids de la structure administrative, le niveau de formalisation ainsi que la formation et la sélection des recrues constituent des facteurs endogènes. Quant à eux, les facteurs exogènes sont mesurés à l'aide d'indicateurs tels que la grandeur de la communauté desservie, les budgets opérationnels<sup>12</sup>, le taux de criminalité violente et le taux de crimes contre la propriété.

Les deux modèles proposés par Randol (2013) ne réussissent qu'à expliquer entre 13% (modèle exogène) et 18% (modèle endogène) de la variance observée pour les différentes catégories d'innovations. Le modèle basé sur les facteurs endogènes a légèrement mieux performé; ce qui tend à corroborer la littérature sur le sujet (King, 2000; Mullen, 1996). Parmi les indicateurs les plus importants, le nombre d'heures de formation, le nombre de critères de

---

<sup>9</sup> Les statistiques de 1997, 2000, 2003, and 2007 du *Bureau of Justice* américain; les rapports uniformes de la criminalité du FBI des années 1996, 1999, 2002, et 2006; une série de données de la *RAND Corporation* intitulée: *Center for Population Health and Health Disparities*.

<sup>10</sup> Mesuré selon le nombre d'unités spécialisées au sein de l'organisation.

<sup>11</sup> Mesuré selon le nombre de politiques et règlements formels dans l'organisation.

<sup>12</sup> Dans l'optique où les organisations policières sont dépendantes des budgets alloués par les instances politiques locales.

sélection pour les nouvelles recrues et la différenciation hiérarchique<sup>13</sup> sont des facteurs endogènes significatifs et positivement associés à tous les types d'innovation. La grandeur de l'organisation<sup>14</sup> est associée positivement et significativement aux innovations techniques et programmatiques.

En ce qui concerne les facteurs exogènes, le budget opérationnel, le pourcentage de minorités, le pourcentage de familles monoparentales ainsi que le taux de criminalité violente sont tous des indicateurs associés significativement et positivement avec l'adoption d'innovations techniques. Le pourcentage de minorités et le pourcentage de familles monoparentales sont également associés positivement avec le nombre d'innovations administratives.

### *3.3.1. Un facteur clef : la taille de l'organisation*

Selon la littérature, l'un des facteurs cruciaux au degré d'innovation d'une organisation est sa taille (Hollenstein, 2004; Mastroski, 2003; Rogers 2003). Selon King (2000), Morabito (2008 A, 2008 B), Randol (2013) et Willis (2011) ce facteur est tout aussi significatif chez les organisations policières.

Ce qui définit la grandeur d'une organisation est le dénombrement de ses effectifs, la complexité de sa structure et surtout la quantité de ressources disponibles. À cet effet, Morabito (2008a, 2008b) réitère l'importance marquée des ressources excédentaires disponibles (*slack resources*). Ces ressources sont caractérisées par la flexibilité de leur allocation. Elles constituent une sorte de « trésor de guerre », rapidement déployé en cas de besoin et facilitant grandement l'adoption de toute nouvelle innovation. Ces ressources constituent un atout considérable des organisations policières et est un important moteur à l'innovation.

---

<sup>13</sup> Réfère à la complexité de la structure hiérarchique verticale de l'organisation.

<sup>14</sup> Calculé à l'aide du nombre total de policiers à temps plein dans l'organisation.

### 3.4. Le cas particulier des unités spécialisées

Tel que mentionné précédemment, l'innovation peut mener à l'altération de la structure organisationnelle et même à la création de branches spécialisées. Tel est le cas des laboratoires médico-légaux, des groupes d'intervention tactique ou des unités spécialisées en criminalité informatique; ces entités incarnent d'une façon ou d'une autre l'adaptation des organisations policières aux développements technologiques et aux nouvelles réalités criminelles.

Klinger (2003) traite de la diffusion des équipes d'intervention tactique (*SWAT<sup>15</sup> teams*) au sein des organisations policières américaines. Vers la fin des années 1990, une hausse marquée de ces unités spécialisées a été observée dans les organisations policières (Kraska, 1997) de cent officiers et plus; certains y ont vu une forme de militarisation de la police. Par contre, selon l'analyse de Klinger (2003) la diffusion de ce type d'innovation organisationnelle peut prendre de 15 à 30 ans avant d'atteindre le point de saturation (une adoption d'environ 90%); dans le cas des équipes d'intervention tactiques on parle d'environ 25 ans avant d'atteindre ce niveau. La hausse marquée décrite par Kraska est donc plutôt due à un phénomène normal de diffusion (à savoir, la courbe en « S » discutée précédemment; voir chapitre II, section 1.2) débutant dans les années 60 et 70, atteignant une masse critique au cours des années 80 et saturant vers la moitié des années 90. La diffusion et l'adoption d'une unité spécialisée semble donc être un processus de longue haleine qu'il faut considérer dans son ensemble.

Katz (2002) a examiné les facteurs expliquant la présence d'une unité spécialisée antigang auprès de 484 grandes organisations policières. Selon l'étude, les deux facteurs significatifs ayant le plus grand impact relatif sont le degré de financement extérieur ainsi que la menace sociale (mesurée par la présence de minorités et le niveau d'inégalités socioéconomiques). Dans ce cas spécifique, les facteurs exogènes semblent avoir eu un impact plus important que les facteurs organisationnels; ceci est également appuyé par l'étude de Zhao (1995) qui a

---

<sup>15</sup> *Special Weapons And Tactics*.

démontré l'importance des facteurs environnementaux dans l'adoption du modèle COP<sup>16</sup>. L'adoption d'une unité spécialisée par un corps policier pourrait donc être principalement due à des facteurs exogènes.

Yesilyurt (2011) a analysé comment les contraintes environnementales et organisationnelles affectent l'adoption de pratiques reliées à l'analyse judiciaire informatique dans plusieurs grandes organisations policières de cent policiers et plus. Selon cette étude, l'adoption de techniques d'analyse judiciaire informatique serait principalement due à des facteurs environnementaux. Parmi les facteurs les plus importants notons : la grandeur de la population desservie, la présence d'un comité de plaintes citoyennes et la présence de partenariats avec divers organismes et institutions. De plus, la grandeur de l'organisation policière affecte également la mise en place et la formalisation des méthodes d'analyse judiciaire informatique.

En résumé, l'adoption d'unités spécialisées par les organisations policières est un processus d'envergure, influencé par une combinaison de facteurs environnementaux et organisationnels. Contrairement aux autres innovations, ces innovations « programmatiques » semblent être engendrées principalement par des facteurs exogènes à l'organisation policière.

### **3.5. Les conséquences de l'innovation et autres considérations**

Tel que démontré dans les sections précédentes, les théories de l'innovation ont plusieurs facettes et de nombreuses applications en sciences humaines. Récemment plusieurs criminologues ont utilisé ces théories afin de mieux comprendre comment les organisations policières innovent.

Willis (2011) fait un état de situation de la recherche sur l'innovation appliquée aux organisations policières. Il examine comment surviennent les innovations dans le contexte policier ainsi que les facteurs structurels et culturels favorisant la diffusion de ces innovations. Willis (2011) effectue toutefois une mise en garde : le défi majeur de ce type d'études est la

---

<sup>16</sup> *Community-Oriented Policing.*

conceptualisation. Les chercheurs voulant étudier l'innovation dans les organisations policières devront porter une attention toute particulière aux éléments suivants : 1) comment ils définissent l'innovation dans le contexte de leur étude, 2) le caractère multifactoriel des innovations et finalement 3) les chercheurs devraient questionner, plutôt que d'accepter d'emblée, la vision populaire que l'innovation est un fait désirable. En effet, innovation n'est pas toujours synonyme d'amélioration systématique des procédures et des technologies déjà en place. Les chercheurs devraient toujours se questionner sur les conséquences à long terme de l'implantation d'une innovation. Pareillement, l'adoption d'une innovation prometteuse ne signifie pas nécessairement une utilisation adéquate ou optimale de cette dernière.

À cet effet, nous croyons qu'il est important de citer l'exemple de Manning (2008). Il a étudié quels impacts ont eu l'introduction des technologies de l'information, de la cartographie de la criminalité (*crime mapping*) et de l'analyse criminelle (*crime analysis*) sur trois grandes organisations policières. Il conclut que ces technologies et leurs fonctions de soutien aux enquêtes n'ont pas significativement changé les pratiques de ces trois services de police. Plusieurs raisons de cet échec sont évoquées : premièrement, les organisations policières sont ancrées dans un mode de fonctionnement réactif plutôt que préventif et deuxièmement, les organisations policières sont menées par différents impératifs organisationnels altérant fréquemment leurs priorités. Ces événements ponctuels forcent la réallocation d'effectifs, provenant de tous les niveaux de la chaîne de commandement, sur des problèmes demandant une réponse immédiate. Ceci rend extrêmement difficile l'introduction de technologies axées sur la gestion des activités opérationnelles puisqu'elles nécessitent un apprentissage, du temps disponible et une certaine rigueur d'utilisation.

Selon Manning (2008), pour qu'un réel changement s'opère plusieurs éléments clefs sont nécessaires : une infrastructure supportant le changement, du personnel qualifié, un pouvoir administratif ainsi que la diffusion adéquate des renseignements générés. Finalement, les organisations policières sont complexes et constituent un amalgame dynamique de réseaux d'influence partiellement liés aux pouvoirs politiques en place ce qui a tendance à influencer le processus l'innovation de l'organisation.

Dernièrement, le choix d'innover a des conséquences et ne doit pas être pris à la légère; adopter une innovation peut signifier le rejet des alternatives existantes (Rogers, 2003). Une organisation peut donc devenir virtuellement prisonnière des choix qu'elle effectue. Les innovations dites de « contingence » (Rogers, 2003) ne peuvent être adoptées que si d'autres innovations préalables sont déjà en place. Si ces préalables ont été rejetés au bénéfice d'autres innovations, il est envisageable qu'il soit impossible d'implanter l'innovation désirée. À titre d'exemple, si une entreprise se dote d'un parc informatique sous la plateforme Windows, il est fort probable qu'elle ne puisse utiliser certains logiciels du système d'exploitation Linux.

#### **4. Résumé et application des éléments théoriques**

Une innovation est une idée, une pratique ou un objet perçu comme étant nouveau (Rogers, 2003). L'adoption successive d'innovations a permis à l'Homme de modeler et de remodeler son univers de façon à construire la société moderne peuplée de prouesses technologiques que nous connaissons. Fondamentalement, nous innovons car nous avons la perception que cette action nous procurera un avantage relatif quelconque (Rogers, 2003).

Ce chapitre a présenté plusieurs éléments théoriques permettant de mieux comprendre comment s'articule le processus d'innovation dans les organisations policières. Premièrement, il a été question de la théorie de l'imitation de Gabriel Tarde, précurseur des théories de l'innovation modernes. Selon Tarde, les individus cherchent à imiter ce qui leur est supérieur et durant ce processus ils altèrent l'idée originale. Telle une onde, les innovations se propagent ainsi d'individus en individus. Ce processus cyclique comporte trois étapes : l'imitation, la résistance et l'adaptation.

Les théories modernes de l'innovation ont ensuite été abordées et l'apport important de Rogers (2003) à cette école a été souligné. Il a été notamment question de ce qu'est une innovation, de ses principales caractéristiques, de la diffusion des innovations et à quelle vitesse celle-ci s'effectue ainsi que du processus décisionnel entourant l'adoption ou non d'une innovation. Finalement le caractère cyclique de l'innovation a été discuté. À cet effet, le cycle de vie des technologies de l'information et des communications semble généralement plus court que leurs contreparties.

Des théories générales de l'innovation, nous sommes passés aux théories concernant spécifiquement les organisations. Une organisation est comme une microsociété, elle possède des objectifs spécifiques et se régule à l'aide de normes et de procédures qui lui sont propres. Lors de l'adoption d'une innovation une vaste gamme de facteurs est susceptible d'affecter ce processus. Le processus d'innovation dans les organisations, tel que présenté par Rogers (2003), se découpe en deux phases principales : la phase d'initiation (composée des étapes de la détermination de l'agenda et de l'appariement) et la phase d'implantation (composée des étapes de la redéfinition, de la clarification et de l'intégration). De plus, certaines innovations peuvent avoir comme conséquences d'altérer de façon permanente la structure organisationnelle.

Enfin, il a été question de la particularité des organisations policières. Un portrait de l'évolution des technologies policières a d'abord été tracé. Quatre principales époques divisent historiquement l'évolution de ces technologies : l'ère politique, l'ère réformatrice, l'ère de la police communautaire et l'ère de la sécurité intérieure. Ces époques reflètent autant les changements technologiques qu'idéologiques de la société. Il est important de se rappeler que les organisations policières opèrent principalement en réaction aux réalités et aux problématiques criminelles vécues par une société.

Les théories de l'innovation appliquées aux organisations policière ont ensuite été abordées. Plusieurs auteurs (King, 2000; Randol, 2013; Weisburd, 2006; Willis, 2011) catégorisent les innovations policières comme suit : les innovations programmatiques, les innovations administratives, les innovations techniques et les innovations stratégiques. Plusieurs facteurs endogènes et exogènes influencent les différentes facettes du processus d'innovation. Les forces exogènes poussant au changement sont principalement de nature politique, sociale et économique. De plus, l'évolution de la criminalité et surtout l'évolution de l'opinion publique face aux formes émergentes de criminalité, exercent une pression extérieure importante et un moteur poussant les organisations policières à l'innovation. D'autre part, des facteurs endogènes à l'organisation, tels que sa taille, sa structure, la formation des employés, les ressources monétaires disponibles et les politiques internes affectent aussi le processus

d'innovation. La taille de l'organisation et les ressources excédentaires disponibles favorisent grandement la capacité à innover.

Le cas particulier des unités policières spécialisées a été traité. Pour une organisation policière, cela signifie la mobilisation de nombreuses ressources humaines et matérielles. La constitution d'une nouvelle branche spécialisée cause aussi la restructuration de l'organisation. Adopter ce genre d'innovation programmatique constitue un processus de longue haleine s'échelonnant sur des dizaines d'années. Le choix d'adopter ce type d'innovation semble principalement motivé par des facteurs exogènes, tels que la perception par le public d'une menace extérieure et le degré de financement externe.

Finalement, il est important de rappeler qu'innover n'est pas nécessairement souhaitable. L'innovation peut entraîner des conséquences indésirables et même aggraver une situation donnée. De plus, même si le processus d'innovation est désirable et bénéfique, son résultat n'est aucunement garanti. De nombreux efforts doivent être déployés pour assurer le succès de cette entreprise. La bonne implantation d'une innovation est donc la clef de sa réussite à long terme.

## **5. Implications pour le présent projet de recherche**

Jusqu'à présent, une vaste gamme d'éléments théoriques pouvant expliquer les mécanismes et les facteurs influençant l'innovation dans les organisations policières a été exposée. Le concours de forces exogènes et endogènes permet de comprendre pourquoi une organisation policière doit adopter de nouvelles innovations afin de s'adapter à une société changeante. L'avènement de la criminalité technologique ne fait pas exception à la règle. Le développement d'une expertise judiciaire en informatique semble le choix privilégié par plusieurs organisations policières afin de faire face à la réalité de l'ère numérique.

Nous croyons que l'adoption d'une telle innovation pour une organisation policière implique la restructuration de ses activités régulières afin de traiter adéquatement la preuve numérique. Cela offre également l'opportunité d'enquêter sur des crimes de nature informatique et assurer le développement d'une expertise cruciale pour l'avenir; spécialement dans la perspective où il



y aura une migration de plus en plus importante de la délinquance vers les médiums électroniques (par exemple : l'augmentation des fraudes en ligne et de la délinquance numérique associée à des actes de violence comme la cyberintimidation).

L'introduction d'une telle unité spécialisée revête de multiples facettes et peut donc être analysée à divers niveaux : il s'agit d'une innovation programmatique, car l'unité créée possède ses objectifs propres et vise une problématique spécifique; il s'agit également d'une innovation administrative, car les autres unités d'enquêtes effectuent des demandes ponctuelles d'assistance (ex. : aide à la perquisition, analyses informatiques, etc.). Il est donc nécessaire d'établir des canaux de communication et un processus administratif afin d'acheminer les demandes en bonne et due forme. Finalement, il s'agit d'une innovation technologique car il y a adoption fréquente de nouvelles pièces d'équipement spécialisées, autant logicielles que matérielles. De plus, ces outils d'analyse doivent être configurés et opérés par des individus ayant les compétences et les connaissances adéquates; il y a donc la nécessité de recruter des spécialistes et de former des individus au sein de l'organisation afin d'assurer la pérennité de l'expertise.

Peu de chercheurs se sont intéressés aux processus d'innovation entourant ces unités spécialisées. Qui plus est, les connaissances académiques sur le fonctionnement interne de ces unités spécialisées semblent pour l'instant insuffisantes, ce qui rend d'autant plus difficile une analyse basée sur les théories de l'innovation. Dans le but de mieux comprendre les mécanismes d'innovation inhérents à ces unités, il est nécessaire d'aller vérifier préalablement leur fonctionnement.

Afin d'atteindre ce but, nous allons premièrement caractériser le travail d'une unité spécialisée en criminalité technologique et en analyse judiciaire informatique. Deuxièmement, nous chercherons à déterminer les contraintes et les enjeux susceptibles d'influencer le processus d'innovation et d'implantation d'une unité spécialisée en analyse judiciaire informatique. Nous croyons que la réalisation de ces objectifs permettra de mieux comprendre les différents processus d'innovation entourant ces unités spécialisées et par le fait même clarifier l'impact

des technologies de l'information et des communications sur les enquêtes policières au 21<sup>e</sup> siècle.

### **5.1. Caractériser le travail d'une unité spécialisée en criminalité informatique**

Les questions de recherche suivantes visent à atteindre une meilleure connaissance des unités spécialisées en criminalité technologique. Ci-dessous sont présentées des interrogations centrales au rôle, au fonctionnement et aux tâches de ces unités. Elles sont accompagnées d'une réflexion quant à l'importance de leur réponse dans le cadre d'une meilleure compréhension de la transformation des enquêtes policières due à l'évolution des technologies de l'information et des communications.

- a) *Quel est le volume de travail d'une unité spécialisée en criminalité technologique ?*
  - *Quels sont les facteurs influençant ce volume et comment ce dernier fluctue-t-il dans le temps ?*

Le volume de travail nous renseigne sur la prédominance de la preuve numérique et son importance relative pour les enquêtes policières. Nous émettons comme hypothèse que le nombre de demandes croîtra avec le temps, signifiant une augmentation générale des enquêtes ayant au moins une composante numérique.

- b) *Quels sont les types de services offerts par une telle unité ?*
  - *Quel est le volume de travail relatif à chacun de ces services ?*
  - *L'évolution des technologies affecte-t-elle les services offerts ?*

Les types de services demandés nous renseignent sur la nature de ou des transformations induites par les technologies de l'information et par la preuve électronique sur les enquêtes policières. Il est également intéressant de savoir quels types de services occupent la plus grande proportion du volume de travail et déterminer si cette tendance se modifie en fonction du temps. Nous croyons que ces éléments aideront à tracer un portrait de l'évolution des besoins relatifs à cette expertise et par le fait même un portrait de l'évolution des enquêtes policières. Finalement, nous nous questionnons sur l'évolution de cette expertise; c'est-à-dire

si les technologies poussent le développement de nouvelles façons de faire ou de nouvelles méthodes d'analyse.

c) *Qui requièrent les services d'une telle unité ?*

- *Les services demandés varient-ils en fonction du demandeur ?*
- *Les besoins de ces demandeurs varient-ils dans le temps ?*

Il est essentiel de savoir quels secteurs d'enquête sont les plus affectés par les technologies de l'information et des communications. En effet, il est peu probable que les transformations apportées par la preuve électronique et les technologies soient uniformes. Il est donc intéressant de se questionner sur la nature des demandeurs et si ces demandeurs se distinguent de par leurs besoins respectifs.

d) *Quels types de crime occupent le plus grand volume de travail ?*

- *Ces tendances évoluent-elles dans le temps ?*

Pareillement, nous croyons que de par la nature de certaines formes de criminalité, ces dernières auront une composante numérique plus ou moins grande. Nous croyons que ce spectre augmentera plus les technologies de l'information et des communications se répandront. Évidemment de tels changements sont susceptibles d'affecter les enquêtes policières.

e) *Quelle est la nature des périphériques expertisés ?*

- *Le matériel analysé évolue-t-il selon les changements technologiques de la société ?*
- *Certains types de périphériques sont-ils surreprésentés ?*

Répondre à ces questions permet d'explorer s'il y a une diffusion des technologies de l'information et des communications chez les délinquants similaire à celle de la société en générale. De plus, cela permet de déterminer si certains types d'appareils sont utilisés plus fréquemment pour la commission de certaines infractions. Ces constatations peuvent contribuer à mieux comprendre la criminalité technologique et donc faciliter le travail des unités œuvrant à la contrer.

- f) *Quelle est l'importance de la preuve numérique pour les enquêtes policières ?*
- *Est-elle essentielle au dépôt d'accusations criminelles ?*
  - *Cette preuve est-elle plus ou moins importante selon le type de crime ?*
  - *Cette preuve augmente-t-elle avec les années ?*

Ici nous cherchons à savoir si la preuve électronique est aujourd'hui essentielle au dépôt d'accusations criminelles. Nous croyons que l'importance relative de la preuve électronique variera en fonction de la nature du crime. Ce fait est susceptible d'affecter grandement les enquêtes policières car s'il s'avère que la preuve numérique est de plus en plus cruciale au dépôt d'accusation pour certaines formes de criminalité, des dispositions particulières devraient être prises au début même de l'enquête. De plus, une augmentation de la quantité de matériel informatique saisi et à analyser est susceptible d'occasionner des délais de traitement additionnels. Ce genre de contrainte peut forcer l'adoption d'innovations permettant de mieux gérer l'affluence des demandes de service acheminées à l'unité.

- g) *Quels sont les défis et les enjeux inhérents à une unité spécialisée en criminalité informatique ?*

Dans la perspective de mieux comprendre les problématiques entourant la création et l'implantation d'une unité spécialisée en criminalité technologique, il est intéressant de se questionner sur les embûches les plus souvent rencontrées. Mieux comprendre ces enjeux permet d'effectuer une meilleure planification et anticiper les problématiques futures. Avoir une bonne compréhension de ces défis et de ces enjeux peut permettre d'éviter certains pièges et ainsi assurer la pérennité de l'unité.

- h) *Quels sont les délais de traitement d'une unité spécialisée en analyse informatique ?*
- *Quel est l'impact de ces délais sur les enquêtes policières ?*

L'analyse et l'extraction des données numériques contenues dans les appareils informatiques saisis sont susceptibles d'occasionner des délais importants. Ces délais peuvent avoir un impact en retardant l'enquête en cours ou en repoussant les procédures judiciaires. Il est

important de comprendre en quoi cette nouvelle réalité est susceptible d'affecter les enquêtes policières en général.

## **5.2. Où se trouvent au Canada les unités spécialisées en criminalité technologique ?**

Les unités spécialisées en criminalité technologique sont de plus en plus présentes dans les organisations chargées d'appliquer la loi. Plusieurs corps policiers et agences gouvernementales possèdent de telles unités, toutefois peu d'informations sont divulguées à leur sujet. Il est à noter que plusieurs firmes privées offrent maintenant des services d'analyse judiciaire informatique au niveau corporatif.

Au Canada, nous avons recensé plusieurs organismes policiers possédant une telle unité. Cette liste n'est pas exhaustive et est constituée à titre indicatif seulement :

- *Police provinciale de l'Ontario (PPO) :*
  - La « Brigade de répression de la criminalité informatique » de la PPO est chargée d'offrir une assistance technique aux détachements provinciaux, aux corps de police municipaux et aux organismes publics de la province de l'Ontario nécessitant l'analyse de périphériques électroniques essentiels à leur enquête (PPO, 2014). De plus cette unité signale une augmentation marquée de la diversité et de la quantité de demandes adressées à leur service due à la forte prolifération des appareils numériques.
  
- *Sûreté du Québec (SQ) :*
  - Selon le site Internet de la Sécurité publique du Québec (2014), les services offerts par la Sûreté du Québec à une municipalité donnée varient en fonction de la population de la ville desservie. Six (6) niveaux de services sont ainsi offerts selon la taille de la ville. Seulement les détachements se trouvant dans une municipalité de 250 000 à 499 999 habitants (niveau de service 3) sont habilités à enquêter les méfaits ou vols concernant des données informatiques.
  - Par contre, la SQ offre dans ses quartiers généraux de Montréal un service complémentaire de soutien (niveau de service 6) lorsqu'un poste ne possède pas les moyens techniques nécessaires à l'enquête.

