CANADIAN POLICE KNOWLEDGE NETWORK

RÉSEAU CANADIEN DU SAVOIR POLICIER

CADRE DE GESTION AXÉ SUR LES COMPÉTENCES POUR LES COMPÉTENCES NUMÉRIQUES DES POLICIERS CANADIENS

Une composante du projet *Formation en cybercriminalité et développement des compétences numériques pour les forces de l'ordre canadiennes* du Réseau canadien du savoir policier

Paul Beesley, M.Sc. M.O.M.
Consultante en projets

Juin 2021

La formation sur la cybercriminalité et le développement des compétences numériques pour le projet d'application de la loi au Canada est financé, en partie, par

Public Safety Canada | Sécurité publique Canada

Table des matières

LISTE DES TABLEAUX

LISTE DES FIGURES

Résumé

À l'aide du cadre de gestion axé sur les compétences du Réseau canadien du savoir policier, ce projet s'est efforcé d'identifier les compétences numériques des membres des forces de l'ordre canadiennes en ce qui concerne la cybercriminalité et les preuves numériques. De plus, le rapport identifie les formations qui sont actuellement disponibles et qui complètent les profils de compétences et fait des recommandations pour le développement de la formation et le renforcement des capacités.

Une revue de la littérature a identifié les pratiques mondiales actuelles en matière de compétences numériques. Une série de groupes de discussion impliquant plus de cinquante chefs de police, experts en cybercriminalité et professionels en cybercriminalité ont considéré le cadre de compétences numériques établi par le Groupe européen de formation et d'enseignement sur la cybercriminalité comme un modèle potentiel pour le Canada. Finalement, une version canadienne d'un dictionnaire numérique de compétences et de profils de compétences a été créée.

Le cadre canadien définit dix compétences numériques composées chacune de cinq niveaux, notamment :

1. Compétences numériques et l'internet
2. Cyber-hygiène et cybersécurité
3. Sensibilisation à la cybercriminalité, prévention et assistance aux victimes
4. Renseignement de source ouverte et collecte de preuves
5. Cyber légalités
6. Analyse des cyberdonnées et du renseignement
7. Crypto-monnaie et Blockchain
8. Programmation et scripts
9. La criminalistique numérique
10. La criminalistique du réseau

De plus, le cadre identifie dix rôles liés à la cybercriminalité dans les organismes d'application de la loi canadien :

1. Tous les membres du service de police (avec accès aux réseaux informatiques et/ou aux systèmes de courriel)
2. Premiers intervenants
3. Fonctions générales des enquêteurs/ détectives
4. Enquêteurs intermédiaires (liés à la cybersécurité)
5. Professionnels de la sensibilisation/ de la liaison avec les victimes
6. Enquêteurs en ligne
7. Analystes de la cybercriminalité
8. Examinateurs criminalistiques numériques
9. Enquêteurs sur la cybercriminalité
10. Cybergestionnaires et dirigeants

Comme indiqué dans le tableau 1, les profils de compétences, qui correspondent aux niveaux de compétence avec les divers rôles, complètent l'aspect compétence du projet.

Tableau 1. Matrice de profils de compétences numériques pour les forces de l'ordre canadiennes

	Compétences numérique et l'Internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et script	La criminalistique numérique	La criminalistique du réseau (Cloud/nuage)
Tous les membres	1	1								
Premiers intervenants*	1	2	2	1	1	1	1		2	1
Détectives généraux*	2	2	2	2	2	2	2		2	2
Enquêteurs intermédiaires*	3	3	3	2	2	2	2	3	3	3
Sensibilisation/liaison avec les victimes*	2	2	4	2	2	1	2		2	2
Enquêteurs en ligne*	4	3	2	4	3	3	3	3	2	3
Analystes de la cybercriminalité*	3	3	2	3	2	4	4	4	2	3
Examinateurs criminalistique numériques*	4	4	2	3	3	3	4	3	5	5
Enquêteurs sur la cybercriminalité*	4	3	3	3	4	3	4	2	2	2
Cyber gestionnaires et dirigeants*	3	3	3	2	4	2	2		2	2

Un sondage sur la formation, qui a suivi l'élaboration des profils de compétences, identifie une formation complémentaire et a informé une analyse des lacunes en formation. L'analyse des lacunes en formation a déterminé que la formation pour des rôles spécialisés tels que l'examinateur criminalistique numérique, l'enquêteur en cybercriminalité ou l'analyste en cybercriminalité soit bien établie sous la direction du Collège canadien de police - Institut d'apprentissage technique sur la criminalité, il existe des lacunes importantes dans la formation requise pour les rôles généralistes non-numériques tels que les premiers intervenants et les enquêteurs/détectives aux fonctions générales. L'analyse des lacunes a également reconnu la nécessité de développer une formation supplémentaire dans les domaines de l'assistance aux cyber-victimes, de la cyber-hygiène aux niveaux inférieurs, de la cyber légalité, des crypto-monnaies, de la criminalistique numérique aux niveaux inférieurs et de la criminalistique des réseaux aux niveaux inférieurs.

RECOMMANDATIONS

Il existe neuf recommandations de « prochaine étape » pour le développement des capacités des compétences numériques :

1. Renforcer les capacités de formation pour les cyber-rôles non spécialisés.
2. Créer une formation en cyber-hygiène facilement accessible avec un programme basé sur le profil de compétences Tous les membres du service de police.
3. Reconstruire le cours de niveau 1 sur les enquêtes sur la cybercriminalité du RCSP avec un programme basé sur le profil de compétences des premiers intervenants.
4. Créer une cyberformation facilement accessible avec un programme basé sur le profil de compétences des enquêteurs/détectives des fonctions générales.
5. Travailler avec des partenaires pour créer des modules d'aide aux victimes avec des programmes basés sur les niveaux de compétence 1 et 2.
6. Travailler avec des partenaires pour créer ou identifier une formation en crypto-monnaie et en blockchain pour les forces de l'ordre avec des programmes de compétences de niveaux 1, 2 et 3.
7. Continuer d'assurer la liaison avec le Comité des cybercrimes de l'ACCP et le Comité des services nationaux de police sur la cybercriminalité pour la révision, l'évaluation et la validation annuels du dictionnaire et des profils de compétences numériques.
8. Poursuivre l'évaluation des cours et de la cyberformation pour s'assurer qu'ils contiennent des programmes d'études valides fondés sur les compétences.
9. Envisager des partenariats avec des établissements d'enseignement publics ou des prestataires du secteur privé actifs dans le domaine de la cyber-éducation.

1. Aperçu du projet

Au début de 2021, le Réseau canadien du savoir policier (