- À cet effet, le site Internet de la SQ (2014) nous renseigne sur ce service de soutien : « En 2001, la Sûreté du Québec a mis sur pied le *Module de la cybersurveillance et de la vigie* pour s'adapter à la croissance du réseau Internet. En contact permanent avec les policiers de 32 pays, ce service a pour but de surveiller les activités illicites sur le Net. »
  - Le Module de la cybersurveillance et de la vigie de la SQ a quatre mandats :
    - Recevoir les demandes d'assistance;
    - Soutenir et former les membres de la Sûreté du Québec;
    - Exercer un rôle de vigie en matière de cybercriminalité;
    - Évaluer la validité et la pertinence des plaintes.
- *Gendarmerie royale du Canada (GRC) :*
- Créé en 2001, le Programme de la criminalité technologique (PCT) est le programme national de la Gendarmerie royale du Canada (GRC) visant à supporter les enquêtes policières impliquant des éléments technologiques et informatiques (GRC, 2012). De plus, ce programme a comme pour mandat d'enquêter les crimes de nature purement technologique. Le PCT comporte onze unités, les Groupes intégrés de la criminalité technologique (GICT), disposées partout au Canada et une structure de commandement bien établie.
- *Vancouver Police Department (VPD) :*
- L'unité de la criminalité technologique de la Police de Vancouver est composée d'un laboratoire d'analyse judiciaire numérique et d'une équipe de cyberenquêteurs. Le laboratoire est chargé d'effectuer l'analyse des pièces à conviction numérique et d'offrir un support technique à l'ensemble du corps policier tandis que l'équipe de cyberenquêteurs est chargée d'assister les enquêtes nécessitant la recherche et la récupération de preuves sur Internet.

### 5.3. Études connexes sur les unités spécialisées en analyse judiciaire informatique

Récemment certains auteurs ont étudié l'augmentation de la preuve numérique en colligeant des informations issues d'unités spécialisées en analyse judiciaire informatique (Turnbull & al., 2009) ou d'autres sources de données (McMillan & al., 2013; Quick & Choo, 2014). Les résultats obtenus ainsi que leurs conclusions peuvent s'avérer très utiles dans l'optique de valider et de comparer les résultats de la présente étude.

Turnbull et al. (2009) ont examiné comment une organisation policière australienne traite et analyse la preuve électronique obtenue dans le cadre de ses enquêtes criminelles. Les auteurs effectuent une analyse de la quantité et de la nature des périphériques expertisés tout en considérant le lien avec le type d'enquête policière effectué. Entre 2005 et 2008, les résultats démontrent une hausse des demandes d'analyse judiciaire informatique adressées<sup>17</sup> ainsi qu'une augmentation du nombre de pièce à conviction expertisées<sup>18</sup>. Selon les auteurs, l'augmentation du nombre de téléphones cellulaires traités est particulièrement marquée. Finalement, selon les données colligées entre 2006 et 2008, la plus grande demande pour cette expertise provient des enquêtes reliées à la drogue.

McMillan et al. (2013) ont étudié l'augmentation de la preuve électronique issue de téléphones cellulaires et utilisée en Cour au Royaume-Uni. En utilisant trois (3) grandes bases de données d'informations juridiques, les auteurs ont identifiés 537 cas, entre le 1<sup>er</sup> janvier 2006 et le 31 juillet 2011, où le contenu de téléphones cellulaires a servi comme preuve. Les auteurs concluent à une augmentation de la preuve provenant de téléphones cellulaires depuis 2008<sup>19</sup>. De plus, il semble y avoir une corrélation entre la nature de la preuve présentée et le type de criminalité. Par exemple, le dépôt de SMS (messages textes) en tant que preuve est particulièrement utilisé dans le cas de dossiers reliés à la drogue.

---

<sup>17</sup> Passant de 268 en 2005-2006 à 409 en 2007-2008.

<sup>18</sup> Passant de 715 en 2005-2006 à 1265 en 2007-2008.

<sup>19</sup> Ce nombre est passé de 51 en 2006 à 157 en 2010.

Enfin, Quick et Choo (2014) examinent l'implication de l'augmentation de la preuve électronique pour les unités spécialisées en analyse judiciaire informatique. Ils présentent notamment une compilation de données du FBI *Regional Computer Forensic Laboratory* qui fait état de l'augmentation, entre 2003 et 2012, du nombre de demandes de service, du nombre d'analyse effectué ainsi que de la quantité de données traitées. Les auteurs concluent que la quantité de données à traiter s'avèrera un défi de plus en plus important pour les analystes judiciaires qui verront leur arriéré augmenter. Des stratégies d'analyse existent déjà (tel que le data mining) pour parer ce phénomène mais l'auteur propose un cadre permettant d'appliquer plus systématiquement ces techniques. De façon générale il s'agit d'un processus permettant d'élaguer séquentiellement les données non pertinentes à l'enquête tout en intégrant les renseignements pertinents recueillis tout au long de l'analyse. À cet effet, l'auteur met l'emphase sur la nécessité de mettre en place un système de gestion de l'information permettant d'être à tout moment au fait des éléments de preuve susceptibles affecter une ou plusieurs enquêtes en cours.

En résumé, les études présentées pointent vers une augmentation de la demande pour les services d'analyse judiciaire informatique. La preuve numérique s'avère de plus en plus importante en Cour mais aussi de plus en plus volumineuse. Les unités spécialisées en analyse judiciaire informatique devront assurément innover afin de faire face à cette demande croissante.

#### **5.4. Projet de stage**

Nous avons approché une unité policière spécialisée en analyse judiciaire informatique (ci-après « l'Unité ») et celle-ci a bien voulu nous offrir l'opportunité d'effectuer un stage académique à ses bureaux<sup>20</sup>. Le prochain chapitre vise à présenter cette unité, sa mission ainsi que le présent projet de recherche. Il sera question de la collecte de données effectuée, de la constitution d'une base de données composée de l'ensemble des demandes de services adressées à l'Unité ainsi que de la création de variables rendant possible les analyses

---

<sup>20</sup> Le nom de l'unité, de ses membres ainsi que toutes références permettant d'identifier l'unité en question ont été retirés.



statistiques présentées dans les chapitres subséquents. Finalement, une série d'entrevues a été réalisée permettant d'approfondir les questions de recherche formulées précédemment et plus particulièrement la question des enjeux et des défis liés au fonctionnement d'une telle unité.

---

## **Chapitre III**

### **Méthodologie**

---

Le présent chapitre vise tout d'abord à expliquer le fonctionnement interne ainsi que la nature du travail de l'unité spécialisée en analyse judiciaire informatique qui nous a ouvert ses portes. Deuxièmement, ce chapitre décrit en détail la collecte de données effectuée, élabore sur la constitution des variables utilisées pour les analyses et discute des biais méthodologiques.

#### **1. L'Unité spécialisée en criminalité technologique et en analyse judiciaire informatique**

L'Unité est composée actuellement de plusieurs membres chargés de lutter contre les crimes de nature informatique et de fournir une assistance technique aux autres services d'enquête. Concrètement, cette unité est composée de policiers et de membres civils effectuant les expertises judiciaires informatiques et un menant directement un certain nombre d'enquêtes.

Cette unité spécialisée est notamment chargée d'extraire et d'analyser le contenu d'appareils informatiques et électroniques ayant été saisis lors de perquisitions. Les activités de cette unité sont principalement orientées vers l'assistance technique d'autres enquêteurs en faisant la demande.

À ce jour, peu d'auteurs (Turnbull & al., 2009) ont quantifié et examiné le travail des unités policières spécialisées en criminalité technologique. Quelques auteurs (McMillan & al., 2013; Quick & Choo, 2014; Yesilyurt, 2011) ont utilisé des données déjà existantes pour le faire. Nous croyons qu'il est nécessaire d'aller plus loin et d'examiner dans les détails le travail quotidien d'une telle équipe. Suite à une consultation avec les responsables de l'Unité, nous sommes arrivés à la conclusion que l'analyse des demandes de services adressées à leur équipe serait la meilleure façon de comptabiliser leur travail et de suivre son évolution au fil du temps. Il a donc été décidé de compiler l'ensemble des demandes de services effectuées depuis la création de l'Unité.

## **2. Constitution d'une base de données des demandes d'assistance**

### **2.1. Nature et objectif de la base de données**

Cette unité spécialisée offre avant tout une assistance spécialisée aux autres services d'enquête en faisant la requête. Le principal vecteur pour effectuer ces demandes est un document intitulé « Demande d'assistance ».

Les demandes de service envoyées à l'Unité contiennent les informations suivantes :

- Le numéro de dossier;
- Le titre du dossier ou le nom du projet;
- La date du rapport d'incident;
- La date de réception de la demande;
- La provenance de la demande (l'entité ou le service effectuant la demande);
- Les coordonnées du demandeur;
- La nature de l'incident;
- Un bref aperçu de l'enquête en cours;
- La date et les détails des perquisitions exécutées (s'il y a lieu);
- Des précisions concernant les renseignements recherchés (liste de mots-clefs) et l'importance relative de chacune des pièces à conviction soumise;
- Les infractions reprochées et les articles du *Code criminel* reliés;
- Si des accusations ont été portées ou non;
- Des détails sur les autorisations légales (mandats et ordonnances) reliées au dossier;
- S'il y a lieu, la date de comparution et la date procès du ou des accusés;
- Pour plus de précision, des documents explicatifs peuvent être joints à la demande;
- Un rapport détaillé sur les pièces à conviction doit accompagner la demande pour que l'unité accepte d'effectuer l'analyse des pièces (le cas échéant).

Ce document constitue le premier contact entre l'enquêteur faisant la demande d'assistance et les spécialistes de l'Unité. Une fois ce canal de communication ouvert, les deux parties échangeront sur la nature de la requête, sur les informations recherchées et sur l'enquête en cours.

Puisque ce formulaire est systématiquement rempli lorsqu'une requête est effectuée, il reflète fidèlement le volume et la nature du travail de l'Unité. Le formulaire actuel de demande de service a fait son apparition en 2004, il a été toutefois modifié et amélioré au fil des années

mais il contient globalement les mêmes informations; ceci permet donc de faire une analyse longitudinale et comparative de ces informations.

## **2.2. Description générale de la base de données**

Afin d'être en mesure d'analyser adéquatement les demandes de services effectuées à l'Unité, une base de données a été constituée contenant l'ensemble des informations pertinentes se retrouvant sur les formulaires. Plus de 1150 formulaires individuels ont été répertoriés s'échelonnant de juillet 2004 à juillet 2011.

### *2.2.1. Description des principales variables*

Suite à l'analyse des demandes de services, plusieurs variables ont été constituées. Nous pouvons les diviser sommairement en trois (3) grandes catégories :

- 1) Les variables « temporelles » permettent de situer dans le temps les demandes de service. Elles concernent notamment, la date de réception de la demande et la date de l'incident (correspondant également à la date d'ouverture du dossier de police);
- 2) Les variables concernant le demandeur permettent de catégoriser le département d'enquête du demandeur (lors de demandes à l'interne) ainsi que le type d'organisme demandeur (autre service de police, ministère, etc.);
- 3) Finalement, les variables concernant la nature de la demande recoupent une grande variété d'informations contenues dans la demande de service. Nous y trouvons notamment, la nature de l'incident, le type de service rendu, si oui ou non des accusations criminelles ont été déposées au moment de la demande, si oui ou non les pièces à conviction ont été obtenues via un mandat et la nature du matériel analysé (type de périphérique).

Les deux premières catégories de variables ont été entrées fidèlement et de façon exhaustive. Il n'y a donc pas eu de manipulations, de regroupement ou de classification de notre part. Par contre, en ce qui concerne la troisième catégorie de variable, il a été nécessaire de regrouper les cas selon certaines catégories. Ces catégories ont été constituées après que l'ensemble des demandes de services ait été entré dans la base de données et selon les thématiques les plus

fréquemment rencontrées. Les prochaines sous-sections traitent de la création de ces variables et de la justification de ces catégorisations.

*Voir l'annexe 1 pour un tableau présentant de façon détaillée les variables contenues dans la base de données.*

### **2.3. Constitution de la variable « Type de service effectué »<sup>21</sup> et dérivés**

Suite à des conversations avec les membres de l'Unité ainsi qu'à une analyse préliminaire des demandes de service, il a été possible d'établir que quatre principaux types de services sont offerts par leur service. Les quatre catégories suivantes ont donc été constituées : 1) les demandes de services concernant l'analyse de matériel informatique, 2) les demandes d'assistance à la perquisition, 3) les demandes concernant l'extraction de données et 4) les demandes concernant une assistance technique générale.

#### *2.3.1. Demande d'assistance à la perquisition*

Lors d'une perquisition, si les éléments recherchés sont susceptibles de se retrouver sur un support informatique, il est possible de demander l'assistance de l'Unité. Cette dernière se chargera d'effectuer adéquatement la saisie du matériel informatique en s'assurant que l'intégrité des informations contenues dans le matériel perquisitionné soit préservée.

Certains appareils électroniques, notamment les cellulaires intelligents, possèdent des mécanismes assurant la destruction à distance des données contenues dans les mémoires internes. S'assurer d'isoler ces périphériques de tout réseau de communication est un exemple de précaution à prendre lors de leur saisie. De plus, de façon générale une saisie mal effectuée pourrait conduire à l'altération des données et soulever des contestations de la partie défenderesse quant à l'authenticité de la preuve soumise.

#### *2.3.2. Demande d'analyse*

Dans notre base de données, le terme « analyse » réfère à un examen en profondeur des données digitales contenues dans un disque dur ou un autre média de stockage. Cette analyse

---

<sup>21</sup> Variable nommée [To\_do] en annexe 1.

en profondeur est effectuée à l'aide de logiciels spécialisés d'analyse judiciaire informatique (par exemple, EnCase ou FTK). Dans la majorité des cas, une image miroir du périphérique est préalablement faite afin de préserver l'intégrité de la pièce à conviction.

### *2.3.3. Demande d'extraction de données*

L'extraction de données consiste à soutirer l'ensemble des données contenues dans un périphérique et d'en remettre le contenu à l'enquêteur principal au dossier. Initialement, il n'y a donc pas d'analyse judiciaire effectuée par le membre de l'Unité. Cette méthode est particulièrement utilisée dans le cas de cellulaires traditionnels (non intelligents), mais ceci est également vrai pour un certain nombre d'autres périphériques électroniques et digitaux tels que des enregistreurs numériques, des terminaux « ATM », des photocopieurs, etc.

En 2014, la majorité des cellulaires vendus sur le marché sont dits « intelligents ». Ces appareils sont considérés comme des mini-ordinateurs. Un spécialiste de l'extraction de données de l'Unité nous a confié qu'il n'y a pratiquement plus de différences entre les cellulaires et les ordinateurs conventionnels; ceux-ci contenant presque autant d'informations que leur homologue.

Conséquemment, les cellulaires intelligents ont généralement été classés dans la catégorie analyse plutôt qu'extraction, ces derniers nécessitant un examen en profondeur de leur contenu afin de récupérer l'ensemble des données présentes sur ledit appareil.

### *2.3.4. Demandes d'assistance technique*

Les demandes d'assistance technique recourent une vaste gamme de services demandés à l'Unité. Il peut s'agir de déterminer la provenance d'une adresse IP, d'effectuer la copie d'un CD ou d'un DVD, d'aider à la rédaction d'un mandat de perquisition contenant des aspects très techniques ou encore une demande de support informatique à l'interne. De plus, des questions techniques ou des demandes spéciales peuvent être acheminées afin de solliciter l'expertise des membres de l'Unité.

### 2.3.5. Création de la variable dichotomique « expertise ou assistance »<sup>22</sup>

Les quatre principaux types de services offerts par l'Unité peuvent être divisés en deux grandes catégories générales : les demandes concernant une expertise (l'analyse et l'extraction de données) et les demandes concernant une assistance. Il y a une importante distinction entre ces deux catégories. La première concerne des manipulations de pièces à conviction dont la preuve numérique est susceptible d'être déposée en Cour. La seconde catégorie concerne plutôt de l'aide à l'obtention de ces preuves numériques. De plus, le fait de rendre « dichotomique » cette variable va faciliter les analyses ultérieures et faciliter l'interprétation des données.

### 2.4. Constitution de la variable « Type d'incident »<sup>23</sup>

La variable catégorielle « type d'incident » a été créée afin de donner une idée générale du sujet du dossier d'enquête policière relié à la demande d'assistance. Les demandes ont donc été regroupées selon les catégories les plus fréquemment rencontrées. Ces catégories sont les suivantes :

- 1) Fraude (incluant la fraude, la contrefaçon, l'utilisation de faux documents, le télémarketing frauduleux et la fabrication de cartes de crédit)
- 2) Stupéfiant (incluant la production, la vente, le trafic, l'importation et l'exportation de stupéfiants, la contrebande de produits du tabac, la possession de tabac non estampillé et avoir comploté l'une ou l'autre des infractions mentionnées)
- 3) Criminalité organisée (incluant le blanchiment d'argent, le gangstérisme, le recyclage des produits de la criminalité, la corruption et le trafic d'influence)
- 4) Télécommunication (concerne principalement la *Loi sur la radiocommunication*; incluant principalement l'interception ou le vol de signaux satellites)
- 5) Droits d'auteur (concerne principalement la *Loi sur le droit d'auteur*; incluant la possession ou la vente de copies illégales, la contrefaçon de CD et DVD et l'utilisation illégale de marques commerciales enregistrées)

---

<sup>22</sup> Variable nommée [To\_do\_dicho] en annexe 1.

<sup>23</sup> Variable nommée [Type\_incident] en annexe 1.



- 6) Sécurité de l'état (incluant le financement et les menaces terroristes, les alertes à la bombe, l'immigration illégale et le trafic humain)
- 7) Pornographie juvénile (incluant la possession, la production et la distribution de matériel pornographique juvénile et le leurre d'enfant)
- 8) Homicide, harcèlement et menaces de mort (incluant également l'extorsion, la séquestration et l'intimidation)
- 9) Piratage et crimes informatiques
- 10) Assistance technique (incluant l'assistance à la perquisition, l'appui à un autre corps policier, déterminer une adresse IP, copier des données, déchiffrer<sup>24</sup> des données, répondre à des demandes de renseignement, assistance technique à l'interne et récupération de données perdues)
- 11) Autres<sup>25</sup> (incluant notamment, entrave à la justice, cas de déontologie, vols, liberté illégale, bris de condition, possession non autorisée d'armes à feu, etc.)

Dans le cas où plusieurs thématiques étaient concernées, l'infraction principale ou la plus grave a été retenue. Par exemple, dans un dossier relatif aux stupéfiants, si un homicide a également été commis, il sera classé dans la catégorie « homicide et menaces de mort ». Similairement, un dossier concernant un cas de vente de stupéfiants ayant une composante importante de criminalité organisée sera catégorisé sous « crime organisé ».

### **2.5. Constitution de la variable « La demande spécifiait-elle du matériel à analyser ? »<sup>26</sup>**

Lorsqu'une demande de service concerne du matériel informatique, peu importe la nature de la demande, le type et la quantité de ces appareils ont été consignés<sup>27</sup>. Si la demande ne faisait aucunement référence à du matériel informatique, zéro (0) était indiqué à chacune des variables. Par la suite, une variable faisant la somme totale [Mat\_total] du nombre d'appareils électroniques a été créée.

---

<sup>24</sup> Nous parlons ici de l'analyse de données encryptées.

<sup>25</sup> Cette catégorie a été créée car de nombreux cas ne recoupaient aucune catégorie et était unique en leur genre.

<sup>26</sup> Variable nommée [Mat\_Saisi] en annexe 1.

<sup>27</sup> Treize (13) variables différentes ont été créées afin d'inclure tous les types de périphériques rencontrés. Les catégories sont par exemple le nombre : d'ordinateurs, de téléphones cellulaires, de téléphones intelligents, de disques durs, etc. Voir l'annexe 1 pour la liste complète des catégories créées.

Lorsque la demande faisait référence à du matériel mais que le nombre d'items saisi était indéterminé, nous avons choisi de comptabiliser le résultat comme si un (1) seul item avait été saisi. De la même manière, lorsque le nombre d'items saisis était indéterminé mais qu'il y avait une référence à plus d'un item saisi (exemple : analyse de plusieurs disquettes) nous avons choisi, de façon conservatrice, d'indiquer deux (2) items. Il est dès lors envisageable que cette décision ait comme effet de sous-estimer le nombre d'items saisis. Par contre, cela permet de maximiser les informations disponibles et permet de constituer une variable très pertinente pour les analyses subséquentes. Par exemple, cela permettra d'estimer le nombre total de périphériques traités par année ou encore de comparer si certaines formes de criminalité entraînent une plus grande quantité de pièces à analyser.

Il importe également de préciser que les capacités de stockage des différents périphériques varient grandement d'un item à l'autre et varient également dans le temps. Si nous nous fions à la « loi de Moore », la capacité des périphériques analysés aura au moins octuplé entre le début (2004) et la fin (2011) de notre période. La quantité de périphériques de stockage spécifié dans la demande n'est donc pas nécessairement associée à la quantité de données numériques à traiter.

En effectuant l'analyse préliminaire de la variable « nombre total d'appareils électroniques », il s'est avéré que la majorité des résultats était soit zéro (0 - aucun matériel de spécifié) ou un (1 - un seul appareil spécifié). Nous avons donc choisi de recoder la variable de façon dichotomique afin de faciliter la compréhension et les analyses ultérieures. La nouvelle variable créée répond donc à la question suivante : « la demande faisait-elle référence à du matériel ? ».

## **2.6. Constitution de la variable « Différence entre la date de réception et de l'incident »<sup>28</sup>**

Cette variable a été calculée en soustrayant la date de réception de la demande de service à la date déclarée de l'incident. Le résultat, en jours, donne le délai qui s'est écoulé entre l'incident

---

<sup>28</sup> Variable nommée [Date\_diff] en annexe 1.

et la demande de service. Par exemple, si un dossier de fraude est ouvert le 14 mars 2014 et que subséquemment une demande d'analyse pour une pièce à conviction est envoyée le 25 avril 2014, la variable indiquera 42 jours.

Suite à l'analyse de la variable créée, plusieurs modifications ont été effectuées afin de rendre les analyses possibles. Premièrement, nous avons constaté que certains résultats étaient négatifs; ce qui voudrait dire que la demande est effectuée avant l'incident. Or, ceci étant logiquement impossible, ce phénomène est dû à l'absence d'une date sur les formulaires ou à une erreur sur le formulaire. Toutes les données négatives ont donc été traitées en tant que données manquantes. Également, les quelques données supérieures à 1000 jours ont été traitées en tant que données éloignées et ont donc été ramenées à la valeur maximale de 1000 jours. Ceci évite de gonfler la moyenne artificiellement et ainsi de mener à une interprétation erronée des données.

### **3. Autres sources de données et considérations méthodologiques**

Suite à l'analyse préliminaire des données recueillies, certains résultats ont été présentés à des membres de l'Unité afin d'obtenir une meilleure compréhension de leur signification. Des questions complémentaires concernant leur travail et les impératifs auxquels ils doivent répondre ont aussi été posées. Ces questions permettent de valider plusieurs interrogations et hypothèses formulées précédemment et de mieux répondre à nos propres questions de recherche.

Ainsi, le 17 juillet 2014, deux groupes de discussion ont été menés avec des membres de l'Unité. Une première rencontre a été effectuée avec deux analystes civils ayant respectivement 7 et 12 années d'expérience au sein de la section (ci-après désignés respectivement comme A1 et A2). Une deuxième rencontre a été menée avec deux policiers de l'Unité ayant respectivement 4 et 8 années d'expérience à l'Unité (ci-après désignés respectivement P1 et P2).

De plus, une entrevue a été effectuée avec un inspecteur d'une agence gouvernementale présentement en formation à l'Unité. Cette rencontre fortuite a permis d'obtenir des

informations sur les défis reliés à la création d'une unité spécialisée en analyse judiciaire informatique.

En outre, tout au long du projet (de juin 2011 à août 2014) de nombreux échanges courriels ont eu lieu afin de clarifier certains éléments et préciser le projet. Ces échanges ont principalement eu lieu avec A2, chef d'équipe des analystes civils de l'Unité. L'ensemble de ces informations de nature qualitative permet de bonifier les réflexions, faciliter l'interprétation des résultats obtenus et assurer la validité des analyses effectuées. Ces entrevues permettent aussi de rationaliser certains phénomènes ou tendances observées dus principalement à des facteurs organisationnels; sans ces interactions avec les membres de l'Unité il aurait été difficile, voire impossible, de déduire la signification de certains résultats.

### **3.1. Limites et biais méthodologiques de la présente étude**

Les données recueillies sont de nature administrative et n'ont donc pas été conçues dans l'optique d'une analyse scientifique. C'est-à-dire qu'aucun système d'évaluation ou de collecte de données n'a été mis au point à ce jour; nous devons donc manuellement colliger les données. Ceci a plusieurs conséquences importantes, dont le nombre important de données manquantes pour certaines variables constituées. Ceci est particulièrement vrai pour les demandes de service adressées au tout début de l'Unité. Ces premiers formulaires étaient remplis de façon maladroite et plusieurs informations étaient manquantes ou parfois illisibles. Ceci était probablement dû au caractère nouveau de ce type de demandes; les services requérants ne sachant pas comment adresser adéquatement ce type de demande. De plus, très souvent, peu de détails concernant le matériel à expertiser ou l'enquête en cours étaient disponibles.

Au cours des années le formulaire « Demande d'assistance » a évolué, devenant plus complet et plus précis. Des indications plus claires facilitent la tâche des demandeurs et ces derniers ont aussi plus d'expérience à effectuer les demandes. Conséquemment, les formulaires remplis à la fin de la période d'analyse le sont avec une plus grande aise et comportent plus de détails. Qui plus est, ces informations complémentaires, souvent sur la nature de l'enquête, ne sont pas

seulement utiles pour la présente étude elles le sont également pour les membres de l'Unité qui en ont besoin pour effectuer leurs analyses.

Quoi qu'il en soit, cet effet est susceptible de se refléter dans les analyses effectuées. En d'autres termes, plus les années passent plus les données sont complètes. Par contre, le nombre total de demandes de service envoyées à l'Unité est exact car une demande doit être impérativement complétée pour qu'un service soit offert au demandeur. La fiabilité de cette information est donc très grande.

Une dernière considération méthodologique importante est qu'une partie appréciable des variables constituées est catégorielle. Plusieurs méthodes d'analyses statistiques permettent de prendre en charge les variables catégorielles mais elles favorisent les variables dichotomiques (deux groupes). En l'espèce, nous avons de nombreuses catégories ce qui risque de réduire les choix s'offrant à nous. Pour ces raisons, les statistiques descriptives (fréquences), les tableaux de contingences (tableaux croisés) et certaines analyses bivariées considérant les variables de plus de deux groupes seront des types d'analyse retenus.

---

## **Chapitre IV**

**Caractériser le travail d'une unité policière  
spécialisée en analyse judiciaire informatique**

---

Ce chapitre présente les résultats des analyses descriptives effectuées en vue de caractériser le travail d'une unité spécialisée en criminalité technologique. Ces analyses permettront d'esquisser des réponses aux questions de recherches formulées précédemment<sup>29</sup>.

Chaque sous-section du présent chapitre est construite de façon similaire : dans un premier temps, les résultats de l'analyse, accompagnés de tableaux et de figures, sont présentés. Par la suite, des explications et des commentaires sont formulés. Les constatations effectuées sont interprétées, corroborées ou infirmées à l'aide des informations recueillies directement auprès des membres de l'Unité. Finalement, un bref résumé rappelle les principales implications et conclusions de la sous-section.

La première sous-section fait état du nombre de demandes de services adressées à l'Unité pour chacune des années de la période d'analyse. Cette analyse permet d'estimer le volume de travail de cette unité spécialisée. La deuxième sous-section effectue une analyse mensuelle des demandes de service afin d'examiner l'effet saisonnier. La troisième sous-section détaille les types de service offerts par l'Unité, soit : l'analyse judiciaire, l'assistance à la perquisition, l'extraction de données et l'assistance technique. Le nombre de demandes relatif à de chacun de ces types de service est détaillé par année. Cet exercice permet de mieux comprendre la nature du travail de l'Unité et quelles activités occupent le plus grand volume de travail. De plus, il sera possible d'observer si certaines tendances se dessinent au fil des années. La quatrième sous-section analyse les entités adressant des demandes de service à l'Unité. Cette analyse permet de déterminer quel est le profil des clients nécessitant le plus fréquemment les services d'une unité spécialisée en soutien informatique et en criminalité technologique. La cinquième sous-section explore la question suivante : « Quels types de crime occupent le plus grand volume de travail ? » afin de déterminer s'il s'agit de crimes informatiques, ou au contraire de crimes classiques pour lesquels la technologie devient un accessoire privilégié. De plus, les données présentées permettent de déterminer quelle forme de criminalité génère la plus grande charge de travail et si cette tendance évolue en fonction du temps.

---

<sup>29</sup> Voir chapitre II, section 5.1.

La sixième sous-section décrit la nature du matériel expertisé par l'Unité. Avec cette information il sera possible de tracer un portrait de l'évolution des technologies utilisées par les délinquants et donc leur modalité d'adoption des nouvelles technologies. De plus, cette analyse permet d'examiner la propension des délinquants à l'innovation. Dernièrement, cela informe sur quel genre de périphérique une unité spécialisée en analyse judiciaire informatique doit traiter le plus fréquemment.

Finalement, il est à noter que dans la majorité des cas, les données présentées dans ce premier chapitre sont issues de dénombrements, subdivisés par années. Les tendances observables décrites sont donc le résultat d'une constatation visuelle des données. Même si à ce stade aucune analyse statistique n'assure la force ou la signification des tendances observées, ces données descriptives contribuent à une meilleure compréhension du phénomène étudié.

## 1. Les analyses descriptives exploratoires

### 1.1. Analyse générale du nombre de demandes de services adressées à l'Unité

La Figure 4 présente le nombre de demandes de service adressées à l'Unité entre 2004 et 2013. Ceci permet d'esquisser un premier portrait du volume de travail annuel de cette équipe.

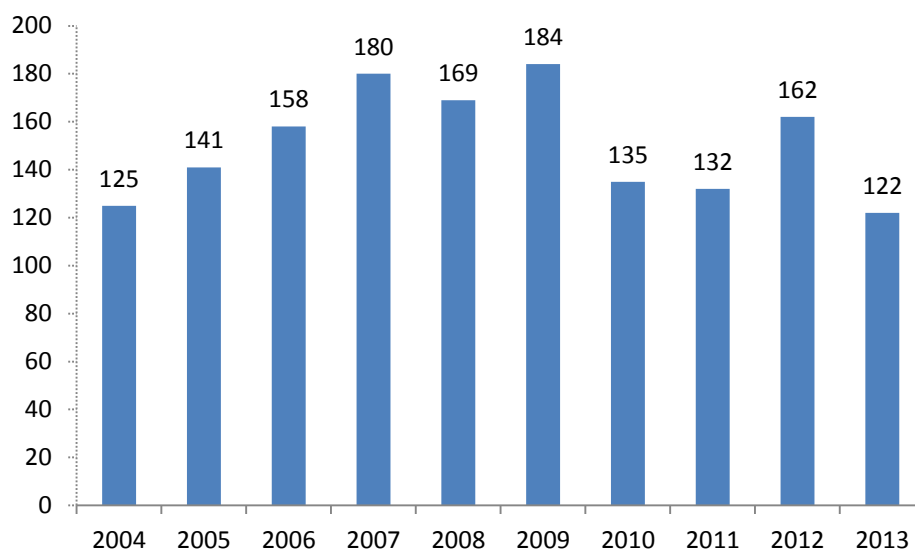


Figure 4. Nombre de demandes de service adressées à l'Unité par année de 2004 à 2013. Le total des années 2011, 2012 et 2013 a été fourni par l'Unité après notre collecte de données de l'été 2011 afin de bonifier l'analyse.



De 2004 à 2009, il y a une augmentation générale du nombre de demandes adressées à l'Unité par année; l'année 2008 n'étant que légèrement en dessous de la tendance. Par contre, les années 2010 à 2013 brisent cette tendance en affichant un nombre de demandes d'environ 25% inférieur; à l'exception de l'année 2012 qui compte un total comparable à l'année 2006.

À première vue, ces résultats semblent difficilement explicables puisqu'on aurait pu s'attendre au minimum à une hausse relativement constante et homogène des demandes de service (McMillan & al., 2013; Quick & Choo, 2014; Turnbull & al., 2009). En effet, vu la place de plus en plus importante prise par la technologie dans notre vie quotidienne, il semble logique que les demandes soient généralement en hausse.

L'explication de cette baisse peut être due à des facteurs de nature organisationnelle ou encore de nature environnementale. Du point de vue des facteurs exogènes, il est peu probable que cette baisse soit due à la diminution de la criminalité ayant une composante informatique. Par contre, il est possible qu'une baisse du financement extérieur (Randol, 2013) ou que des conditions économiques difficiles affectent la quantité de demandes envoyées. Le manque de ressource pouvant limiter la quantité d'enquêtes et le nombre d'opérations d'envergure pouvant être menées simultanément.

Les facteurs endogènes semblent donc offrir de meilleures pistes de solution. En effet, il est possible que certaines réorganisations administratives soient à l'origine de ces fluctuations. Parmi les causes possibles, notons : la modification de la façon dont les demandes de service sont adressées et compilées, la réaffectation de certains membres du personnel ou encore le filtrage des demandes de service envoyées à l'Unité. Afin de vérifier ces hypothèses et de mieux comprendre les résultats observés, ces derniers ont été présentés à certains membres de l'Unité lors de deux groupes de discussions.

#### *1.1.1. Éléments soulevés par les membres de l'Unité*

A2 est analyste judiciaire senior à l'Unité depuis 2002; il attribue cette baisse des demandes à l'instauration d'un programme de triage durant cette période. En effet, par le passé l'Unité pouvait recevoir, suite à une perquisition, plusieurs appareils à analyser, que ce soit des

ordinateurs ou des téléphones cellulaires, alors que parmi ceux-ci seulement quelques appareils étaient pertinents pour l'enquête. On a donc demandé aux partenaires de trier les appareils et de remettre pour analyse seulement les appareils pertinents. Pour ce faire, on a offert une formation sur les outils de triage existant aux enquêteurs qui avaient parfois peu ou pas de connaissances informatiques.

Selon les membres de l'Unité, le résultat de ce programme est d'avoir significativement réduit les demandes adressées à leur unité, surtout celles concernant des téléphones cellulaires dits simples (style « *flip-phone*<sup>30</sup> »).

En investiguant plus profondément l'impact de ce programme, nous avons obtenu auprès de l'Unité des statistiques concernant les cellulaires analysés par un tiers formé par leur équipe. Durant l'année 2012, l'Unité a formé vingt et un (21) membres de leur organisation, appartenant à d'autres sections, à l'analyse de cellulaires. Cette année-là seulement, plus de 70 appareils cellulaires ont été analysés par ces individus. Ceci a permis d'éviter qu'une quarantaine de demandes de services ne soient envoyées à l'Unité. Ce nombre correspond à 25% de toutes les demandes envoyées cette année-là. Théoriquement, cette initiative a permis d'éviter une charge substantielle de travail. En pratique, la majorité de ces demandes auraient été refusées puisque les critères de sélection des demandes de service ont été grandement resserrés au fil des années. Malgré ce succès apparent, il semble que personne d'autre n'ait été formé durant l'année 2013, toutefois des formations sont planifiées pour l'année 2014.

A2 souligne une limite importante de ce programme. Puisque ce dernier visait principalement les téléphones cellulaires simples, qui sont relativement faciles à analyser, l'efficacité de ce programme risque de s'effriter avec le temps. En effet, de plus en plus de téléphones intelligents sont disponibles sur le marché, et ce, à de faibles coûts. Conséquemment, ils risquent de complètement remplacer les téléphones d'ancienne génération d'ici quelques années, rendant ainsi le programme - dans son état actuel - désuet.

---

<sup>30</sup> Téléphone à rabat.

Les analystes rencontrés ont également fait part que depuis deux ou trois années, un système de triage a été mis en place de façon à filtrer les demandes de services envoyées à l'Unité. À ce sujet, A2 mentionne qu'il y a une liste de dossiers majeurs qui sont priorisés établie par le commandement de l'organisation policière et cette liste peut être sujette à changement selon les dates d'audiences devant la Cour.

De plus, à la question « Est-ce que certaines demandes sont priorisées ? », A2 répond que toutes les demandes sont filtrées pour établir une priorité de traitement. Il fut une époque où l'ensemble des demandes étaient traitées par l'Unité, mais maintenant on fait un tri afin de s'assurer d'accepter seulement les demandes qui pourront être traitées de façon réaliste.

Selon A2, c'est l'enquêteur qui a maintenant le fardeau de démontrer pourquoi l'analyse de leur pièce à conviction est essentielle à leur dossier. De plus, une série de critères sont utilisés pour coter les dossiers en cours. Ils tiennent compte principalement de la valeur probante de la pièce à conviction pour l'enquête mais aussi de l'imminence de la menace, de l'atteinte à la vie humaine ou à la sécurité de l'état, de la proximité des dates de comparution et des priorités organisationnelles. Pour des fins d'impartialité, les détails exacts de ce calcul de priorisation sont inconnus des membres de l'Unité. Ceci évite également d'avoir à choisir arbitrairement l'ordre des dossiers à prioriser; de façon générale, ceci constitue un avantage pour eux, car ils n'ont qu'à consulter la liste de dossiers prioritaires afin d'accepter ou de refuser une demande. Il est important de mentionner que l'ensemble des participants ont précisé, à un moment ou à un autre, que le temps investi pour une demande peut grandement varier. Ceci est explicable par le fait qu'une demande peut être accompagnée d'un ou plusieurs périphériques. Qui plus est, la nature de la preuve recherchée et les caractéristiques du périphérique analysé sont également susceptibles d'influencer la durée des expertises. Conséquemment, il faut être prudent dans l'interprétation du nombre de demandes de service reçues par années en tant qu'indicateur du volume de travail.

### *1.1.2. Synthèse*

À la lumière de ces explications, il semble qu'un processus de diffusion s'est opéré afin de soulager la pression due à l'augmentation des demandes de services. Cette diffusion a pris la

forme de formations dispensées à certains membres des autres sections et départements de l'organisation. Les individus ainsi formés sont en mesure d'effectuer les analyses les plus simples.

Avec l'expérience et les années, il a été vite constaté par le commandement de l'organisation que leur unité spécialisée en criminalité informatique a une capacité de traitement limitée. Ainsi, des stratégies ont été mises en place afin de prioriser et filtrer les demandes envoyées à l'Unité. Un système de classement permet d'évaluer la priorité des demandes adressées. De plus, les critères pour qu'une demande soit acceptée ont été resserrés.

Finalement, certains impératifs organisationnels entraînent la réallocation rapide des effectifs sur des projets majeurs ce qui peut paralyser momentanément les activités. Ces dernières constatations sont en accord avec les conclusions de Manning (2008) qui stipulent qu'à tout moment des urgences ou des priorités forcent l'ensemble de l'organisation à réagir à l'événement en relocalisant une grande partie de ses effectifs.

## 1.2. Analyse mensuelle du nombre de demandes adressées à l'Unité

Dans un deuxième temps, il est pertinent d'examiner la répartition des demandes de service adressées à l'Unité en fonction des mois de l'année afin de vérifier si un effet saisonnier est présent. La Figure 5 présente le résultat de cette analyse :

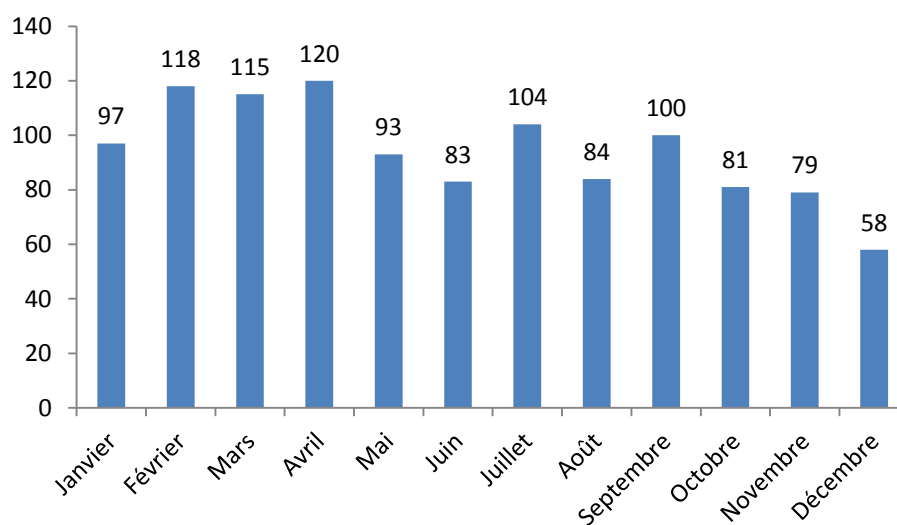


Figure 5. Nombre de demandes de service adressées à l'Unité selon le mois, de janvier 2004 à août 2011.

À première vue, les mois de février, mars et avril se démarquent du lot. Encore une fois nous avons cherché à comprendre ce qui pourrait expliquer ce phénomène. En 2011, un membre de l'Unité avait été questionné à ce sujet et selon lui, ceci est dû au fait que la majorité des opérations policières majeures sont effectuées au printemps ou à l'automne. Conséquemment, la période hivernale est très chargée puisque la plupart des demandes découlant de ces opérations sont envoyées à ce moment. Cet effet saisonnier n'est pas négligeable car il est susceptible de doubler l'affluence des demandes de service.

À ce sujet A2 explique également que souvent les perquisitions d'importance seront planifiées avant la période estivale et la période de vacances.

Également, l'analyste civil A1 ajoute que c'est en fonction des demandes relatives à la Cour. Les demandes urgentes, en vue d'une comparution rapprochée, sont acheminées avant la fermeture estivale. Finalement, il argumente que c'est possiblement une question de budget. Les budgets excédentaires de fin d'année financière poussent les unités à accélérer la cadence.

La Figure 6 fait état du nombre de demandes de service reçues par mois de janvier 2004 à août 2011. Elle permet d'avoir une vue d'ensemble de l'entièreté de la période d'analyse. À l'examen de ce graphique, le mois de mars 2007 se démarque des autres, l'Unité ayant reçu trente demandes dans ce seul mois. En consultant les demandes de services effectuées durant ce mois, nous constatons qu'elles découlent de deux principales opérations.

Nous pouvons conclure que le volume de travail de l'Unité est variable et grandement influencé par les aléas des opérations policières d'envergure. Anticiper l'affluence de ces demandes de service pourrait s'avérer un atout considérable. Sans aborder spécifiquement cette question, il appert que la communication entre les différentes sections soit essentielle à un tel processus.

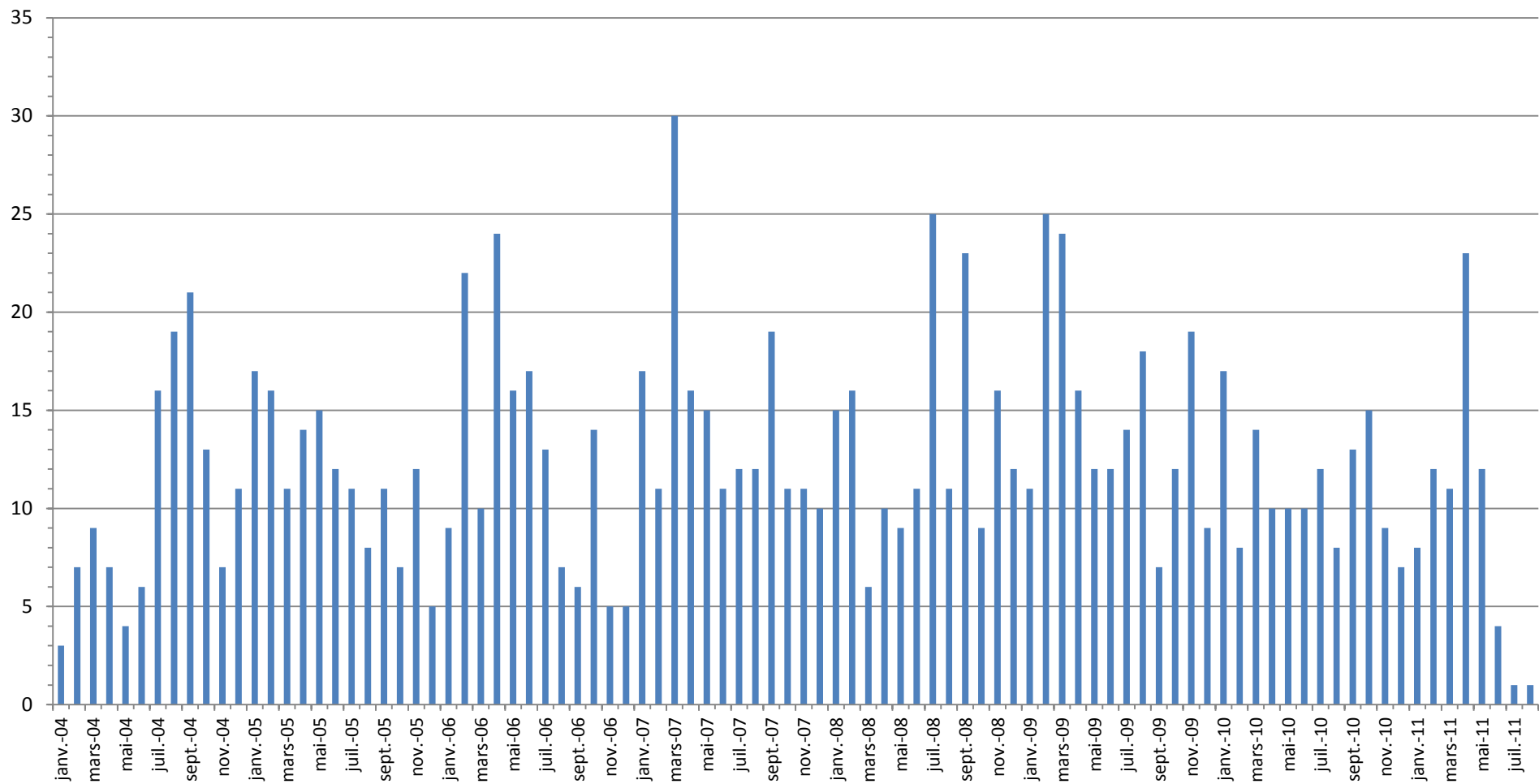


Figure 6. Histogramme du nombre de demandes de service adressées par mois à l'Unité de janvier 2004 à août 2011.

### 1.3. Analyse des types de services rendus par l'Unité

Le Tableau 2 et la Figure 7 présente le nombre de demandes de services par année en fonction du type d'expertise requis. Le but de ce tableau est premièrement d'observer la répartition des tâches effectuées, puis de suivre leur évolution dans le temps. Par la suite, il sera possible de constater s'il y a des tendances ou une évolution de la nature des demandes de services adressées à l'Unité. Voici les résultats obtenus :

Tableau 2

*Nombre de demandes adressées par années à l'Unité selon le type de service effectué*

Année	Analyse	Assistance perquisition	Extraction de données	Assistance technique	Données manquantes	Total
2004	30	30	21	39	5	<b>125</b>
2005	38	30	17	50	6	<b>141</b>
2006	32	30	30	48	18	<b>158</b>
2007	54	36	39	42	9	<b>180</b>
2008	59	32	34	40	4	<b>169</b>
2009	62	29	41	42	10	<b>184</b>
2010	38	18	30	47	2	<b>135</b>
<b>Total</b>	<b>313</b>	<b>205</b>	<b>212</b>	<b>308</b>	<b>54</b>	<b>1092</b>

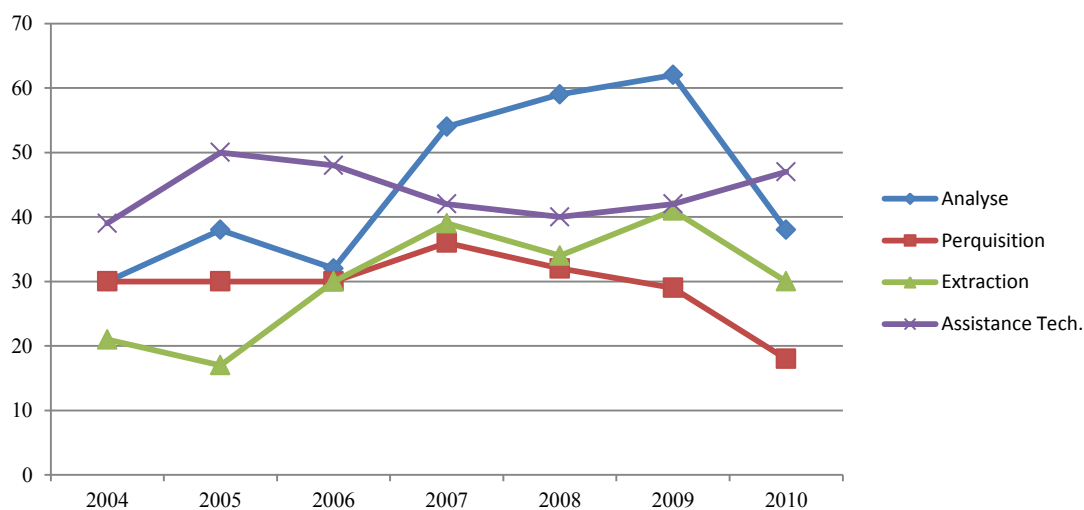


Figure 7. Représentation graphique du nombre de demandes de service adressées par années à l'Unité selon le type de service effectué.

Les types de demande les plus fréquemment adressées à l'Unité sont celles d'analyse et d'assistance technique. L'Unité reçoit en moyenne 44 demandes par année de chacune de ces deux catégories. En ce qui concerne les demandes d'aide à la perquisition et d'extraction de données, elles sont moins fréquentes; environ 30 de chacune de ces deux catégories sont acheminées à l'Unité par années.

En examinant les tendances annuelles, il est possible de constater qu'entre 2006 et 2009 il y a eu une augmentation marquée du nombre de demandes concernant spécifiquement les analyses informatiques. Les demandes concernant l'aide à la perquisition sont en déclin depuis 2007 pour atteindre leur point le plus bas en 2010. Depuis 2005, les demandes concernant de l'extraction de données connaissent une hausse similaire à celle d'analyse.

Tous les types de demandes chutent en 2010 à l'exception des demandes concernant de l'assistance technique. Cette baisse est principalement due à la chute généralisée des demandes observée précédemment (voir l'année 2010 de la Figure 4). En ce qui concerne les demandes d'assistance technique qui augmentent, ce phénomène pourrait être la conséquence des changements administratifs instaurés. En effet, le système de triage mis en place affecte uniquement les demandes incluant des pièces à conviction visant ou la saisie de celles-ci (assistance à la perquisition); il en va de même pour le programme de formation. Puisque les demandes d'assistance technique recourent une vaste gamme de service que seul l'Unité peut dispenser, il est raisonnable de croire que ce genre de demandes ne serait pas affecté les initiatives administratives mises de l'avant.

### *1.3.1. Éléments soulevés par les membres de l'Unité*

Concernant la baisse observée des demandes relative à une assistance à la perquisition, A2 explique que cela fluctue mais que c'est normalement relativement stable. A1 rétorque en émettant l'hypothèse qu'il y a maintenant de plus en plus de perquisitions majeures et de moins en moins de petites perquisitions isolées, ce qui aurait pour effet de réduire le nombre de demandes. Ainsi il est probable que les demandes d'assistance pour une série de perquisitions soient maintenant faites via le même formulaire.



A2 explique aussi qu'il est impossible pour eux de connaître de façon approfondie tous les dossiers de la division. Conséquemment, ils procèdent de plus en plus fréquemment à l'extraction des données et délèguent la tâche d'analyse aux enquêteurs au dossier en leur fournissant les outils de visionnement adéquats. Il est plus facile pour les enquêteurs de savoir exactement ce qui est recherché et quant à eux, les membres de l'Unité peuvent ainsi se concentrer sur les tâches nécessitant leur expertise de façon plus pointue.

A1 explique que le volume de données à analyser informatiquement est de plus en plus élevé puisque des preuves qui étaient auparavant sous forme papier sont maintenant sous support numérique.

Finalement, tous les intervenants de l'Unité rencontrés mentionnent que ce qui détermine réellement le type d'analyse effectué est la nature de la preuve recherchée et la nature du périphérique analysé.

### *1.3.2. Synthèse*

L'analyse du nombre de demandes de service par années selon le type de service effectué tend à confirmer que les programmes de tirage et de formation ont eu un impact réel sur le nombre de demandes de service adressées à l'Unité; spécifiquement sur les demandes d'analyse. Ceci est confirmé par le fait que les demandes d'assistance technique sont stables et ne sont pas affectées par les mesures de gestion mises en place.

Puisque l'organisation se concentre de plus en plus sur des projets et des opérations majeurs, les perquisitions sont plus ciblées et regroupées ce qui entraîne une baisse des demandes concernant ce type d'assistance.

Finalement, selon les intervenants de l'Unité, ils procèdent de plus en plus à l'extraction des données afin de permettre aux enquêteurs d'effectuer eux-mêmes l'analyse des données extraites. Ceci permet de les soulager de cette lourde tâche afin qu'ils puissent se concentrer sur des mandats nécessitant leur expertise technique de façon plus pointue.

#### 1.4. Analyse du profil des départements adressant les demandes de service

Le Tableau 3 et la Figure 8 dénombrent la quantité de demandes de services envoyées à l'Unité par années selon différents requérants internes et externes. Ceci permettra d'ordonner ces demandeurs selon leur importance relative et d'examiner s'il y a évolution de ces tendances tout au long de la période d'analyse.

Tableau 3

*Nombre de demandes de service par années par département demandeur*

Département demandeur	2004	2005	2006	2007	2008	2009	2010	Total
Criminalité économique	33	40	43	61	67	90	56	<b>390</b>
Criminalité organisée	39	28	56	48	47	21	23	<b>262</b>
Sécurité étatique	34	35	30	52	32	31	34	<b>248</b>
Autre service de Police	11	25	16	11	16	30	14	<b>123</b>
Support aux opérations	1	2	3	3	2	3	5	<b>19</b>
Renseignements criminels	0	1	2	3	0	1	0	<b>7</b>
Services de protection	1	1	0	0	0	1	0	<b>3</b>
Données manquantes	6	9	8	2	5	7	3	<b>40</b>
<b>Total</b>	<b>125</b>	<b>141</b>	<b>158</b>	<b>180</b>	<b>169</b>	<b>184</b>	<b>135</b>	<b>1092</b>

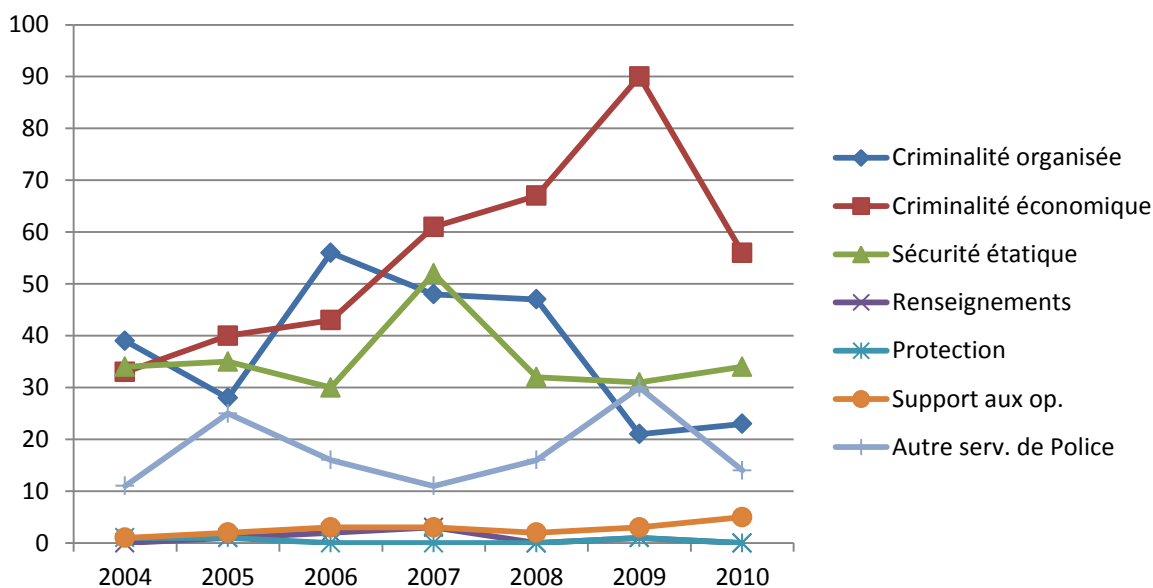


Figure 8. Représentation graphique du nombre de demandes de service adressées par années à l'Unité selon le département effectuant la demande.

Une des premières constatations pouvant être faites est que le département de la criminalité économique nécessite grandement les services de l'Unité. De 2004 à 2009, c'est le département qui a vu ses besoins le plus rapidement progresser avec une augmentation moyenne de 22,9% de ses demandes par année. De plus, entre 2007 et 2010, section unité a effectué plus du tiers (35,7%) des demandes; en 2009 seulement, le département de la criminalité économique a fait près de deux fois plus de demandes que tous les autres départements confondus.

De façon générale, les types de demandes du département de la criminalité économique se découpent ainsi : 39,1% sont des demandes d'analyse, 20,3% d'assistance à la perquisition, 8,4% d'extraction de données et 32,2% d'assistance technique.

Les autres principaux clients de l'Unité sont les départements de la criminalité organisée (24,0%), de la sécurité étatique (22,7%) ainsi que les autres services de police (11,3%). En 2009, le département de la criminalité organisée a vu ses demandes chuter de 55% et cette baisse se confirme en 2010. Les demandes du département de la sécurité étatique restent relativement stables avec 35 demandes en moyenne par années. L'année 2007 fait exception avec 52 demandes adressées à l'Unité.

Les demandes effectuées par le service de renseignements criminels, le service de support aux opérations et le service de protection sont plutôt rares. Au cours de la période d'analyse de sept années, ces trois services n'ont adressé qu'une trentaine de demandes; ceci équivaut à 2,7% de toutes les demandes reçues durant cette période. Ceci est explicable par le fait que ces départements sont eux aussi des unités de support aux enquêtes; les rares demandes effectuées concernent principalement de l'assistance technique.

#### *1.4.1. Éléments soulevés par les membres de l'Unité*

La question « Qui nécessite le plus souvent votre expertise et pour quelle raison ? » a été posée aux membres de l'Unité. A2, analyste senior de l'Unité, a répondu que la plupart des requêtes provenaient des autres sections de l'organisation. En termes d'importance, au niveau du nombre de requêtes, viennent ensuite les demandes en provenance des autres corps policiers.

À la question sous-jacente : « Comment les différents demandeurs se distinguent-ils ? », A2 souligne plusieurs éléments très intéressants. D'abord, les demandeurs se distinguent par la qualité de leurs demandes. Certaines demandes sont bien justifiées et appuyées, alors que d'autres le sont moins. La qualité de la demande est importante puisque maintenant on ne peut plus faire l'analyse d'appareil technologique sans mandat vu les développements jurisprudentiels et législatifs. Il est important de bien démontrer qu'il ne s'agit pas d'une partie de pêche.

Un système a été mis en place pour aller offrir des formations aux sections effectuant des demandes afin de les aider et de les familiariser avec ce qu'on doit inclure dans celles-ci. Des formations régulières sont nécessaires afin de s'assurer que les gens soient à jour.

A2 termine en disant que dorénavant il y a plus d'information requises sur le formulaire et qu'on est plus rigoureux, exigeant que toutes les informations soient fournies. Il y a donc un filtrage important qui s'opère.

#### *1.4.2. Synthèse*

Pour l'Unité, les différents demandeurs se distinguent principalement par la qualité de leur demande. Également, la qualité des demandes n'est pas totalement indépendante de la quantité, puisque qu'avec le temps un partenariat se bâtit entre les deux sections et le processus de demande s'en voit grandement facilité. L'établissement d'un bon canal de communication entre une section cliente et l'Unité signifie donc des demandes plus claires, moins de requêtes refusées et un meilleur roulement.

Les principaux demandeurs de l'Unité sont la section de la sécurité étatique et le département de la criminalité économique. Quant à eux, les autres services de police effectuent des demandes lorsqu'ils sont dans l'impossibilité d'effectuer eux même une analyse.

### **1.5. Analyses des demandes selon le type d'incident concerné**

Cette sous-section présente deux tableaux concernant le type d'infraction enquêté par le requérant lors du dépôt de la demande de service. L'objectif de ces analyses descriptives est de

déterminer quels types de crime enquêtés nécessitent, d'une façon ou d'une autre, l'expertise de l'Unité et d'examiner les tendances qui s'en dégagent.

Tableau 4

*Nombre de demandes de service par années par types d'incident*

Type de crime	2004	2005	2006	2007	2008	2009	2010	Total
Fraude	23	27	23	29	33	66	29	<b>230</b>
Stupéfiants	33	25	44	27	41	27	30	<b>227</b>
Criminalité organisée	21	15	26	36	24	15	5	<b>142</b>
Sécurité étatique	11	17	21	25	11	5	16	<b>106</b>
Droit d'auteur	3	8	12	9	22	15	22	<b>91</b>
Assistance technique	9	10	12	18	8	9	10	<b>76</b>
Homicide, harcèlement, menaces	9	6	2	11	7	5	7	<b>47</b>
Télécommunication	9	7	4	10	7	3	0	<b>40</b>
Pornographie juvénile	1	10	3	3	3	8	1	<b>29</b>
Piratage et crimes informatiques	0	4	0	1	0	0	1	<b>6</b>
Autres	1	3	6	5	5	9	11	<b>40</b>
Données manquantes	5	9	5	6	8	22	3	<b>58</b>
<b>Total</b>	<b>125</b>	<b>141</b>	<b>158</b>	<b>180</b>	<b>169</b>	<b>184</b>	<b>135</b>	<b>1092</b>

Considérant l'entièreté de la période d'analyse, le Tableau 4 indique que les dossiers d'enquête où l'infraction principale concerne de la fraude (21,8%) ou est en lien avec des stupéfiants (20,8%) constituent un peu moins de la moitié (42,6%) des demandes de service communiquées à l'Unité. En moyenne ces deux types d'infractions génèrent une trentaine de demandes par années.

En troisième position, les dossiers concernant de la criminalité organisée représentent 13% des demandes traitées. Finalement, les dossiers concernant les droits d'auteur (8,3%), la sécurité étatique (9,7%) ainsi qu'une assistance technique (7,0%) constituent l'essentiel du reste des demandes (25%). Les dossiers concernant un homicide, du harcèlement ou des menaces (4,3%), la loi sur la télécommunication (3,7%), de la pornographie juvénile (2,7%) et du piratage informatique (0,5%) ne constituent qu'une petite partie du travail de l'Unité (11,2% en tout).

En examinant la Figure 9 il est difficile d'établir des tendances claires pour tous les types de crimes, mais certaines données se distinguent du reste.

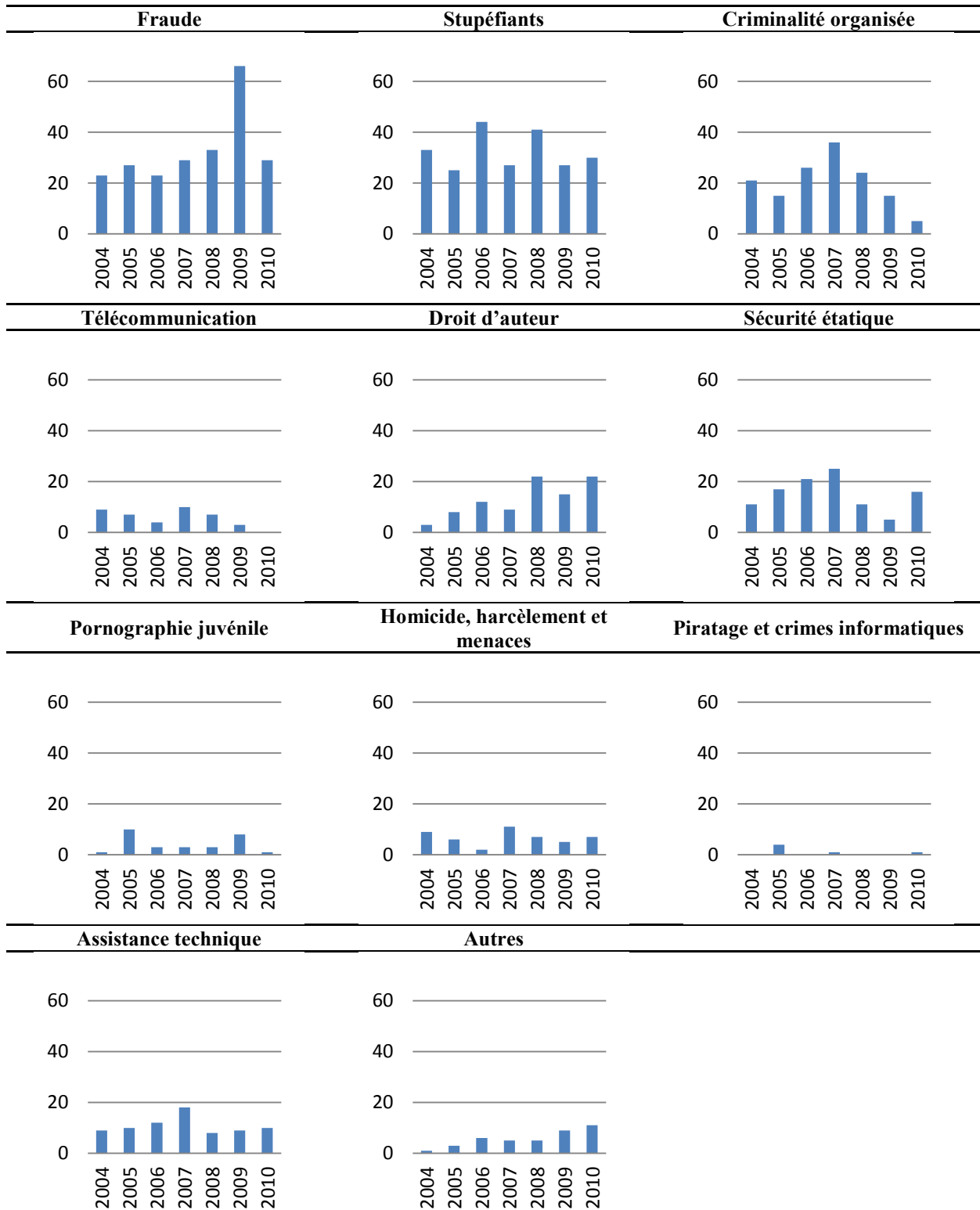


Figure 9. Histogrammes représentant le nombre de demandes adressées par années selon le type de crime.

Depuis 2004, en moyenne 32 dossiers concernant de la fraude sont traités par années. Par contre, l'année 2009 se démarque et affiche un nombre de requêtes deux fois supérieur à la moyenne. En ce qui concerne les stupéfiants, le même phénomène se produit. La tendance est relativement stable hormis les années 2006 et 2008 qui se démarquent par un nombre de dossiers traités excédant la moyenne observée. Ces variations importantes pourraient être dues à des opérations complexes de grande envergure ou encore à de multiples frappes visées contre une forme particulière de criminalité. Ces hypothèses devront être vérifiées auprès des membres de l'Unité.

Concernant les autres formes de criminalité, les demandes visant de la criminalité organisée semblent décroître depuis 2007, suite à une période de croissance marquée de 2005 à 2007. Les dossiers concernant les droits d'auteur semblent croître de façon générale depuis 2004. Les dossiers concernant la sécurité étatique ont connu une hausse de 2004 à 2007. Par contre, les années 2008 à 2010 et particulièrement 2009 sont en bas de cette tendance. Les autres histogrammes ne présentent que des informations anecdotiques et le petit nombre de demandes rend l'interprétation difficile. À ce stade, nous préférons nous fier aux membres de l'Unité pour comprendre les tendances concernant les types d'infractions traités par leur équipe.

#### *1.5.1. Éléments soulevés par les membres de l'Unité*

Nous nous sommes donc informés auprès des membres de l'Unité afin de savoir quels types de dossier d'enquête constituent la majorité de leurs demandes. A2 a indiqué qu'il s'agit de dossiers allant de la sécurité de l'état aux crimes économiques et commerciaux, en passant par les crimes relatifs aux droits d'auteurs.

P2 précise que depuis quelques années, on a énormément de demandes relatives à la sécurité de l'état, c'est la priorité de l'Unité. De plus, il ajoute qu'il y a beaucoup de dossiers de fraude, souvent des fraudes reliées de prêt ou de loin à du financement terroriste.

A1 mentionne que la tendance c'est de plus en plus aux fraudes par télémarketing. De plus, il ajoute qu'il y a des dossiers concernant le crime organisé et les stupéfiants, cependant les dossiers relatifs aux stupéfiants sont de plus en plus rares. La raison de leur rareté croissante est que ces demandes sont principalement pour des fins de renseignement. Puisque ce genre de

demandes est classé très bas dans les priorités, elles sont souvent refusées, et ce de plus en plus fréquemment.

L'hypothèse de l'accroissement soudain des demandes de services dues à des opérations et des projets spéciaux, notamment en ce qui concerne les dossiers reliés à de la fraude, à des stupéfiants ou à de la criminalité organisée, a été vérifiée auprès des membres de l'Unité.

À la question « Quelle est la charge de travail générée par les opérations ou projets spéciaux ? », A2 nous répond très clairement que c'est vraiment l'essentiel de leur travail, ce sur quoi on se concentre.

Quant à lui, P2 mentionne : « Moi je dirais que les opérations et les projets spéciaux c'est eux qui nous accaparent le plus. Je dirais facilement entre 50 et 75 pour cent du travail qu'on a à faire. ». De plus, il précise que souvent ces opérations sont classées « catégorie 1 », ce qui les priorise au-dessus du reste.

Selon A2, l'Unité mène aussi de plus en plus souvent des enquêtes de nature purement informatique. P2 mentionne à ce sujet qu'en huit ans, c'est vraiment la première année où on fait autant d'enquêtes informatiques. De plus, A2 et P2 ajoutent l'Unité a eu plusieurs succès récents dans ce domaine et qu'il y a comme projet de former une équipe complètement dédiée aux enquêtes informatiques.

### *1.5.2. Synthèse*

Selon les analyses effectuées et les informations colligées auprès des membres de l'Unité il appert que la majorité des dossiers acheminés à leur équipe pour expertise concernent de la fraude, des stupéfiants, la criminalité organisée ou la sécurité de l'état. Depuis quelques années, il semble également avoir une recrudescence de la fraude par télémarketing. De plus, la majorité de ces demandes découlent d'une façon ou d'une autre de projets ou d'opérations spéciales, suivant les priorités organisationnelles. Finalement, l'Unité mène de plus en plus d'enquêtes de nature informatique et cette tendance semble s'ancrer puisque l'organisation



projet de former une équipe d'enquête spécialisée et dédiée uniquement à cette forme de criminalité.

Finalement, il est bon de mentionner que les demandes adressées à l'Unité le sont en fonction des priorités de l'organisation. Elles ne reflètent donc pas nécessairement les tendances réelles de la criminalité informatique et technologique.

### 1.6. Analyse du profil du matériel analysé par l'Unité

Cette dernière sous-section s'intéresse aux types de périphériques analysés par l'Unité. L'objectif de ces analyses descriptives est de déterminer sous quelle forme la preuve numérique se présente. Le Tableau 5 ainsi que les Figures 10 et 11 font état de l'ensemble des périphériques, toutes demandes confondues, expertisés par l'Unité au cours de la période d'analyse.

Tableau 5

*Nombre et nature des périphériques traités par années*

Type de périphérique	2004	2005	2006	2007	2008	2009	2010	Total
Téléphone cellulaire	53	47	29	67	54	156	39	<b>445</b>
Ordinateur	17	15	21	36	81	46	42	<b>258</b>
CD	6	4	3	3	97	37	21	<b>171</b>
DVD	0	2	0	7	0	0	161	<b>170</b>
Téléphone cellulaire intelligent	1	4	16	19	21	57	47	<b>165</b>
Disquette	14	41	5	36	49	0	6	<b>151</b>
Stockage amovible (USB, etc.)	3	1	18	1	8	27	52	<b>110</b>
Ordinateur portable	4	10	8	9	18	23	33	<b>105</b>
Disque dur	12	1	18	15	6	10	27	<b>89</b>
Agenda électronique	4	4	3	5	6	0	0	<b>22</b>
Téléavertisseur	3	0	0	0	0	0	2	<b>5</b>
« Écrèmeuse »*	2	1	1	0	0	0	0	<b>4</b>
Console de jeu	0	2	0	0	0	0	0	<b>2</b>
<b>Total</b>	<b>119</b>	<b>132</b>	<b>122</b>	<b>198</b>	<b>340</b>	<b>356</b>	<b>430</b>	<b>1697</b>

\*De l'anglais « Skimmer » : Appareil permettant de lire les cartes magnétiques (cartes de crédit / débit) afin d'en faire des reproductions frauduleuses.

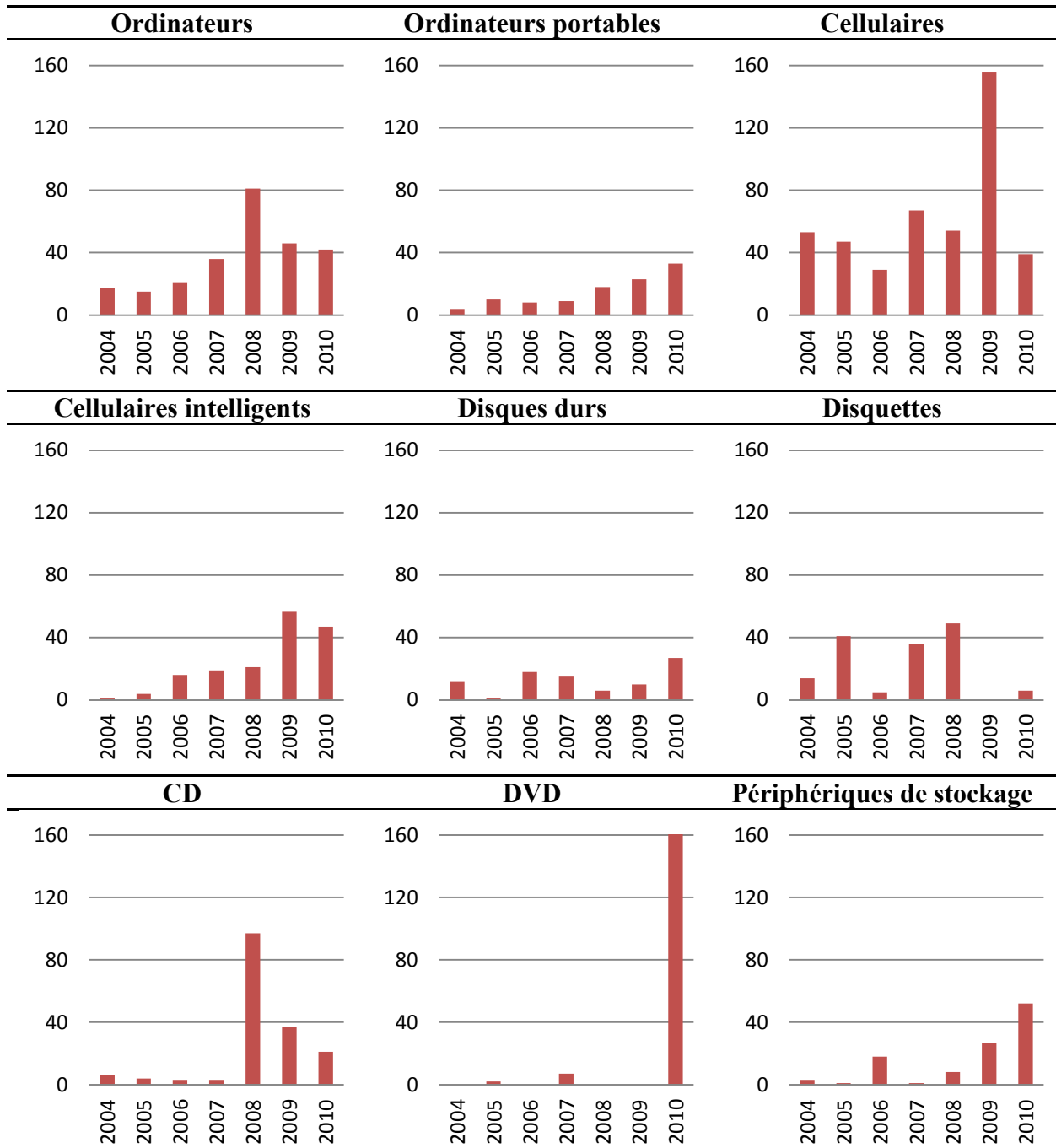


Figure 10. Histogrammes représentant le nombre et la nature des périphériques traités par l'Unité par années.

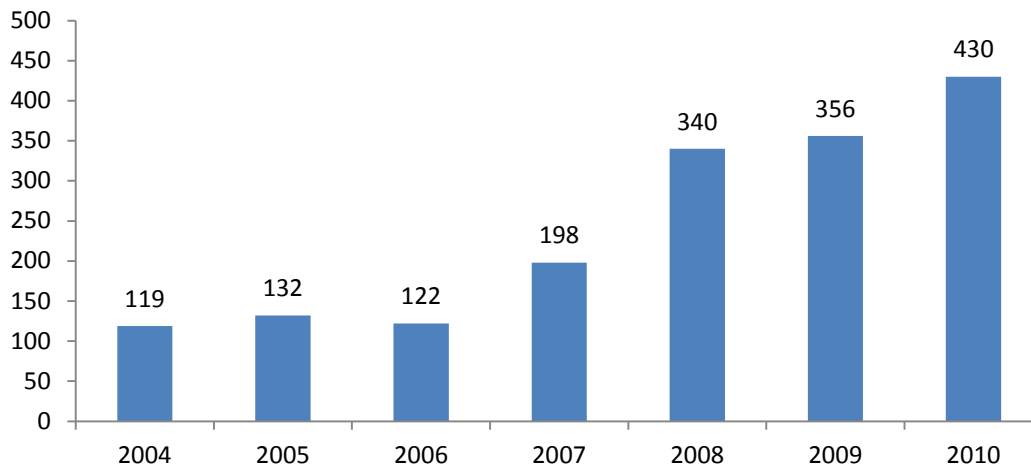


Figure 11. Représentation graphique du nombre de périphériques traités par années par l'Unité.

Le type de périphérique le plus souvent analysé est le téléphone cellulaire et il constitue 26,2% de tous les appareils expertisés par l'Unité entre 2004 et 2010. Si on ajoute les téléphones intelligents à ce compte, les appareils mobiles représentent plus du tiers (36,0%) de tous les périphériques traités par l'Unité. Les ordinateurs et les ordinateurs portables représentent respectivement 15,2% et 6,2% des analyses, pour un total de 21,4%.

Tous les périphériques de stockage confondus représentent 40,7% du matériel expertisé par l'Unité. Ils sont décomposables ainsi : CD (10,1%), DVD (10,0%), disquettes (8,9%), périphériques USB (6,5%) et disques durs (5,2%)<sup>31</sup>. La Figure 11 fait état d'un autre fait intéressant, contrairement aux demandes de service qui diminuent à compter de 2010 (voir Figure 4), le total des pièces analysées par l'Unité croît continuellement. Ce résultat concorde d'ailleurs avec la littérature citée précédemment (McMillan & al., 2013; Quick & Choo, 2014; Turnbull & al., 2009). Cette donnée pourrait donc s'avérer un meilleur indicateur de la charge totale de travail, plutôt que le nombre de demandes de service; d'autant plus que la complexité des demandes est extrêmement variable.

---

<sup>31</sup> La variable concernant le nombre de disques durs ne considère pas les disques durs contenus dans un ordinateur portable ou un ordinateur de bureau.

L'analyse de la Figure 10 révèle plusieurs éléments forts intéressants. Premièrement, il est possible de constater l'émergence de certaines tendances avec l'invention et la diffusion de nouvelles technologies. Cet élément est important car il permet de valider l'utilisation criminelle de certaines formes de technologies. Ceci est particulièrement apparent dans le cas des ordinateurs portables, des téléphones intelligents et des périphériques de stockage (clef USB et cartes SD par exemple) où il y a une augmentation progressive de leur popularité tout au long de la période d'analyse.

Similairement, la disparition progressive de technologies d'ancienne génération est également remarquable. En effet, entre 2008 et 2010 il y a une diminution marquée du nombre de CD analysés et la quasi-disparition des disquettes traitées par l'Unité. Ce phénomène est accompagné d'une hausse des périphériques substituant ces technologies désuètes, c'est-à-dire les périphériques de stockage USB et les DVD.

Finalement, la Figure 10 permet de constater qu'un nombre important de cellulaires a été traité en 2009 mais que ce nombre chute brusquement en 2010. Fait intéressant, cette baisse coïncide avec le programme de triage mentionné précédemment qui concernait spécifiquement ce type d'appareil.

#### *1.6.1. Éléments soulevés par les membres de l'Unité*

Les membres de l'Unité rencontrés mentionnent de nombreux éléments concernant la nature des périphériques et la complexité des analyses. Tout d'abord, A2 confirme la validité de nos analyses en mentionnant que règle générale la plupart des dossiers reçus présentement sont des dossiers d'analyse de cellulaires et de téléphones intelligents. De plus, il ajoute qu'au fil des années la tendance s'est modifiée passant de principalement des ordinateurs et des serveurs à surtout des appareils mobiles.

Finalement, il ajoute que maintenant on retrouve des cellulaires associés à n'importe quels types de crimes. Depuis les douze dernières années, les demandes d'analyses de cellulaires ont de loin surpassé les autres types d'analyses.

Par contre, la complexité et le temps d'analyse sont très variables d'un périphérique à l'autre et dépendent également de la nature de la preuve recherchée. Pour P1, c'est les copies miroirs qui requièrent la plus grande partie de son temps. En effet, l'augmentation rapide de la capacité des disques durs signifie aussi l'augmentation du temps requis pour mener à bien cette opération; considérant également que le matériel d'analyse n'évolue pas à la même vitesse.

À cet effet, P2 traite de l'impact de l'évolution technologique. Lors de son arrivée au à l'Unité, on traitait des disques durs de 500 gigaoctets. Aujourd'hui, on traite des disques durs de deux à quatre téraoctets. Si auparavant, cela prenait cinq heures pour faire l'acquisition<sup>32</sup> d'un disque dur, maintenant ça peut prendre jusqu'à dix ou quinze heures.

Concernant l'augmentation de la quantité de périphériques à analyser, A1 croit qu'en fait c'est la capacité des périphériques qui augmente et non la quantité. Due à l'évolution des technologies, la capacité des disques durs augmente mais les gens ont moins de périphériques. La quantité a diminué, à cause de la capacité et du type de technologie. Maintenant un appareil fait tout. Cette affirmation est également entérinée par P2 qui a mentionné la même chose lors de son entrevue.

### *1.6.2. Synthèse*

Les appareils mobiles semblent occuper une part de plus en plus importante des analyses effectuées à l'Unité. L'augmentation de la capacité de stockage de ces périphériques les rend très versatile mais cela fait aussi en sorte qu'ils contiennent beaucoup plus de données. Selon la perception des intervenants rencontrés, la quantité de périphériques n'est pas vraiment en hausse ou du moins elle s'est stabilisée. Par contre, la quantité de données à traiter augmente continuellement. Cela a aussi comme conséquence d'augmenter la longueur des analyses : imager un disque dur peut prendre de deux à trois fois plus de temps.

---

<sup>32</sup> Faire l'acquisition ou imager un disque dur signifie effectuer une copie miroir du disque dur afin de préserver l'intégrité de la pièce à conviction. Les analyses sont donc effectuées sur la copie de sauvegarde plutôt que sur la pièce originale.

Les données recueillies indiquent que les délinquants semblent avoir un profil d'adoption des nouvelles technologies similaire au reste de la population; du moins, concernant les formes de criminalités enquêtées par l'organisation policière. En effet, plusieurs périphériques tels que les CD et les disquettes sont de moins en moins présents, tandis que certains périphériques gagnent en popularité tels que les ordinateurs portables, les cellulaires intelligentes et les périphériques de stockage USB.

## **2. Synthèse du chapitre et constatations préliminaires**

Le présent chapitre constitue un premier effort visant à caractériser le travail d'une unité spécialisée en criminalité technologique et en analyse judiciaire informatique. Les tableaux et figures présentés ont touché plusieurs grandes thématiques soit : le nombre de demandes reçues, les types de services offerts, le profil des clients, les formes de criminalité concernées par les dossiers d'enquêtes et la nature des périphériques traités.

Le principal rôle de l'Unité en est un d'assistance et de support technique. Conséquemment, ils ne contrôlent peu ou pas les demandes acheminées à leur service. Ces demandes concernent majoritairement des projets et des opérations d'envergure. Avec le temps et la croissance du nombre de demandes, il a été nécessaire d'instaurer des processus administratifs afin d'exercer une forme de contrôle sur les requêtes entrantes. Ainsi, des programmes de formation et un système de triage ont été mis au point afin de prioriser les demandes les plus urgentes et d'atténuer la pression générée par l'augmentation de l'arriéré. De plus, des outils sont mis à la disposition des enquêteurs afin qu'ils effectuent eux-mêmes l'analyse des données saisies.

Désormais, toutes formes de criminalité est susceptible de comprendre une composante technologique puisque virtuellement tout le monde possède un cellulaire. Ces appareils mobiles constituent d'ailleurs le type de périphérique le plus souvent traité et leur analyse s'avère l'activité qui occupe le plus grand volume de travail.

Les principaux clients de l'Unité sont les départements de la criminalité économique, de la criminalité organisée et de la sécurité étatique. Conséquemment les dossiers les plus souvent soumis pour fin d'expertise sont reliés à de la fraude, à des stupéfiants, au gangstérisme ou à

du terrorisme. Par contre, depuis les dernières années, il y a augmentation des enquêtes informatiques menées directement par l'Unité et cette tendance semble se maintenir.

À ce stade, il est clair que la gestion d'une unité spécialisée en analyse judiciaire comporte de nombreux défis et nécessite des ajustements constants. Le prochain chapitre vise à décortiquer plusieurs de ces enjeux afin de comprendre quels sont les éléments clefs assurant la bonne implantation et le succès d'une telle unité.

---

## **Chapitre V**

### **Les défis et les enjeux d'une unité policière spécialisée en analyse judiciaire informatique**

---



Les défis pour une unité spécialisée en criminalité informatique sont nombreux. Lorsqu'une organisation choisit de se doter d'une telle innovation, elle doit investir massivement en équipement et en formation pour mener à bien ce projet. Dans le présent chapitre, nous allons aborder certains défis et enjeux propres à une telle unité.

Le premier thème abordé sera celui des délais de traitement. En effet, un des défis majeurs d'une unité spécialisée en analyse judiciaire informatique est de maintenir un arriéré « acceptable » car ce dernier constitue un risque important pour plusieurs raisons. Entre autres, l'accumulation de retards est susceptible de nuire au dépôt d'accusations criminelles ou de créer des délais judiciaires importants. Ultimement, cela peut mener à la perte d'un dossier en Cour en raison de la longueur des procédures. La gestion adéquate de cet arriéré constitue donc un enjeu crucial; une section sera entièrement consacrée à cet aspect majeur.

Le deuxième thème traitera des facteurs exogènes exerçant une pression sur une unité spécialisée en analyse judiciaire informatique. Deux enjeux principaux seront abordés, soit l'évolution rapide des technologies et la jurisprudence. À tout moment, l'un ou l'autre de ces facteurs peut forcer la modifier des pratiques et des méthodes en place. Il est donc essentiel pour ces unités d'être à l'affût de tous changements juridiques et technologiques pouvant influencer leur travail.

Le troisième thème examinera les facteurs endogènes à l'organisation affectant la prestation de service d'une telle unité. Cinq (5) principaux enjeux et défis seront abordés : la diffusion de l'expertise, l'effet « CSI », la formation du personnel, la gestion de ressources limitées ainsi que les priorités et impératifs organisationnels.

Dernièrement, la section synthèse de ce chapitre fera un retour sur les thèmes abordés, soulignera les facteurs clefs et mettra en place les éléments essentiels aux analyses et réflexions du chapitre suivant.

## **1. Le délai de traitement des dossiers**

La présente section tente de comprendre les facteurs influençant les délais de traitement pour une unité spécialisée en criminalité technologique et en analyse judiciaire informatique. Dans un premier temps, les facteurs soulevés par les membres de l'Unité seront partagés. Dans un second temps, puisqu'il a été impossible d'obtenir des informations quantitatives sur le délai de traitement, aucune analyse n'a été faite spécifiquement sur ce sujet. Par contre, des analyses concernant le délai entre l'incident et la demande de service seront présentées. Ces analyses permettent d'estimer le temps entre l'ouverture du dossier de police et le moment où une demande est adressée. Ces analyses permettent également d'alimenter une seconde série de discussions avec les membres l'Unité et ils expliquent la pertinence de cette information. Finalement, une synthèse des principaux facteurs influençant les délais de traitement sera présentée.

### **1.1. Facteurs influençant le délai soulevés par les membres de l'Unité**

La question suivante a été posée aux membres de l'Unité : « Selon vous, quels sont les principaux facteurs influençant les délais de traitement d'une demande de service adressée à votre unité ? »

A2 répond spontanément : « Initialement, la qualité de la demande. ». Il précise qu'il est essentiel que le demandeur réponde à toutes les questions du formulaire qui permettent d'établir la valeur probante de la demande. Cela permet d'évaluer rapidement si l'analyse demandée est un élément clef du dossier. C'est-à-dire si cet élément de preuve est essentiel à la continuité du dossier ou au dépôt d'accusations criminelles.

De plus, A2 ajoute qu'avant même qu'une demande soit acceptée ou refusée il y a beaucoup de va-et-vient entre les partenaires afin de colliger les informations nécessaires à l'évaluation de la demande. Cela peut prendre du temps; souvent une question de semaines. Pour cette raison, si initialement la demande est bien écrite et contient les bonnes informations, beaucoup de temps est économisé. Dans un deuxième temps, si la demande est retenue, l'importance relative de la preuve s'avère un élément déterminant à la priorisation de la demande et donc au délai.

A2 aborde ensuite une série de facteurs affectant le délai de traitement. Le premier facteur spécifié concerne la priorisation des demandes. En effet, les enquêtes relatives à la sécurité de l'état ou relative à la vie humaine par exemple seront priorisées. Ce processus de triage fait en sorte que certaines demandes seront traitées moins rapidement mais dans un délai raisonnable, alors que d'autres demandes pourront être traitées immédiatement.

Le deuxième facteur mentionné concerne les exigences technologiques. Il est parfois nécessaire de faire de la recherche et du développement pour être en mesure d'analyser tous les types de périphériques mis sur le marché. Pour ce faire, l'Unité est en contact constant avec leur direction ainsi que d'autres partenaires du « *Big Five* »<sup>33</sup>.

Le troisième facteur souligné est l'arriéré des demandes, c'est-à-dire le nombre de dossiers entrant versus la capacité de traitement des demandes.

Un quatrième facteur est abordé par A2 et concerne les délais de Cour. Lors de la réception d'une demande, on doit regarder à quelle étape de judiciarisation en est le dossier. Ainsi, si un dossier doit être présenté à la Cour dans la semaine suivante, il faut procéder rapidement à l'analyse et fournir les rapports requis. Générer des rapports qui sont compréhensibles par un non-initié en informatique demande beaucoup de temps. Il est nécessaire de vulgariser des informations qu'une majorité de gens ne comprendrait pas autrement. D'autre part, cela signifie aussi que les demandes ne nécessitant pas de rapports peuvent être effectuées plus rapidement.

Suite aux éléments apportés par A2, A1 ajoute que d'autres facteurs peuvent aussi influencer le délai de traitement, tels que les effectifs en place, l'évolution rapide des technologies, la précision de la demande et la quantité de périphériques à analyser. De plus, lors de grosses

---

<sup>33</sup> Le *Big Five* est une collaboration entre la Nouvelle-Zélande, les États-Unis, l'Australie, le Royaume-Uni et le Canada visant à échanger des renseignements criminels, stratégiques et de sécurité.

opérations, il est possible qu'il y ait des demandes subséquentes à la demande initiale, ce qui augmente aussi la charge de travail.

A2 ajoute qu'il y a d'autres facteurs qui peuvent entrer en ligne de compte tel que la formation nécessaire des enquêteurs et le roulement de personnel. Cela prend beaucoup de temps pour former un nouvel employé et il doit acquérir beaucoup d'expérience afin d'être capable d'utiliser tout le matériel et de faire le travail sans ou avec peu de supervision.

A2 ajoute un autre élément soit la conviction qu'ont certains demandeurs que des appareils contiennent des éléments de preuves alors qu'il n'en est rien. Cette conviction peut mener les enquêteurs à chercher pendant de longs moments des éléments de preuve qui ne se trouve pas sur les appareils analysés.

A1 termine en ajoutant un dernier facteur : la collaboration du client lui-même. Parfois, pour effectuer une analyse on aura besoin d'informations supplémentaires. Si le client prend du temps pour fournir les informations requises, la demande sera retardée. D'autre part, une fois le rapport terminé, il arrive parfois que le client ne vienne pas le chercher promptement. Cela fait en sorte que le dossier ne peut pas être fermé.

Cela signifie qu'à l'interne, avant qu'un dossier soit officiellement clos pour l'Unité il faut qu'il soit remis en bonne et due forme au demandeur. Or, il s'avère que dans certains cas des rapports d'analyse complétés peuvent rester longtemps sur les tablettes en attente d'être récupérés par le client.

## **1.2. Analyse du délai entre la réception d'une demande et l'ouverture du dossier d'enquête**

La Figure 12 présente le résultat du calcul de la différence entre la date de réception de la demande de service et la date de l'incident<sup>34</sup>. Ce calcul permet d'estimer le nombre de jours

---

<sup>34</sup> Date coïncidant à l'ouverture du dossier de police ou l'événement initiateur.

moyens s'écoulant entre l'ouverture d'un dossier policier et l'envoi d'une demande à l'Unité. Cette information complète le délai de traitement et peut être intéressante dans une perspective de gestion de l'afflux des demandes de service. De plus, l'analyse de cette variable permet d'offrir une meilleure compréhension des facteurs retardant l'envoi de certaines demandes de service.

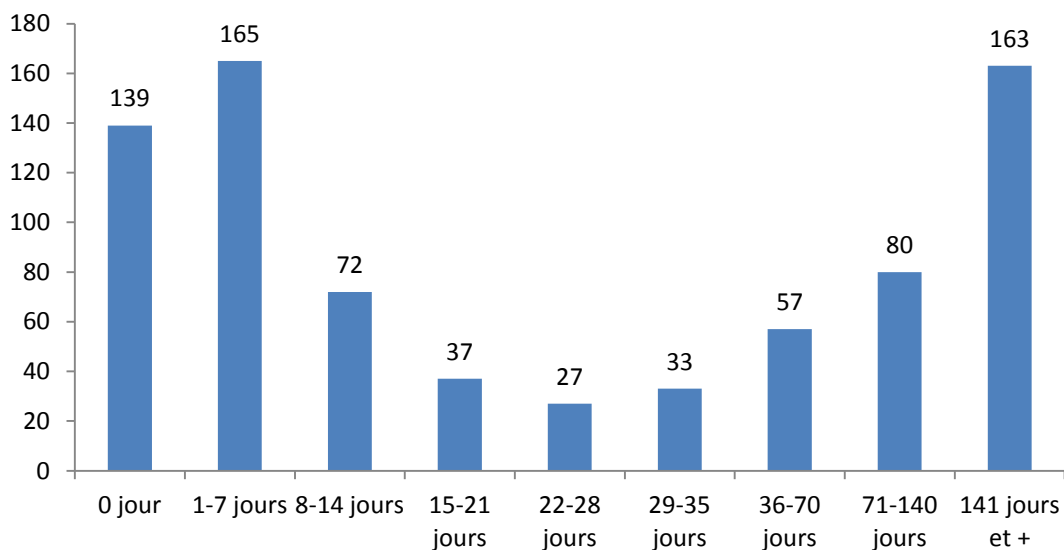


Figure 12. Représentation graphique du nombre de jours écoulés entre la date de l'incident et la réception d'une demande de service.

En examinant la Figure 12, il est possible de constater que la distribution présente une très forte asymétrie positive. Cela signifie qu'un nombre important de demandes de service sont effectuées la journée même de l'incident (18,0%). La majorité (53,4%) des demandes sont effectuées dans les trois semaines suivant l'ouverture du dossier. Toutefois, environ 20% des demandes sont effectuées plus de quatre mois après l'ouverture du dossier. En l'espèce, compte tenu de la forte asymétrie observée, la meilleure mesure de tendance centrale est la médiane. Conséquemment, en général il faudra 17 jours, après l'ouverture du dossier, pour qu'une demande soit acheminée à l'Unité.

En ce qui concerne les demandes effectuées le jour même, elles sont à 62,2% des demandes d'assistance à la perquisition et d'assistance technique. Il est logique que la date de l'incident coïncide avec la date de la demande puisque cette dernière est acheminée aussitôt que le

besoin se manifeste. De plus, 8,6% de ces demandes proviennent d'un autre service de police. Dans ce cas, la journée de la demande coïncide également avec la date de l'incident car un dossier propre à l'organisation est créé en réponse à la demande. En ce qui concerne les 30% restant<sup>35</sup>, il a été impossible de déterminer une tendance claire mais certaines requêtes (3,6%) correspondent à des demandes urgentes relative à la sécurité de l'état ou à d'autres opérations de nature informatiques (par exemple : extraire un vidéo de l'Internet ou récupérer des fichiers effacés).

### 1.2.1. Facteurs influençant le délai entre l'incident et la demande de service

Afin de vérifier les facteurs pouvant influencer le délai entre l'incident et la demande, une association statistique a été effectuée entre le délai et six (6) autres variables clefs de notre base de données.

Tableau 6

#### Tests bivariés non paramétriques entre le délai et six variables catégorielles

Variables	Groupes	Médiane (jours)
Type de service effectué	Analyse	21
	Aide à la perquisition	18,5
	Extraction de données	15
	Assistance technique	8
Est-ce que les pièces ont été obtenues à l'aide d'un mandat ? ***	Non	10
	Oui	25
Est-ce que des accusations sont déposées au moment de la demande ?	Non	20
	Oui	16
La demande spécifiait-elle du matériel à analyser ?	Non	14
	Oui	17,5
Type de crime visé par la demande ***	Fraude	38,5
	Stupéfiants	13,5
	Criminalité organisée	8
	Droit d'auteur	45
	Sécurité de l'état	8
	Homicide, harcèlement et menaces	22
Département effectuant la demande ***	Autres infractions	22
	Criminalité organisée	9
	Criminalité économique	28
	Sécurité étatique	12,5
	Autres services de soutien	0
	Autres services de police	41

\*\*\* p≤0,001 \*\* p≤0,01 \*p≤0,05

†Lorsque le nombre de groupes est 2 le « U de Mann Whitney » est utilisé. Lorsque le nombre de groupes est supérieur à deux, le test de Kruskal Wallis est utilisé.

<sup>35</sup> Corresponds aux demandes d'analyse et d'extraction de données des sections internes.

Le Tableau 6 montre que trois (3) des six (6) variables présentent des différences significatives entre leurs catégories respectives. En d'autres termes, pour une variable catégorielle donnée, si le cas sélectionné appartient à une catégorie plutôt qu'à une autre, ceci va influencer significativement le délai entre l'incident et la demande de service.

Afin d'interpréter ces différences, puisqu'il s'agit d'un test non paramétrique, les médianes respectives de ces groupes sont comparées. Les demandes comprenant des pièces à conviction obtenues à l'aide d'un mandat de perquisition prennent généralement plus de temps (environ 2 semaines de plus) avant d'être acheminées à l'Unité. Il est possible d'expliquer ce résultat par la quantité de travail qui a été effectué préalablement à la demande. Nécessairement une portion de l'enquête a été réalisée et cette dernière a mené à la saisie des dites pièces à conviction. Inversement, les pièces obtenues sans autorisation judiciaire ou dans d'autres circonstances peuvent être acheminées plus rapidement. Compte tenu de l'absence de mandat, ces demandes concernent probablement la collecte de renseignements plutôt que le dépôt d'accusations criminelles.

Concernant les deux autres variables significatives, il serait nécessaire de comparer deux par deux leurs catégories respectives afin de déterminer quels groupes se distinguent significativement des autres. Toutefois, cette opération est fastidieuse dû au grand nombre de permutations à effectuer; qui plus est, l'interprétation des résultats ainsi obtenus s'avère difficile et hasardeuse. Conséquemment, il est préférable dans un premier temps de présenter ces analyses aux membres de l'Unité afin de confirmer leur validité et de déterminer les limites de leur interprétation. Par la suite, les résultats du Tableau 6 seront interprétés à la lumière des informations recueillies.

### *1.2.2. Explication de la signification du délai par les membres de l'Unité*

L'analyste civil A2 explique, selon lui, la signification du délai entre la date de l'incident et la date de la demande s'explique par le court délai restant entre le moment de la réception de l'élément de preuve à analyser et la date ultime de rétention permise.

En effet, selon l'article 490 (2) du *Code criminel*, les biens saisis lors d'une perquisition peuvent être conservés un maximum de trois mois sans quoi une ordonnance de prolongation doit être faite. Puisque les pièces à conviction ne servant pas aux procédures en cours doivent être redonnées au propriétaire, il est souvent urgent d'accéder le contenu d'un appareil afin de déterminer si son contenu est pertinent à l'enquête.

A2 ajoute que parfois, en fin d'enquête, il est constaté que l'expertise d'un élément technologique est manquante ou s'avère maintenant nécessaire. Une demande doit donc être faite pour parer à ce manquement. Que ce soit par oubli ou pour une autre raison, ce type de demande tardive a pour effet de limiter le délai disponible pour le traitement de cet élément.

A1 intervient pour préciser que, puisque qu'on se concentre essentiellement sur des projets d'envergures, les enquêteurs vont demander des analyses vers la fin du projet afin de corroborer des éléments de preuve ou d'en ajouter.

En résumé, le délai entre la date de l'incident et la date de la demande peut donc signifier deux choses : premièrement, certaines pièces à conviction sont analysées vers la fin de l'enquête afin de corroborer certaines informations, enquêtes qui souvent s'échelonnent sur plusieurs années. Deuxièmement, certaines pièces à conviction, par oubli ou autre, demeurent non traitées et sont acheminées à l'Unité en urgence. Ce genre de demandes urgentes est susceptible de générer des ennuis et des inconvénients autant du côté de l'Unité que du demandeur.

### *1.2.3. Analyse des facteurs influençant le délai entre l'incident et la demande*

Afin de valider les résultats obtenus au Tableau 6, les demandes excédant un délai de six (6) mois (représentant environ 20% de l'ensemble des demandes adressées à l'Unité au cours de la période d'analyse) ont été examinées. L'objectif est de déterminer si certains types de crime ou certains demandeurs génèrent une plus grande proportion de ces demandes « tardives »<sup>36</sup>.

---

<sup>36</sup> Le barème de référence est 20%. Toute proportion excédant ce seuil signifie une plus grande quantité de demandes dites tardives.



En analysant les types de crimes, trois données se distinguent : 30,7% des demandes concernant une infraction de fraude excèdent le délai de six mois entre l'incident et la demande; similairement, 41,7% des demandes concernant la *Loi sur les télécommunications* excèdent ce délai. Inversement, seulement 5,3% des demandes concernant la sécurité de l'état dépassent le délai de six mois.

Au niveau des départements demandeurs, les données obtenues corroborent les résultats du Tableau 6 : 24,4% des demandes du département de la criminalité économique excèdent le délai de six (6) mois. Inversement, seulement 11,4% des demandes du département de la sécurité étatique dépasse les six mois. Fait intéressant : 27,6% des demandes des autres services de police dépassent le délai de six mois entre l'incident et la demande. Toutefois, il est possible d'expliquer ce résultat par les délais administratifs inhérents aux demandes entre services de police.

En présentant les résultats obtenus jusqu'à présent, A1 nous met en garde quant à l'interprétation de ces résultats. Il mentionne qu'ils reflètent probablement les priorités organisationnelles et que ces priorités ont changé au fil des années. Le filtrage des demandes de service peut également venir biaiser ces résultats.

Compte tenu de cet avertissement, il est difficile de tirer des conclusions claires des analyses effectuées dans cette section. Toutefois, il transparaît que les demandes concernant la sécurité de l'état, une grande priorité de l'organisation, soient acheminées avec une plus grande célérité à l'Unité. Les demandes moins prioritaires, concernant de la fraude par exemple, prennent généralement plus de temps avant d'être déposées. Ceci peut être aussi expliqué partiellement par la complexité inhérente à ces dossiers.

### **1.3. Synthèse des facteurs influençant le délai de traitement**

Les facteurs susceptibles d'influencer le délai de traitement sont nombreux. Selon les informations colligées et les analyses effectuées dans la présente section, ces facteurs peuvent être classés en quatre (5) grandes catégories :

- Les facteurs relatifs à la communication, comprenant :

- La qualité et la clarté de la demande
- La fréquence et la qualité des échanges entre les partenaires
- Les facteurs technologiques, comprenant :
  - La complexité de l'analyse à effectuer
  - La nature de la technologie expertisée
- Les facteurs relatifs aux impératifs organisationnels, comprenant :
  - Les priorités organisationnelles
  - Les projets spéciaux et les demandes urgentes
- Les facteurs propres à la demande, comprenant :
  - La valeur probante de la preuve
  - Les délais judiciaires
- Les facteurs internes à l'unité spécialisée :
  - Le niveau d'arriéré
  - Les tâches administratives connexes
  - Le nombre d'analystes formé
  - Le niveau de roulement du personnel

## **2. Les facteurs exogènes : l'évolution rapide du cadre technologie et juridique**

La gestion du délai de traitement constitue probablement l'un des plus grands défis d'une unité spécialisée en analyse judiciaire informatique. Toutefois les environnements technologique et juridique changeants amènent ponctuellement de nouveaux défis à relever. En effet, une nouvelle technologie signifie souvent une période d'adaptation et de familiarisation; similairement, une jurisprudence est susceptible d'imposer des changements dans les pratiques afin de se plier aux nouvelles exigences de la Cour.

### **2.1. L'évolution rapide des technologies**

La question suivante a été posée aux membres de l'Unité : « Selon vous, est-ce que l'évolution des technologies a un impact sur votre travail ? Si oui, de quelle manière ? ».

A2 explique que les individus sont de plus en plus conscients de la protection de la vie privée et prennent des mesures technologiques pour protéger leurs données. Les compagnies offrent

également de plus en plus de solutions de protection clé en main et faciles à comprendre pour l'utilisateur moyen. Les services de police doivent donc s'adapter à ces technologies et les contrer. Pour y arriver, il y a des besoins grandissants pour de la formation de pointe, pour l'établissement de partenariats avec d'autres services de police et pour de la recherche appliquée.

Également deux des membres de l'Unité soulignent que la simple mise à jour d'un système d'exploitation peut forcer à changer les techniques d'extraction de données. Qui plus est, ces mises à jour sont de plus en plus fréquentes, spécialement en ce qui concerne les téléphones cellulaires intelligents. Il est donc nécessaire que certains outils d'analyses soient actualisés à chaque nouvelle version du système d'exploitation afin de tenir compte des spécificités de l'itération.

Tous les intervenants de l'Unité sont unanimes : une conséquence de l'évolution rapide des technologies est l'augmentation de la quantité brute de données à analyser. Toutefois, ils soulignent aussi que les technologies utilisées pour faire l'extraction de données ne suivent pas la cadence.

A2 mentionne que l'utilisation que font les gens de la technologie change également. Oui, il y a plus d'informations de disponibles, sur les réseaux sociaux par exemple, mais il faut être en mesure d'aller les récupérer. A1 mentionne que l'évolution des technologies signifie aussi la modification des habitudes des délinquants :

*« Les pirates informatiques visent de plus en plus les téléphones intelligents au lieu des ordinateurs. Par exemple, toutes les données bancaires sont contenues à l'intérieur d'un téléphone intelligent. Aussi, plusieurs informations personnelles sont sur nos téléphones intelligents puisqu'ils peuvent se synchroniser avec nos ordinateurs, nos agendas, nos calendriers et ainsi de suite. »*

De plus, il ajoute qu'avec l'apparition du « *cloud computing*<sup>37</sup> », l'informatique en nuage, c'est la disparition de l'ordinateur personnel tel qu'on le connaît. Ceci constituera un défi majeur pour les organisations policières dans l'avenir.

Finalement, P2 mentionne que : « La technologie est en constante évolution, ce qu'on faisait il y a huit ans est vraiment différent de ce qu'on fait maintenant. ».

En résumé, la technologie est un facteur majeur pour les unités policières spécialisées en criminalité technologique. L'évolution rapide des technologies signifie une mise à niveau constante des méthodes d'analyse mais aussi des connaissances sur le sujet. De plus, l'utilisation criminelle de nouvelles technologies force l'élaboration de stratégies permettant d'enquêter sur ces crimes. Dernièrement, l'augmentation de la quantité de données contenues dans les appareils numériques s'avère un enjeu majeur pour l'avenir.

## **2.2. La jurisprudence**

Le système judiciaire canadien s'adapte progressivement aux réalités de l'ère numérique mais ce processus est lent et fastidieux. Néanmoins, de plus en plus de jugements viennent encadrer divers aspects de la preuve numérique. Ces jurisprudences affectent directement les pratiques policières relatives à la saisie de pièces à conviction numériques ainsi qu'aux analyses judiciaires informatiques. Les unités policières spécialisées dans l'analyse de ces preuves n'ont pas le choix de tenir compte de ces jurisprudences, qui sont d'ailleurs de plus en plus pointues.

À titre d'exemple, une jurisprudence récente de la Cour suprême du Canada, *R. c. Vu* (2013), requiert maintenant des forces de l'ordre qu'elles obtiennent une autorisation judiciaire couvrant spécifiquement le contenu des ordinateurs. Ils doivent ainsi démontrer qu'ils ont des motifs raisonnables de croire que ce qu'ils cherchent puisse se retrouver dans un ordinateur. À cet effet, aucune distinction n'est faite entre un ordinateur et un appareil mobile.

---

<sup>37</sup> En français : infonuagique.

L'ordinateur n'est donc plus considéré comme un « contenant » ordinaire pouvant être fouillé, au même titre qu'une simple boîte, lors d'une perquisition. Compte tenu de la grande quantité de données personnelles que contient un ordinateur, il y a une expectative de vie privée accrue. Cette jurisprudence considère donc plutôt l'ordinateur comme un lieu distinct : un ordinateur ou un téléphone cellulaire peut donc être comparé à un coffre verrouillé.

Ce genre de jurisprudence vient fréquemment réajuster le tir en matière technologique et a un impact important sur les intervenants du milieu. Les membres de l'Unité soulignent les récents changements dans le domaine juridique entourant les expertises informatiques judiciaires. À cet effet, P2 mentionne qu'on doit s'assurer de fournir des motifs valables pour pouvoir procéder à la recherche d'information. On doit rester à l'affût de l'évolution de la jurisprudence pour ne pas compromettre la preuve recueillie. De plus, il ajoute que cette jurisprudence est de plus en plus raffinée, contraignante et encadre avec plus de rigueur les analyses qu'ils effectuent.

P1 discute de l'évolution de la jurisprudence et des tendances pour l'avenir :

*« Les juges sont de plus en plus pointilleux, plus chirurgical au niveau de l'information [...] Par exemple, si tu recherches des messages textes, des SMS, ils vont te demander entre quelle date et quelle date. L'ère où on demandait tout le contenu de l'ordinateur, surtout avec la grosseur des disques durs [est terminée]. [...] J'ai vu des mandats rejetés par le juge justement parce que c'était trop vague, trop général. »*

En résumé, les récents changements imposés par la jurisprudence viennent baliser la preuve numérique; autant au niveau de sa saisie que de son analyse. Les enquêteurs devront être de plus en plus précis sur ce qui est recherché dans les ordinateurs et justifier pourquoi la preuve s'y trouverait.

### **3. Les facteurs endogènes : une expertise méconnue et des ressources limitées**

Outre les facteurs externes à l'organisation, certains facteurs internes constituent des défis tout aussi importants pour une unité spécialisée en analyse judiciaire informatique. Dans la présente section, cinq (5) défis et enjeux propres à l'Unité seront présentés.

Premièrement, la diffusion de l'expertise est une stratégie avantageuse permettant de faire face aux délais d'analyses grandissants. Toutefois cette tâche est complexe, ne donne pas toujours les résultats escomptés et constitue un défi en soi. Il est donc nécessaire d'encadrer ces pratiques afin de maximiser leurs retombées.

Deuxièmement, les utilisateurs du service d'analyse judiciaire informatique doivent être sensibilisés aux capacités et aux limites de ce dernier. Une mauvaise conception de la nature du travail signifie également une mauvaise utilisation de ses ressources.

Troisièmement, la capacité d'analyse d'une telle unité est pondérée par le nombre d'analystes judiciaire en fonction. Former un analyste judiciaire informatique autonome est un processus fastidieux et de façon générale peu d'enquêteurs souhaitent intégrer une unité spécialisée en criminalité technologique.

Quatrièmement, une unité spécialisée doit composer avec des ressources humaines et matérielles limitées. L'évolution des technologies nécessite une mise à jour constante des connaissances, des méthodes d'analyse et du matériel informatique. Ceci n'est pas toujours possible compte tenu des coûts engendrés. Toutefois, une saine gestion de ces ressources permet d'optimiser leur potentiel et d'éviter le gaspillage en temps et en argent.

Cinquièmement, il est désormais impossible d'analyser systématiquement l'ensemble des appareils numériques compte tenu de l'augmentation constante de la quantité de données qu'ils contiennent. Une telle unité doit donc transiger avec cette réalité et développer des stratégies afin de trier et d'ordonner les demandes de services. De plus, elle doit s'adapter aux impératifs organisationnels et composer avec des demandes urgentes ou des projets spéciaux.

### **3.1. La diffusion de l'expertise**

Afin de faire face au nombre grandissant de demandes, l'Unité a instauré un programme visant à former certains enquêteurs à l'analyse de cellulaires jugés « simples ». Cette formule permet d'alléger la tâche des analystes tout en permettant aux enquêteurs d'obtenir le contenu d'appareils évalués comme étant non prioritaires. Au sujet de ce programme, l'un des membres de l'Unité, P2, mentionne que l'Unité a mis en place une formation pour les personnes d'autres sections afin qu'ils puissent procéder à des analyses de bases, surtout de l'extraction de données. Cela permet que la demande ne soit pas purement rejetée, mais plutôt qu'elle soit traitée ailleurs. Néanmoins, il n'y a pas encore beaucoup de personnes qui se sont prévaluées de la possibilité de faire ces analyses qui nécessitent de se rendre à l'Unité pour utiliser les appareils nécessaires. Cela fait en sorte que l'Unité reçoit encore occasionnellement des demandes d'analyse de cellulaires d'autres sections.

Précédemment, il a été mentionné que ce programme a potentiellement réduit les demandes de 25% (voir chapitre IV, section 1.1.1). Même si ce programme peut être jugé comme une réussite, il appert que seulement un petit nombre d'enquêteurs se prévalent de ce privilège. Nonobstant le fait qu'une section s'est dotée de membres aptes à faire ce genre d'analyse, il semble qu'elle génère tout de même des demandes concernant des analyses qu'elle pourrait effectuer sans l'intervention directe de l'Unité.

Il appert donc que ce genre de programme a un impact positif mais le réel défi est d'encourager les départements et les sections à solliciter les enquêteurs formés plutôt qu'à recourir à une demande de service. Il semble y avoir une forme de résistance à l'utilisation de ce service. Plusieurs raisons pourraient expliquer cette résistance, notamment : le manque d'expérience relatif à l'utilisation des outils d'analyses, le manque d'intérêt ou de temps pour effectuer les analyses ou encore la peur de compromettre l'intégrité de la pièce à conviction ou des données contenues dans celle-ci.

Cet aspect de la diffusion de l'expertise pourrait faire l'objet de plus amples investigations. Dans cette optique, des données exactes sur l'utilisation de ce genre de programmes devraient

être colligées. Au minimum, le nombre de périphériques analysés, le nombre d'enquêteurs formés ainsi que la proportion d'enquêteurs utilisant le programme devraient être considérés.

### **3.2. L'effet CSI**

Afin de mieux faire comprendre les capacités de l'Unité des présentations sont dispensées aux enquêteurs des autres sections de l'organisation. L'objectif de ces ateliers est de sensibiliser les enquêteurs à la « sursaisie<sup>38</sup> » de matériel informatique, à la complexité des analyses judiciaires informatiques et de faire connaître les possibilités et les limites de ces analyses. Ce faisant, l'Unité outille ses clients afin qu'ils soient en mesure d'adresser des demandes cadrant le mieux possible avec les capacités et les priorités de l'unité.

P2 est chargé d'effectuer ces présentations. À ce sujet il mentionne que depuis quelques années des présentations quant aux capacités de l'Unité sont offertes aux autres. Malgré ces présentations, encore beaucoup d'intervenants ont de la difficulté à comprendre la complexité des analyses ou la quantité de données qu'il peut y avoir sur un disque dur.

À cet effet, P2 mentionne que des séries télévisées comme « CSI »<sup>39</sup> ont un effet très néfaste sur la perception générale que les individus ont de leur travail. Ce genre d'émission présente les techniques d'analyses comme étant extrêmement rapides et faciles. Ce biais de perception élève grandement les attentes que les autres ont de l'Unité. P2 traite d'ailleurs de cet « effet CSI » lors de ses présentations afin de sensibiliser les enquêteurs à ce phénomène et démystifier la nature réelle de leur travail.

Traditionnellement, la littérature scientifique décrit l'effet CSI comme une série de croyances et de perceptions erronées, concernant les analyses judiciaires, véhiculées par les médias de masse et certaines séries télévisées de fiction (Cooley, 2006; Schweitzer, 2007). Ces croyances, partagées par une partie de la population, recourent trois grands thèmes : 1) les

---

<sup>38</sup> L'Unité encourage les enquêteurs à restreindre la saisie de périphériques électroniques lors d'une perquisition à seulement ce qui est essentiel à l'avancement de l'enquête.

<sup>39</sup> « CSI: Crime Scene Investigation », une série télévisée très populaire concernant une équipe spécialisée d'analystes judiciaires a été présentée la première fois le 6 octobre 2000 sur CBS.



laboratoires de criminalistique sont des « sanctuaires » scientifiques toujours à la fine pointe de la technologie; 2) ces laboratoires emploient seulement les meilleurs scientifiques et ces derniers ne commettent jamais d'erreurs et finalement 3) les analystes judiciaires effectuent de la « vraie science » (Cooley, 2006).

L'effet CSI a été étudié surtout pour son impact sur les jurés. Cela mène généralement à deux cas typiques : soit il n'y a pas assez de preuves criminalistiques présentées pour convaincre de la culpabilité, soit les analyses judiciaires présentées en Cour sont perçues comme étant incontestables et les jurés penchent invariablement en faveur des conclusions de l'expert (Schweitzer, 2007).

Dans la présente, il s'agit d'une variante très intéressante de ce phénomène puisqu'il s'opère à l'intérieur même de l'organisation policière. Cela signifie qu'une proportion des enquêteurs connaît peu ou pas la nature des analyses effectuées par l'Unité. Cela peut engendrer la production de demandes de services inadéquates, la création d'attentes irréalistes, une sous-estimation du potentiel de la preuve digitale et la prolifération de stéréotypes néfastes.

Finalement, A1 mentionne qu'il y a : « Encore beaucoup d'éducation à faire pour expliquer la complexité de notre travail. [C'est le] syndrome de CSI [où] informatique rime avec automatique. ». Il semblerait donc que ce travail d'éducation et de sensibilisation soit un processus de longue haleine et qu'il soit nécessaire de le répéter fréquemment.

### **3.3. La formation du personnel**

Composer avec le manque de personnel qualifié est une réalité importante pour une unité spécialisée en criminalité technologique. La formation d'un seul analyste prend des années, est très coûteuse et peu d'individus sont intéressés à travailler dans ce domaine très spécifique.

À cet effet, A2 précise que le programme actuel de formation vise à amener un membre de l'organisation, avec peu ou pas de connaissances en informatique mais ayant un intérêt, à être capable d'effectuer des analyses judiciaires et ce en deux années. A1 mentionne toutefois qu'il y a une différence entre être formé puis être complètement à l'aise avec les analyses

judiciaires. Former un individu peut se faire en six mois, mais c'est l'expérience acquise au fil des enquêtes qui permet une plus grande aisance. A2 intervient et mentionne que cela dépend de l'individu : certains seront capable de faire ces analyses en quelques mois alors que pour d'autres le processus sera plus long. Cela dépend grandement des aptitudes et des connaissances de l'individu.

Finalement, A2 mentionne que l'Unité est un endroit où les enquêteurs deviennent très spécialisés dans un domaine d'enquête particulier et technique qui diffère des enquêtes régulières. Cela peut affecter les perspectives de carrière et faire en sorte que des enquêteurs ne seront pas intéressés à y travailler.

### **3.4. La gestion de ressources limitées**

Les technologies de l'information et des communications évoluant à très grande vitesse, il est nécessaire pour les analystes judiciaires informatiques de rester à jour autant au niveau du matériel et des outils d'analyse qu'au niveau de la formation et des techniques d'expertise. Par contre, l'achat de matériel tout comme le suivi de formations est coûteux.

P2 explique que si de nouvelles techniques ou technologies font leur apparition et que la formation n'a pas été offerte en contrepartie par rapport à ces techniques ou technologies, cela rend le travail plus difficile parce qu'il faut faire de la recherche supplémentaire. De plus, cela augmente le risque d'erreurs.

Dans une perspective de bonne gestion des ressources humaines et financières, certaines analyses judiciaires entraînant des coûts importants sont parfois refusées. À cet effet, A2 souligne que l'importance du dossier ou la gravité du crime risque d'influencer la gamme de techniques utilisées. A2 mentionne à titre d'exemple que dans un cas de fraude de moins de cinq mille dollars, on évitera d'effectuer des analyses avancées susceptibles d'excéder cinq mille dollars.

La capacité de traitement ainsi que les coûts importants reliés à certaines analyses obligent une rationalisation des ressources disponibles. Une mauvaise utilisation des services offerts par

une unité spécialisée peut dilapider rapidement des ressources qui auraient été mieux attribuées autrement.

A2 mentionne que certains clients avaient l'habitude de tout envoyer les éléments de preuve pour analyse alors que certains éléments n'étaient pas utiles. Lorsqu'on rappelait le client plus tard pour savoir s'ils avaient bien besoin de l'analyse demandée, on se rendait compte que non seulement l'analyse pouvait ne pas être nécessaire mais que parfois le dossier était clos ou que le suspect avait finalement plaidé coupable.

Une mauvaise communication ou la mauvaise évaluation de l'importance de l'analyse d'une pièce à conviction est susceptible d'engendrer des pertes en temps et en argent.

Finalement, P2 aborde les coûts reliés à la création d'une équipe spécialisée. Compte tenu de l'augmentation des enquêtes technologiques menées directement par l'Unité, l'organisation prévoit former une équipe d'enquête cybernétique attitrée uniquement à ce type d'enquêtes. Ceci étant dit, lorsqu'on demande du personnel supplémentaire il y a souvent des questions d'argent qui entrent en ligne de compte.

De façon générale, les contraintes budgétaires constituent un important frein au développement, à long terme, des unités spécialisées. Souvent des budgets importants sont débloqués durant la phase d'adoption de l'innovation mais pour différentes raisons ces budgets s'effritent progressivement. Ces unités spécialisées doivent donc composer avec moins de ressources une fois le budget initial dépensé.

### **3.5. Les priorités organisationnelles**

Dans la perspective d'une gestion efficace des ressources, des priorités doivent être établies. Toutefois, ces priorités peuvent changer et sont sujettes à des impératifs divisionnaires changeants. De plus des opérations et des projets ad hoc sont susceptibles de changer les priorités momentanément.

P2 donne un exemple de ce phénomène. Il rapporte que depuis quelques années, le département de la sécurité étatique travaille sur des projets d'envergure. Quand il travaille sur ces projets, ils recrutent beaucoup de personnes des autres sections. Cela entraîne une diminution des demandes provenant des sections touchées puisque les enquêteurs recrutés ne travaillent plus sur leurs propres dossiers.

Selon P2 les opérations et les projets spéciaux accaparent de 50 à 70 pour cent du volume de travail de l'Unité. De plus, lorsque ces projets d'envergure se préparent, une attention particulière est portée à la preuve numérique et l'Unité est directement consultée.

Par contre, l'élaboration de priorité signifie également que certaines demandes seront reléguées au second plan ou même complètement refusées. P2 mentionne l'exemple de l'analyse de cellulaires pour fin d'intelligence : on a constaté avec le temps que ces analyses représentaient une bonne proportion du volume de travail. Puisqu'il ne s'agissait pas d'une priorité, ces demandes étaient toujours repoussées, mais dans les faits on ne les traitait jamais. Nous avons simplement décidé de ne plus accepter ce type de demande.

Avec l'omniprésence des appareils numériques, il est maintenant invraisemblable de tout analyser. L'élaboration de protocoles de triage, de stratégies de gestion et de priorités organisationnelles est inévitable.

#### **4. Synthèse du chapitre**

Le présent chapitre a traité des enjeux et défis inhérents à une unité spécialisée en analyse judiciaire informatique et en criminalité technologique. Un des plus grands enjeux d'une telle unité est sans aucun doute l'accumulation des demandes de service. À cet effet, une grande variété de facteurs organisationnels et environnementaux est susceptible d'affecter le délai de traitement. Ces différents facteurs interviennent tout au long du processus de demande de service. Initialement, la qualité de la demande et la bonne communication entre les intervenants sont essentielles. Par après, des facteurs relatifs à la technologie, aux priorités organisationnelles ainsi qu'à l'unité elle-même détermineront la vitesse de traitement de la demande.

À l'ère numérique, la démocratisation des appareils mobiles, l'évolution rapide des technologies et l'augmentation de la capacité des périphériques constituent de véritables défis pour une telle unité spécialisée. Il est très difficile pour les analystes de rester à jour au niveau des techniques d'analyses et des connaissances informatiques; le besoin pour de la formation continue est évident. De plus, le matériel d'analyse n'évolue pas aussi rapidement que la sortie des nouvelles technologies ce qui complexifie d'autant plus la tâche.

Le système de justice cherche également à encadrer de façon de plus en plus contraignante la preuve numérique, les analyses judiciaires informatiques et les processus qui en découlent. La quantité de données personnelles contenues dans les appareils numériques rend de plus en plus grande l'expectative de vie privée. Il est donc nécessaire pour les enquêteurs de préciser ce qu'il cherche et de justifier avec plus de rigueur pourquoi ces informations se trouveraient sur un appareil digital.

En plus des facteurs extérieurs, de nombreuses restrictions et limitations organisationnelles viennent s'ajouter aux défis d'une unité spécialisée en criminalité technologique. Les priorités organisationnelles, les urgences occasionnelles, les ressources limitées et le manque de formation sont des facteurs importants. De plus, un travail d'éducation constant est nécessaire afin de sensibiliser l'organisation aux capacités d'analyse réelles et aux limites techniques d'une telle unité. Finalement, la prédominance de projets spéciaux vient occasionnellement chambouler les priorités. Toutefois, ces projets constituent une grande partie du volume de travail.

Pour une telle unité, il est essentiel de prendre conscience de ces défis et de quantifier leur impact sur leur travail. Pour ce faire un processus d'introspection est nécessaire et colliger des données sur la nature de leur travail peut grandement faciliter ce travail.

---

## **Chapitre VI**

### **Synthèse, réflexions et conclusion**

---

Le dernier chapitre vise à synthétiser l'ensemble des éléments recueillis au cours du présent projet de stage. Dans un premier temps, un résumé des principales caractéristiques de l'Unité et des défis importants que ses membres doivent surmonter sera présenté. Un retour sera fait sur les thèmes les plus significatifs abordés aux chapitres IV et V. Une importance particulière sera accordée aux faits soulignés et aux opinions énoncées par les membres de l'Unité.

Dans un deuxième temps, afin de généraliser les éléments et les thèmes abordés au cours du présent projet, ces derniers seront articulés à l'aide de la théorie du processus d'innovation dans les organisations, tel qu'élaborée par Rogers (2003). Plus particulièrement, une analyse sera effectuée en fonction de la phase d'implantation, puisque les données recueillies dans la présente étude concernent une unité déjà en place depuis plus de dix ans. Cette analyse visera à débusquer les pièges pouvant faire échouer l'implantation de ce genre d'unité. Cet exercice permettra d'énoncer des principes généraux applicables à toutes les unités spécialisées en analyses judiciaires informatiques et démontrer la complexité de ce processus d'implantation.

Finalement, des constats et des réflexions émanant du présent projet seront formulés. Il y aura élaboration de certaines recommandations concernant l'avenir de ces unités spécialisées. De plus, les implications de cette étude pour les milieux académique et policier seront discutées. En guise de conclusion, la contribution de cette étude sera mentionnée et certaines pistes de recherche pour de futures études seront énoncées.

## **1. Résumé des faits saillants**

La présente section revisite l'ensemble des thèmes et des éléments importants abordés au cours des précédents chapitres d'analyse. Il sera premièrement question du profil général des clients de l'Unité. La nature des infractions enquêtées par les principaux demandeurs sera abordée ainsi que les types de services les plus souvent requis. Par la suite, un portrait de la réalité quotidienne de cette unité spécialisée sera tracé afin de démontrer l'ampleur et la variété des obstacles à surmonter. Finalement, les données et les témoignages recueillis permettront de jeter un regard nouveau sur la criminalité technologique.

## **1.1. Le profil des clients de l'Unité**

Compte tenu du mandat de l'organisation policière, les demandes d'assistance envoyées à l'Unité concernent principalement la sécurité de l'état (surtout en ce qui a trait au financement terroriste), la criminalité économique (*white-collar crime*) et les droits d'auteur. Dans une moindre mesure, des dossiers concernant le gangstérisme et la criminalité organisée ainsi que les stupéfiants sont également traités. De plus, récemment il semble avoir une recrudescence des cas de fraude par télémarketing.

Par conséquent, les clients effectuant la majorité des demandes de service sont les départements de la criminalité économique, de la criminalité organisée et de la sécurité étatique. Qui plus est, environ une demande sur dix (10) provient d'un autre service de police.

Une importante portion du volume de travail de l'Unité est attribuable aux opérations et aux projets spéciaux; une des grandes priorités de l'organisation. Les aléas de ces opérations d'envergure ont pour effet de faire fluctuer l'affluence des demandes de service à l'Unité. Cette dernière n'ayant qu'un contrôle très réduit sur ces fluctuations. Toutefois, les individus chargés de coordonner ces projets prennent de plus en plus souvent le temps de consulter les membres de l'Unité et de les l'inclure dès le début de l'enquête dans la planification des opérations.

## **1.2. La réalité d'une unité de soutien spécialisée en criminalité technologique**

Le quotidien d'une unité spécialisée en analyse judiciaire informatique est peuplé de défis techniques, humains et organisationnels. Cette section résume brièvement la complexité de cette réalité en mettant l'accent sur les capacités limitées d'une telle unité ainsi que sur la perception que les autres se font de ses moyens.

### *1.2.1. Des capacités limitées pour répondre à une demande croissante*

La démocratisation des appareils numériques, l'accroissement du besoin en expertise judiciaire informatique ainsi que la « sursaisie » de matériel informatique ont causé l'augmentation de la quantité des demandes de service adressées à l'Unité. Cette augmentation est d'ailleurs similaire à celle observée par d'autres auteurs (McMillan & al., 2013; Quick &



Choo, 2014; Turnbull & al., 2009). Afin de maintenir un arriéré raisonnable, une grande diversité de stratégies a dû être déployée pour réguler l'affluence des demandes de service. Premièrement, un système de priorisation des demandes a été élaboré afin de traiter en premier les demandes nécessitant une attention immédiate. Deuxièmement, les diverses sections de l'organisation ont été sensibilisées, à l'aide de présentations, à la « sursaisie » de matériel informatique, à la réalité du travail de l'Unité ainsi qu'à l'importance de la preuve numérique. Troisièmement, des programmes de formation ont été élaborés afin de permettre à certains enquêteurs de traiter eux-mêmes les périphériques et appareils numériques dont l'analyse est jugée simple. Quatrièmement, l'Unité effectue de plus en plus uniquement l'extraction de la preuve numérique laissant l'analyse de celle-ci aux enquêteurs. Cinquièmement, les critères relatifs à l'acceptation d'une demande de service ont été resserrés. Il est nécessaire que la demande soit dûment remplie et que le demandeur démontre de quelle manière l'expertise requise fera progresser son dossier. On s'assure ainsi que les « parties de pêche » et les demandes concernant uniquement du renseignement soient refusées.

L'ensemble de ces initiatives a eu pour effet de filtrer de façon appréciable les demandes acheminées à l'Unité. On s'assure ainsi que leur expertise ne soit pas utilisée à mauvais escient, mais plutôt consacrée à des tâches cadrant avec les priorités organisationnelles. Compte tenu des effectifs humains et matériels limités, cette rationalisation des activités assure que les enquêtes nécessitant réellement une expertise judiciaire informatique l'obtiennent, et ce, dans un délai raisonnable.

### *1.2.2. Une expertise méconnue*

L'effet « CSI » réfère à une série de croyances erronées concernant la science et les analyses judiciaires. Traditionnellement, ce phénomène a surtout été étudié auprès de la population en général et visait à déterminer l'impact de cet effet sur les jurés lors d'un procès (Cooley, 2006; Schweitzer, 2007). Toutefois, selon les membres de l'Unité, ces croyances et ces perceptions erronées sont également présentes au sein même de leur organisation. En effet, une connaissance étendue des analyses informatiques judiciaires et de la preuve numérique n'est pas donnée à tous; un travail d'éducation et de sensibilisation est donc nécessaire. Des présentations sont dispensées fréquemment aux autres sections afin de démystifier la preuve

numérique et d'expliquer les possibilités et les limites inhérentes aux analyses judiciaires informatiques. Ce travail est constamment à refaire puisque le fort roulement du personnel favorise la dissipation de ces connaissances. Il est donc essentiel de répéter fréquemment cet effort de conscientisation en s'assurant de maintenir un partenariat efficace avec l'ensemble des autres sections. De façon générale, une bonne communication favorise grandement l'ensemble du processus de demande, assure de bons résultats et génère une meilleure satisfaction de la part de tous les intervenants.

### **1.3. La criminalité technologique**

En 2014, virtuellement toutes les formes de criminalité sont susceptibles d'avoir une composante informatique, la quasi-entière de la population nord-américaine possédant un ordinateur ou un téléphone cellulaire intelligent. Nous croyons même qu'aujourd'hui il n'est plus pertinent de faire la distinction entre criminalité et criminalité technologique puisque les enquêtes policières à l'ère numérique impliquent nécessairement la présence de preuves se trouvant, en partie ou la totalité, sur un support numérique. La pertinence de cette preuve, pour un dossier donné, doit toutefois être évaluée.

L'analyse des types de périphériques (voir chapitre IV, section 1.6) expertisés par l'Unité montre d'ailleurs que les délinquants adoptent les nouvelles technologies de façon similaire au reste de la population. La diversité des crimes touchés par les analyses informatiques de l'Unité démontre également que la criminalité technologique n'est pas l'affaire d'un seul type de délinquant, elle se trouve plutôt dans toutes les sphères de la société.

Une distinction doit tout de même être faite entre la criminalité technologique et la criminalité informatique ou cybercriminalité. En ce qui concerne cette dernière, une certaine forme d'expertise informatique est nécessaire autant dans la commission de cette forme de criminalité que dans son investigation. Pour l'instant la cybercriminalité ne représente qu'une petite partie du travail de l'Unité (moins de 1% des demandes), toutefois l'organisation songe à former une équipe dédiée à la lutte à la cybercriminalité, signe que cette forme de criminalité est réelle et en hausse.

D'autre part, un défi technologique majeur est l'augmentation de la capacité de stockage des appareils numériques. Même si les mécanismes de filtrage et de priorisation limitent le nombre de demandes acheminées, il n'en demeure pas moins que la quantité de données augmente constamment. Selon les membres de l'Unité, rester à jour autant au niveau de la formation que des outils d'analyse s'avère le défi technologique le plus important. D'autant plus que l'apparition de nouvelles technologies sera toujours accompagnée par sa potentielle utilisation criminelle. À cet égard, l'informatique en nuage pourrait constituer l'un des prochains défis importants pour les unités spécialisées en criminalité technologique, les données n'étant plus stockées physiquement sur l'ordinateur du suspect.

## **2. L'implantation d'une unité policière spécialisée en analyse judiciaire informatique**

L'évolution parallèle de la société, des technologies et de la criminalité a forcé l'élaboration de techniques permettant de tirer profit de la preuve numérique. Par le concours de forces endogènes et exogènes certaines grandes organisations policières se sont dotées d'unités spécialisées en criminalité technologique aptes à analyser cette preuve numérique. Une fois la décision prise d'adopter cette innovation, une série de facteurs doivent être considérés afin de mener à bien l'implantation de cette dernière.

Selon Rogers (2003) la phase d'implantation du processus d'innovation dans les organisations est divisée en trois étapes : la redéfinition et la restructuration, la clarification et l'intégration aux activités routinières. À l'aide de cette théorie, les constats effectués dans le présent projet pour l'Unité seront généralisés à une organisation fictive souhaitant se doter d'une équipe spécialisée en criminalité technologique. Le but de cet exercice est d'alimenter les réflexions et de souligner la complexité d'une telle entreprise.

### **2.1. La redéfinition et la restructuration**

Selon Rogers (2003), à l'étape de la redéfinition et de la restructuration, l'innovation est modifiée et adaptée afin de se conformer aux exigences de l'organisation. De plus, la structure de l'organisation est altérée afin de faire place à l'innovation.

Dans la présente, de nombreux processus administratifs doivent être créés afin d'encadrer le cheminement des demandes à l'unité spécialisée. Les éléments suivants devraient être considérés lors de cette étape :

*Objectifs généraux :*

- Établir les orientations stratégiques de l'unité spécialisée et déterminer son rôle au sein de l'organisation;
- Établir la structure de l'unité spécialisée et sa place dans la hiérarchie organisationnelle;
- Recruter du personnel à l'externe ou réallouer des effectifs internes à l'unité;
- Allouer un budget pour l'aménagement, l'achat d'équipements et la formation du personnel.

*Concernant le mécanisme de prestation de service :*

- Établir un processus administratif afin d'acheminer les demandes de service du demandeur vers l'unité spécialisée;
- Établir une stratégie de priorisation des demandes;
- Maintenir un historique de l'ensemble des demandes adressées à l'unité spécialisée;
- Effectuer une présentation auprès de tous les individus susceptibles d'utiliser ce service afin de leur expliquer le fonctionnement de celui-ci;
- S'assurer d'une bonne communication entre le demandeur et l'unité spécialisée tout au long du processus d'expertise.

*Concernant l'expertise interne :*

- Établir un programme de formation pour les nouveaux membres de l'unité en tenant compte des exigences du milieu (accréditations, standards, etc.);
- Participer à des forums et à des tables de discussion afin de former des partenariats avec d'autres organisations possédant une expertise similaire;
- Établir un mécanisme de recherche et développement afin d'avoir des solutions d'analyse pour les technologies émergentes;
- Faire accréditer ou tester les outils d'analyse utilisés afin de s'assurer de leur fiabilité et de la reproductibilité des analyses;
- Établir des procédures internes et des meilleures pratiques concernant chacun des types d'analyses effectuées.

*Autres considérations :*

- Si l'organisation est un organisme chargé d'appliquer la loi, considérer :
  - L'établissement de mécanismes assurant l'étanchéité de la chaîne de possession;
  - Le respect des exigences judiciaires en matière d'expertise et d'analyses reconnues;

- Demander au contentieux de rester à l'affût des jurisprudences pouvant influencer le travail de l'unité. Le cas échéant, communiquer un résumé des décisions à l'unité accompagnée d'une opinion juridique.

## **2.2. La clarification**

Lors de cette étape, le rôle de l'innovation se définit et la relation entre cette dernière et l'organisation se clarifie (Rogers, 2003). L'organisation devrait donc avoir une idée plus claire du rôle que joue son unité spécialisée et de quelle manière elle souhaite orienter la prestation de service. L'organisation devrait se poser les questions suivantes :

- Les objectifs stratégiques définis initialement sont-ils respectés ?
- L'arriéré de l'unité spécialisée est-il acceptable ? Sinon, comment l'améliorer ?
- Y-a-t-il nécessité d'agrandir l'unité ou acheter de nouveaux équipements ?
- Quel est le type de demande le plus souvent acheminée à l'unité ?
- Le processus de priorisation des demandes sert-il son objectif ?

De plus, à ce moment l'organisation devrait effectuer des vérifications internes afin de diagnostiquer tout problème relié à l'unité. L'historique des demandes de services devrait être utilisé dans ce processus d'évaluation afin de produire des statistiques pertinentes sur l'utilisation du service et effectuer un profil des principaux clients et du genre de demandes acheminées. Ce processus d'introspection devrait permettre de corriger les problèmes rencontrés et réorienter les objectifs de l'unité afin de mieux refléter les priorités organisationnelles.

## **2.3. L'intégration aux activités routinières**

Finalement, cette étape consiste à l'incorporation complète de l'innovation aux activités de l'organisation (Rogers, 2003). L'innovation n'est donc plus considérée comme un corps étranger mais fait plutôt partie intégrante de l'organisation.

En l'espèce, même si à cette étape l'Unité a fait ses preuves, les défis technologiques demeurent toujours présents. En effet, une fois la phase d'intégration aux activités routinières atteinte, les contraintes endogènes sont réduites au minimum. Les processus internes sont bien établis et l'ensemble de l'organisation possède une connaissance suffisante de la nature du travail de l'unité et des mécanismes encourageant les demandes de service. Néanmoins, les

facteurs exogènes continuent d'exercer une pression sur l'Unité; elle devra s'assurer de maintenir à jour son expertise (par la formation et la recherche), actualiser ses outils d'analyse périodiquement et s'ajuster à l'environnement technologique et juridique changeant.

#### **2.4. Implantation d'une unité spécialisée : un cas réel**

Lors de notre stage, nous avons eu la chance de rencontrer un inspecteur-enquêteur d'une agence gouvernementale. Ce dernier est actuellement en formation à l'Unité puisque son employeur a décidé d'implanter une unité spécialisée en analyse judiciaire informatique au sein de leur organisation. Cet exemple démontre concrètement la pertinence des constatations amenées jusqu'à présent.

L'inspecteur-enquêteur relate qu'il y a quelques années leur organisation a réalisé l'importance de la preuve numérique dans leurs enquêtes. Il explique qu'ils ont commencé à faire affaire avec un tiers pour les aider dans l'analyse et la saisie du matériel informatique, toutefois des coûts importants étaient reliés à cette assistance. De plus, le tiers avait une charge de travail de plus en plus importante, ce qui faisait en sorte qu'il avait moins de temps pour procéder aux analyses requises par l'agence.

Par la suite, il explique qu'ils ont aussi fait affaire avec l'organisation policière de l'Unité, mais eux aussi étaient débordés et arrivaient difficilement à analyser la preuve numérique qui n'était pas jugée comme étant reliée à des dossiers prioritaires. Pour ces raisons, leur organisation a commencé à penser sérieusement à former leur propre équipe afin que de traiter les dossiers dans un délai raisonnable et d'éviter les coûts importants reliés à ce genre d'expertise.

L'inspecteur rencontré a été choisi par son organisation pour devenir analyste judiciaire informatique même s'il n'a que très peu d'expérience dans le domaine. Nous lui avons posé la question : « Selon vous, quels sont les principaux défis reliés à la création d'un tel programme ? ». Il nous a répondu qu'il s'agissait de l'ampleur de la formation requise.

Il nous a rapporté que l'entraide dans le milieu et le partage de l'expérience acquise par les membres de l'Unité facilitait toutefois ce processus.

Finalement, il aborde les coûts importants reliés à l'achat du matériel informatique et au renouvellement des licences d'utilisation des logiciels d'analyse. Il souligne aussi que l'évolution rapide des technologies oblige à réapprendre souvent des éléments qu'on croyait acquis. De façon générale, il croit qu'il y a tellement de choses à apprendre dans le milieu que c'est plus facile de se spécialiser et de recourir à l'aide d'autres partenaires pour les analyses avec lesquelles on est moins familier. Ainsi tout le monde possède une expertise plus pointue et la collaboration est la clef.

Notre entrevue avec cet inspecteur nous a permis de constater les nombreux défis reliés à la création et à l'implantation d'une unité spécialisée en analyse judiciaire informatique. Ces propos confirment que le processus d'implantation est coûteux et nécessite un investissement en temps et en argent. De plus, il réitère l'importance d'avoir des partenaires et des mentors d'expérience. Le développement d'une telle expertise est donc un processus difficile, mais il permet à toute organisation empruntant cette voie de bénéficier d'une plus grande autonomie et de réduire les délais reliés au traitement de la preuve numérique.

### **3. Implications pour les organisations policières et la recherche scientifique**

Cette section conclut le présent projet de recherche en entamant une réflexion sur les unités spécialisées en analyses judiciaires informatiques et leur avenir. À l'aide des éléments recueillis dans la présente étude, des constats et des suggestions sont formulés afin d'assurer la pérennité de telles unités.

#### **1) Garder un historique des demandes de service et des périphériques traités au fil des années afin de permettre une meilleure introspection.**

Le nombre de demandes, en valeur absolue, n'est pas nécessairement le meilleur indicateur de la charge de travail. En effet, compte tenu de la grande variété des tâches exécutées et la complexité relative des demandes, il est important de catégoriser les types d'analyse effectués

et compiler la nature et le nombre de pièces à conviction traitées. Consigner les temps d'analyse, la quantité de données traitée ainsi que le délai de traitement du début à la fin de la demande s'avère également essentiel. Ces données permettront de créer un historique du travail de l'unité et ainsi favoriser l'évaluation de sa performance et le diagnostic des problématiques rencontrées. Un tel registre permet aussi de rendre des comptes aux instances supérieures et de justifier l'investissement de ressources additionnelles dans un tel programme.

## **2) Le piratage informatique n'est qu'une petite partie de la criminalité technologique.**

Quoique très sensationnels et « glamours », les pirates informatiques ne constituent qu'une petite partie des délinquants s'adonnant à la criminalité technologique. Tel que vu précédemment (chapitre IV, section 1.5), les demandes de service relatives à du piratage informatique représente moins d'un pour cent de l'ensemble de la criminalité technologique. En effet, l'utilisation de la technologie dans la commission d'actes délictueux est maintenant un incontournable. Il pourrait être toutefois fort intéressant d'examiner et de comparer le niveau de sophistication technologique propre à plusieurs types d'infractions. Qui plus est, de la même manière que certains outils facilitent la perpétration de certains crimes, certaines technologies sont probablement plus fortement associées à certaines formes de délinquance. Explorer ces pistes de recherches s'avérerait sans aucun doute très profitable et augmenterait les connaissances sur le sujet.

## **3) La recherche criminologique sur les unités spécialisées en analyse judiciaire informatique permet aussi d'augmenter les connaissances sur la criminalité technologique.**

De par la nature de ces unités spécialisées, qui souvent agissent en soutien aux autres services d'enquêtes policières, elles sont souvent appelées à toucher à une grande variété de formes de criminalité. Tous ces dossiers ont toutefois la particularité de comporter un élément informatique. L'analyse du genre de dossiers traités permet donc d'avoir une vision partielle de l'état de la criminalité technologique. Il est nécessaire d'être prudent quant à la généralisation de ces données. Toutefois, en situant bien le rôle de l'unité et la juridiction du



service de police il est possible d'obtenir des données et des analyses révélant une facette de la criminalité technologique et informatique.

**4) Compte tenu de l'augmentation de la preuve numérique et de l'omniprésence de la criminalité technologique, les sections d'enquêtes ne devraient-elles pas toutes posséder leur propre unité interne spécialisée en analyse judiciaire informatique ?**

Il est raisonnable de se questionner sur le sujet, car avec l'augmentation de la capacité de stockage des appareils numériques (Quick & Choo, 2014) et de la présence grandissante de la preuve numérique dans les enquêtes (Turnbull & al., 2009), ces unités sont susceptibles de ne plus fournir à la tâche. Posséder des enquêteurs-analystes judiciaires dédiés spécifiquement à une section signifierait également le développement d'une expertise d'analyse concernant une forme particulière de criminalité. Dans une perspective à long terme, il pourrait donc être souhaitable d'avoir des enquêteurs capables d'effectuer des analyses informatiques judiciaires de bases tout en conservant une unité capable de répondre aux demandes plus techniques et spécialisées.

**5) De plus en plus d'organisations chargées d'appliquer la loi doivent se doter d'une unité spécialisée en criminalité technologique.**

Tel qu'illustré par l'exemple de l'agence mentionnée ci-haut (chapitre VI, section 2.4), de plus en plus d'organisations effectuant des perquisitions et la saisie de matériel informatique constituent leur propre équipe d'analyse judiciaire informatique afin d'éviter les coûts importants reliés à la sous-traitance. De plus, cette pratique accélère grandement la vitesse de traitement des pièces à conviction. Dans le futur, il est raisonnable de croire que ce genre d'unité deviendra la norme. Toutefois, elles ne seront pas toutes en mesure de maintenir une expertise à la fine pointe de la technologie puisque les coûts reliés à la formation et à l'équipement sont exorbitants. L'importance de former des partenariats ou des associations entre ces unités est d'autant plus essentielle afin de favoriser le partage de l'expertise.

### **Conclusion et mot de la fin**

Les unités spécialisées en analyse judiciaire informatique entretiennent un lien étroit avec l'innovation. Elles sont à la merci des évolutions technologiques qui dictent une grande partie de leur travail. Nous croyons qu'il est même possible de parler de « dépendance » à l'innovation. En effet, les technologies de l'information et des communications se renouvelant constamment, il devient essentiel pour ces unités de développer des stratégies systémiques afin d'innover. Une forme de vigie doit être levée, permettant de détecter les nouvelles innovations, de juger de leur pertinence et de les intégrer au besoin au fonctionnement de l'unité.

Dans la présente, l'Unité semble être au fait de ces changements et de l'évolution rapide des technologies. Toutefois, des contraintes, principalement budgétaires, ne permettent pas de renouveler suffisamment rapidement le matériel d'analyse et limitent l'accès à de la formation continue. Un fossé semble donc se creuser entre la capacité de traitement de l'Unité et la demande grandissante. Qui plus est, cette demande comporte trois aspects distincts, tous susceptibles de croître : la quantité de demandes, la quantité de pièces à analyser par demande ainsi que la quantité de données contenue dans chacune des pièces. L'amalgame de ces trois aspects peut rapidement causer un débordement de la charge de travail.

L'élaboration de procédure visant la priorisation et le filtrage des demandes de service adressées semble un incontournable. En la matière, l'Unité semble avoir développé des procédures qui ont permis de maintenir l'équilibre en leur capacité de traitement et la demande. Ce type d'innovations « administratives » est sans aucun doute aussi important que les innovations de nature technologique.

D'autre part, l'Unité semble se préoccuper de plus en plus de la criminalité « purement informatique ». Cette forme de criminalité semble en hausse depuis quelques dernières années, ce qui pousse l'organisation à former une équipe entièrement dédiée à contrer la cybercriminalité. Cette autre innovation est susceptible de développer une expertise essentielle pour l'avenir.

En ce qui concerne le présent projet de stage, la présence de mécanismes d'évaluation aurait grandement facilité la collecte de données. À cet effet, nous encourageons les organisations policières à mettre en place des outils permettant la mesure, l'évaluation et la collecte systématique d'informations concernant le nombre de requêtes d'assistance reçues, la quantité de pièces à conviction traitées, la quantité de données examinées ainsi que la nature des périphériques analysés.

Également, nous incitons fortement les chercheurs à répéter notre expérience dans d'autres unités de ce genre. Il serait ainsi possible de contraster les résultats obtenus afin d'avoir une vision complémentaire de l'évolution des analyses judiciaires informatiques, de la preuve numérique et de la criminalité technologique. De plus, il s'avère que de par leur nature les unités spécialisées en criminalité informatique touchent à une grande variété de dossiers d'enquête. Examiner les enquêtes traitées par différentes unités spécialisées en analyse judiciaire informatique pourrait contribuer à avoir une vision plus complète de la criminalité technologique dans son ensemble.

En conclusion, il est clair que la présente étude ne fait qu'effleurer un le sujet. Par contre, elle permet de mieux comprendre la nature des unités spécialisées en analyse judiciaire informatique et leur relation étroite avec l'innovation. Dans une mesure, il a été possible de quantifier l'ampleur de leur travail, de mieux comprendre les défis auxquels ils font face et de souligner la nécessité qu'ils ont de constamment renouveler leur pratique.

## Références

- Association des banquiers canadiens (2014). *Les Canadiens et leurs services bancaires*. Récupéré le 23 novembre, 2014, de <http://www.cba.ca/fr/media-room/50-backgrounders-on-banking-issues/125-technology-and-banking>
- Baker, W., Hutton, A., Hylender, C. D., Pamula, J., Porter, C., & Spitler, M. (2011). 2011 data breach investigations report. *Verizon RISK Team, Available: www.verizonbusiness.com/resources/reports/rp\_databreach-investigations-report-2011\_en\_xg.pdf*, 1-72.
- Bossler, Adam M. & Holt, Thomas J. (2009). *On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory*. *International Journal of Cyber Criminology*, 3 (1), 400–420.
- Brodeur, J. P. (2010). *The policing web*. Oxford University Press.
- Carof, S. (2007, 5 octobre). Gabriel Tarde (1843-1904) - Les lois de l'imitation. *Sciences Humaines*. Récupéré le 2 janvier 2014, de [http://www.scienceshumaines.com/gabriel-tarde-1843-1904-les-lois-de-l-imitation\\_fr\\_21353.html](http://www.scienceshumaines.com/gabriel-tarde-1843-1904-les-lois-de-l-imitation_fr_21353.html)
- Charters, I. (2009). The Evolution of Digital Forensics: Civilizing the Cyber Frontier. Récupéré le 23 novembre, 2014, de <http://www.guerilla-ciso.com/wp-content/uploads/2009/01/the-evolution-of-digital-forensics-ian-charters.pdf>
- Choi, K.-S. (2008). *Computer Crime Victimization and Integrated Theory: An Empirical Assessment*. *International Journal of Cyber Criminology*, 2 (1), 308–333.
- Cooley, C. M. (2006). CSI Effect: Its Impact and Potential Concerns, The. *New Eng. L. Rev.*, 41, 471.
- Damanpour, F. (1991). Organizational innovation: A meta-analysis of effects of determinants and moderators. *Academy of management journal*, 34(3), 555-590.
- Dunham, K. (2005). Wireless Worries and Wisdom. *Information Systems Security*, 14(3), 5-8.
- Ericson, R. V. & Haggerty, K. D. (1997). *Policing the risk society*. Oxford University Press.
- Fagerberg, J., Mowery, D. C., & Nelson, R. R. (Eds.). (2006). *The Oxford handbook of innovation*. Oxford Handbooks Online.
- Garicano, L., & Heaton, P. (2010). Information Technology, Organization, and Productivity in the Public Sector. *Journal of Labor Economics*, 28(1), 167-201.
- Gendarmerie royale du Canada – GRC (2012). *Vérification du Programme de la criminalité technologique*. Récupéré le 12 mai, 2014, de <http://www.rcmp-grc.gc.ca/aud-ver/reports-rapports/tech-crime-crimin-tech-fra.htm>
- Grabosky, P. N. (2007). *Electronic crime*. Upper Saddle River, NJ: Pearson Prentice Hall.
- Gundenon, L. & Brown, D. (2000). *Using a Multi-Agent Model to Predict Both Physical and Cyber Criminal Activity*. Department of Systems Engineering, Thornton Hall, Charlottesville, VA.

- den Hengst, M. & Warnier, M. (2013). Cyber Crime in Privately Held Information Systems: Personal Data at Stake. *Intelligence and Security Informatics Conference (EISIC)*, 117-120.
- Hollenstein, H. (2004). Determinants of the adoption of information and communication technologies (ICT): an empirical analysis based on firm-level data for the Swiss business sector. *Structural change and economic dynamics*, 15(3), 315-342.
- Hinduja, S. (2007). Computer crime investigations in the United States: leveraging knowledge from the past to address the future. *International Journal of Cyber Criminology*, 1(1), 1-26.
- Hutchings, A. & Hayes, A. (2008). *Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'?* Current Issues IN Criminal Justice, 20 (3).
- Lessard, C., & Belleau, L. (2013). *L'enquête québécoise sur l'accès des ménages à Internet 2012 : Présentation et analyse des résultats*. Institut de la statistique du Québec, Gouvernement du Québec.
- Jewkes, Y., & Yar, M. (Eds.). (2013). *Handbook of Internet crime*. Routledge.
- Katz, C. M., Maguire, E. R., & Roncek, D. W. (2002). The creation of specialized police gang units: A macro-level analysis of contingency, social threat and resource dependency explanations. *Policing: An International Journal of Police Strategies & Management*, 25(3), 472-506.
- Kelling, G. L., & Moore, M. H. (1988). *The evolving strategy of policing*. US Department of Justice, Office of Justice Programs, National Institute of Justice.
- King, W. R. (1998). *Innovativeness in American municipal police organizations* (Doctoral dissertation, University of Cincinnati).
- King, W. R. (1999). Time, constancy, and change in American municipal police organizations. *Police Quarterly*, 2(3), 338-364.
- King, W. R. (2000). Measuring police innovation: issues and measurement. *Policing: An International Journal of Police Strategies & Management*, 23(3), 303-317.
- Klinger, D. A. (2003). Spreading diffusion in criminology. *Criminology & Public Policy*, 2(3), 461-468.
- Kraska, P. B., & Kappeler, V. E. (1997). Militarizing American police: The rise and normalization of paramilitary units. *Soc. Probs.*, 44 (1).
- Manning, P. K. (2008). *The technology of policing: crime mapping, information technology, and the rationality of crime control*. NYU Press.
- McQuade, S. C. (2001). *Cops versus crooks: Technological competition and complexity in the co-evolution of information technologies and money laundering* (Doctoral dissertation, George Mason University).
- McMillan, J. E. R., Glisson, W. B., & Bromby, M. (2013). Investigating the increase in mobile phone evidence in criminal activities. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on System Sciences*, 4900-4909.
- Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics*, 38(8).

- Moore, M. H. (2003). Sizing up Compstat: an important administrative innovation in policing. *Criminology & Public Policy*, 2(3), 469-494.
- Moore, M. H., Sparrow, M., & Spelman W. (1997) Innovations in policing: from production lines to jobs shops. In *Innovation in American Government: Challenges, Opportunities, and Dilemmas* (ed. A Altshuler, RD Ben, pp. 274–298). Washington, DC: Brookings Inst.
- a. Morabito, M. S. (2008). The adoption of police innovation: the role of the political environment. *An International Journal of Police Strategies & Management*, 31(3), 466-484.
  - b. Morabito, M. S. (2008). Understanding community policing as an innovation: Patterns of adoption. *Crime & Delinquency*, 56(4), 564-587.
- Mullen, K. L. (1996). The computerization of law enforcement: a diffusion of innovation study (Doctoral dissertation, University At Albany, State University of New York).
- Office québécois de la langue française (2007). *Grand dictionnaire terminologique : fiche terminologique de « technologies de l'information »*. Récupéré le 22 novembre, 2014, de [http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id\\_Fiche=8875723](http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8875723)
- Oliver, W. M. (2006). The fourth era of policing: Homeland security. *International Review of Law Computers & Technology*, 20(1-2), 49-62.
- Police Provinciale de l'Ontario – PPO (2014). *Ce que nous faisons - Soutien aux enquêtes*. Récupéré le 1<sup>er</sup> septembre, 2014, de <http://www.opp.ca/ecms/index.php?id=251>
- Pratt, Travis C. & al. (2010). *Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory*. *Journal of Research in Crime and Delinquency*, 47, 267.
- Quick, D., & Choo, K. K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*.
- Randol, B. M. (2013). *Modeling a decade of organizational change in municipal police departments: A longitudinal analysis of technical, administrative, and programmatic innovations*. Washington State University, Department of Criminal Justice and Criminology. (Doctoral dissertation).
- Ratcliffe, J. H. (2012). *Intelligence-led policing*. Routledge.
- Rice, R. E. (2009). Diffusion of innovations: Theoretical extensions. In *SAGE handbook of media effects*. Edited by Robin L. Nabi and Mary Beth Oliver, 489–503. Thousand Oaks, CA: SAGE.
- Rogers, E. M. (2003). *Diffusion of innovations*. (5th ed.). New York: Free Press.
- Ryan, B., & Gross, N. C. (1943). The diffusion of hybrid seed corn in two Iowa communities. *Rural sociology*, 8(1), 15-24.
- Schweitzer, N. J., & Saks, M. J. (2007). The CSI effect: Popular fiction about forensic science affects the public's expectations about real forensic science. *Jurimetrics*, 357-364.
- Seaskate Inc. for the National Institute of Justice, The National Committee on Criminal Justice Technology. (1998). *The evolution and development of police technology*.

- Sécurité publique Québec (2014). *Services de police*. Récupéré le 1<sup>er</sup> septembre, 2014, de <http://www.securitepublique.gouv.qc.ca/police/police-quebec/services-police.html>
- Soullière, N. (1999). *Police and technology: Historical review and current status*. (Canadian Police College, Ottawa, Canada).
- Shayo, C. (2009). Information technology adoption. In *Encyclopedia of Library and Information Sciences* (3 ed., pp. 2653-2665).
- Skogan, W. G., & Hartnett, S. M. (2005) The Diffusion of Information Technology. *Policing, Police Practice and Research: An International Journal*, 6(5), 401-417.
- Sonis, M. (2009). Innovation diffusion theory: 100 years of development. In *Tool Kits in Regional Science* (pp. 243-271). Springer Berlin Heidelberg.
- Sureté du Québec – SQ (2014). *Cybercriminalité – Notre Expertise*. Récupéré le 1<sup>er</sup> septembre, 2014, de <http://www.sq.gouv.qc.ca/cybercriminalite/notre-expertise/expertise-cybercriminalite.jsp>
- a. Statistique Canada (2010). Utilisation d'Internet par les individus, selon la préoccupation de la protection des renseignements personnels sur Internet et l'âge. Récupéré le 23 août 2014, de <http://www.statcan.gc.ca/tables-tableaux/sum-som/l02/cst01/comm31a-fra.htm>
- b. Statistique Canada (2010). Utilisation d'Internet par les individus, commerce électronique, commandes domestiques et à l'étranger par les Canadiens. Récupéré le 23 août 2014 de <http://www.statcan.gc.ca/tables-tableaux/sum-som/l02/cst01/comm23-fra.htm>
- Touret, D. (1999). Gabriel (de) Tarde (1843-1904) - Le juriste sociologue. Récupéré le 23 août 2014, de <http://www.denistouret.fr/ideologues/Tarde.html>
- Turnbull, B., Taylor, R. & Blundell, B. (2009). The Anatomy of Electronic Evidence – Quantitative Analysis of Police E-Crime Data. *International Conference on Availability, Reliability and Security 2009*, 143-149.
- Vancouver Police Department – VPD (2014). *Forensic Services Section*. Récupéré le 1<sup>er</sup> septembre, 2014, <http://vancouver.ca/police/organization/investigation/investigative-support-services/forensic-services/index.html>
- Van de Ven, A. H., & Rogers, E. M. (1988). Innovations and Organizations Critical Perspectives. *Communication research*, 15(5), 632-651.
- Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.
- Walter, C. (2005). Kryder's law. *Scientific American*, 293(2), 32-33.
- Weisburd, D., & Braga, A. A. (Eds.). (2006). *Police innovation: Contrasting perspectives*. Cambridge University Press.
- Weisburd, D., Mastrofski, S. D., McNally, A., Greenspan, R., & Willis, J. J. (2003). Reforming to Preserve: Compstat and Strategic Problem Solving in American Policing. *Criminology & Public Policy*, 2(3), 421-456.

- Weiss, A. (1997). The communication of innovation in American policing. *Policing: An International Journal of Police Strategies & Management*, 20(2), 292-310.
- Willis, J. J., & Mastrofski, S. D. (2011). Innovations in policing: Meanings, structures, and processes. *Annual Review of Law and Social Science*, 7, 309-334.
- Willis, J. J., Mastrofski, S. D., & Weisburd, D. (2007). Making sense of Compstat: A theory-based analysis of organizational change in three police departments. *Law & Society Review*, 41(1), 147-188.
- Willison, R. (2004). *Understanding the Offender/Environment Dynamic for Computer Crimes: Assessing the Feasibility of Applying Criminological Theory to the IS Security Context*. Proceedings of the 37th Hawaii International Conference on System Sciences.
- Yar, M. (2005). *The Novelty of 'Cybercrime' : An Assessment in Light of Routine Activity*. *European Journal of Criminology*, 2, 407.
- Yesilyurt, H. (2011). *The Response of American Police Agencies to Digital Evidence* (Doctoral dissertation, University of Central Florida Orlando, Florida).
- Zaltman, G., Duncan, R., & Holbek, J. (1973). *Innovations and organizations*. New York: Wiley.
- Zhao, J. (1996, January). Why police organizations change: A study of community-oriented policing. Washington, DC: Police Executive Research Forum.



## Annexe 1 - Présentation détaillée des variables de la base de données

Nom de la variable	Description et type de variable	Nature de la variable, précisions et justifications (s'il y a lieu)
No_ref	Numéro de référence de la demande d'assistance	À titre indicatif seulement.
Date_rap_inc	Date du rapport d'incident (ex. : 2002/10/12) - <i>Variable continue</i>	Cette date coïncide avec la date d'ouverture du dossier de police.
Date_reception	Date de réception de la demande d'assistance (ex. : 2004/01/22) - <i>Variable continue</i>	
Annee	Année du rapport d'incident (ex. : « 2005 ») - <i>Variable continue</i>	
Mois	Mois du rapport d'incident (ex. : « Janvier »)	
Jour	Jour du rapport d'incident (ex. : « 12 »)	
Time_scale	Variable mois du rapport d'incident en continue pour l'ensemble de l'échantillon de 2004 à 2011 (ex. : 28) - <i>Variable continue</i>	Cette variable a été créée afin d'avoir une échelle temporelle viable pour l'ensemble de l'échantillon. Avec cette variable il est donc possible d'effectuer des analyses sur une base mensuelle pour les sept années couvertes par les demandes de services disponibles.
Type_incident	Type d'incident (Drogue, Fraude, Piratage, etc.) - <i>Variable catégorielle</i> - <i>Construite à partir de la variable « Incident_string »</i>	Catégories construites selon les thèmes revenant le plus souvent dans la variable « Incident_string » : <ol style="list-style-type: none"> <li>1. Fraude (fabrication et utilisation de faux, contrefaçon, etc.)</li> <li>2. Stupéfiants (production, vente, importation, exportation, etc.)</li> <li>3. Crime organisé (blanchiment d'argent, complot, produits de la criminalité)</li> <li>4. Télécommunication (ex. : vol de signaux satellites)</li> <li>5. Droit d'auteur (copies de films, marques de commerces, etc.)</li> <li>6. Sécurité de l'état (terrorisme, immigration illégale, etc.)</li> <li>7. Pornographie juvénile</li> <li>8. Homicide et menaces de mort</li> <li>9. Piratage et crimes informatiques</li> <li>10. Assistance technique (copies, perquisition, etc.)</li> <li>11. Autres</li> </ol>
Incident_string	Description, en texte, de la nature de l'incident	Données qualitatives.
Demandeur	Département du demandeur (entité qui a effectué une demande de service à l'Unité) - <i>Variable catégorielle</i>	<ol style="list-style-type: none"> <li>1. Criminalité organisée</li> <li>2. Criminalité financière</li> <li>3. Sécurité étatique</li> <li>4. Renseignements criminels</li> <li>5. Services de protection</li> <li>6. Support aux opérations</li> <li>7. Autre service de police</li> </ol>

Nom de la variable	Description et type de variable	Nature de la variable, précisions et justifications (s'il y a lieu)
Type_demandeur	Type de demandeur - <i>Variable catégorielle</i>	1. Demande interne 2. Demande interne (type 2) 3. Autre service de police 4. Ministère ou Gouvernement 5. Autre
To_do	Type de service effectué - <i>Variable catégorielle</i>	1. Analyse 2. Assistance lors de la perquisition 3. Extraction de données 4. Assistance technique
Demandeur_string	Description, en texte, du service du demandeur	Données qualitatives.
Warrant	Est-ce que le ou les appareils électroniques à analyser ont été obtenus suite à un mandat de perquisition ? - <i>Variable dichotomique (oui / non)</i>	
Charge	Est-ce que des accusations criminelles sont déposées au moment de la demande d'assistance ? - <i>Variable dichotomique (oui / non)</i>	
Art_CCR	Description en texte de l'article du Code criminel lorsque des charges ont déjà été déposées	Données qualitatives.
CPU	Nombre d'ordinateurs à traiter - <i>Variable continue</i>	
Laptop	Nombre d'ordinateurs portables ( <i>Laptop</i> ) à traiter - <i>Variable continue</i>	
Cellphone	Nombre de téléphones cellulaires à traiter - <i>Variable continue</i>	
Smartphone	Nombre de téléphones intelligents ( <i>Blackberry, iPhone, etc.</i> ) à traiter - <i>Variable continue</i>	
PDA	Nombre d'agendas électroniques personnels ( <i>PDA</i> ) à traiter - <i>Variable continue</i>	
HD	Nombre de disques durs ( <i>HD</i> ) à traiter - <i>Variable continue</i>	
Disquette	Nombre de disquettes à traiter - <i>Variable continue</i>	

Nom de la variable	Description et type de variable	Nature de la variable, précisions et justifications (s'il y a lieu)
CD	Nombre de disques compacts (CD) à traiter - <i>Variable continue</i>	
DVD	Nombre de DVD à traiter - <i>Variable continue</i>	
USB_Key	Nombre de périphériques de stockage (clé USB, carte mémoire, lecteur MP3, etc.) à traiter - <i>Variable continue</i>	
Divers1	Nombre de pagettes à traiter	
Divers2	Nombre de « <i>Skimmer</i> » à traiter	Un « <i>Skimmer</i> » est un appareil servant à lire les cartes magnétiques afin d'en enregistrer le contenu pour cloner des cartes de crédit / débit.
Divers3	Nombre consoles de jeux à traiter	
Mat_total	Nombre total d'appareils électroniques à traiter - <i>Variable continue</i>	Variable faisant la somme de tous les appareils électroniques à traiter indépendamment de leur nature.
Mat_saisi	La demande concerne-t-elle des appareils électroniques à traiter ? - <i>Variable dichotomique (oui / non)</i>	Suite à l'examen de la variable [Mat_Total] il appert que le nombre total d'appareils à traiter est dans la majorité des cas « 0 » ou « 1 ». La variable a donc été « dichotomisée » afin de faciliter les analyses ultérieures.
Notes	Notes sur l'enquête, sur les analyses effectuées, etc.	Données qualitatives concernant l'enquête.
Dossier	Numéro du dossier sur PROS.	À titre indicatif seulement. Relatif au numéro de dossier policier.
Date_diff	Différence en jours entre la date de réception de la demande [Date_reception] et la date de l'incident [Date_rap_inc] - <i>Variable continue</i>	Cette variable a été calculée en soustrayant la date de réception de la demande de service à la date déclarée de l'incident. Le résultat, en jour, donne le délai qui s'est écoulé entre l'incident et la demande de service.
Date_diff_fix	Variable [Date_diff] recodée - <i>Variable continue</i>	Suite à l'analyse de la variable [Date_diff], certains résultats étaient négatifs; ce qui voudrait dire que la demande est effectuée avant l'incident. Or, ceci étant impossible, ce phénomène est dû à l'absence de plusieurs dates manquantes sur les formulaires. Toutes les données négatives ont donc été traitées comme des données manquantes. Également, les données supérieures à 1000 jours ont été traitées en tant que données éloignées et ont donc été ramenées à 1000. Ceci évite de gonfler la moyenne artificiellement.
Date_diff_ord	Variable [Date_diff_fix] recodée - <i>Variable ordinale</i>	Variable catégorisant de façon ordinale le délai entre la demande de service et le rapport d'incident. Les catégories sont les suivantes : 1. 0 jour 2. De 1 à 7 jours 3. De 8 à 14 jours 4. De 15 à 21 jours 5. De 22 à 28 jours 6. De 29 à 35 jours 7. De 36 à 70 jours 8. De 71 à 140 jours 9. 141 jours et plus

Nom de la variable	Description et type de variable	Nature de la variable, précisions et justifications (s'il y a lieu)
Incident_corr	Variable [Type_incident] recodée - <i>Variable catégorielle</i>	Variable recodée afin d'inclure les catégories « Télécommunication », « Pornographie juvénile » et « Piratage et crimes informatiques » dans la catégorie « Autres ». De plus, la catégorie « Assistance technique » a été déclarée manquante afin de correspondre uniquement aux types de crimes. Variable utilisée afin de simplifier les analyses bivariées. Ceci a notamment permis d'effectuer un tableau croisé sans briser les postulats d'utilisation.
Autres_peri	Addition des variables [PDA], [Divers1], [Divers2] et [Divers3] - <i>Variable continue</i>	Cette variable constitue une catégorie « autres » périphériques.
To_do_dicho	Variable [To_do] dichotomisée Cette variable divise les demandes de services en deux principales catégories : 1) les demandes concernant une expertise et 2) les demandes d'assistance - <i>Variable dichotomique</i>	Les catégories « Analyse » et « Extraction de données » de la variable [To_do] ont été regroupées dans un premier groupe (expertise) et les catégories « Assistance lors de la perquisition » et « Assistance technique » dans un second (assistance).
Demandeur_corr	Variable [Demandeur] recodée - <i>Variable catégorielle</i>	Variable recodée afin d'inclure les catégories « Renseignements criminels », « Services de protection » et « Support aux opérations » dans « Autre demandeur interne ». Variable utilisée afin de simplifier les analyses bivariées.

## **Annexe 2 – Questionnaire destiné aux membres de l'Unité**

### **Thème 1 – Caractériser le travail de l'Unité**

1. Quels types d'analyses requièrent la plus grande partie de votre temps ?
2. Quel genre de dossier d'enquête constitue la majorité de vos demandes de service ?
3. Qui nécessite le plus souvent votre expertise et pour quelle raison ?
  - a. Le cas échéant, comment les différents demandeurs se distinguent-ils ?
4. Selon vous, quels sont les principaux facteurs influençant les délais de traitement d'une demande de service adressée à votre unité ?
5. Quelle est la charge de travail générée par les opérations ou projets spéciaux ?
6. Est-ce que certaines demandes sont priorisées ?

### **Questions sur les résultats d'analyse obtenus :**

7. Je peux constater une chute d'environ 25% des demandes de service pour les années 2010 et 2011 comparativement à 2009. Comment expliquez-vous ce résultat ?
8. Des programmes de formation, permettant de déléguer une partie des analyses, ont-ils été mis en place afin de réduire votre charge de travail ?
9. En regardant la distribution des demandes de façon mensuelle je me rends compte que certains mois, notamment février, mars et avril, sont beaucoup plus achalandés que d'autres. Comment expliquez-vous ce phénomène ?

## **Thème 2 – Les technologies et la preuve numérique**

10. Selon vous, est-ce l'évolution des technologies à un impact sur votre travail ? Si oui, de quelle manière ?
  - a. La quantité de pièces à traiter a-t-elle augmenté ?
  - b. La nature des pièces a-t-elle changé ?
  - c. La quantité de données à analyser a-t-elle augmenté ?
  
11. Quelle est l'importance de la preuve numérique pour les enquêtes policières en 2014 ?
  - a. En quoi cette preuve est-elle essentielle au dépôt d'accusations criminelles ?
  - b. Cette preuve est-elle plus ou moins importante selon le type de crime ?
  - c. Le volume de cette preuve augmente-t-il avec les années ?

## **Thème 3 – L'expertise de l'Unité**

12. Combien de temps est-il nécessaire pour former un analyste judiciaire informatique ?
  
13. Quelle est la perception des autres départements et enquêteurs face à votre unité ?
  
14. Comment voyez-vous le futur des unités spécialisées en criminalité informatique ?
  
15. Selon vous, il y a-t-il une complexification des analyses judiciaires informatiques ?

### **Annexe 3 – Questionnaire pour l’inspecteur d’une agence gouvernementale**

1. Quelles sont les raisons qui ont poussé votre agence à développer une expertise ou un programme spécialisé en analyse judiciaire informatique ?
  - a. Ce programme a été initié en quelle année ?
  
2. Quelles sont vos fonctions et votre rôle au sein de votre organisation ?
  
3. Avez-vous déjà une expertise en la matière ?
  
4. Votre agence souhaite-t-elle continuer à développer cette expertise ?
  
5. Selon vous, quels sont les principaux défis liés à la création d’un tel programme ?
  
6. Quels sont les plus grands défis personnels liés à l’occupation de cette nouvelle fonction ?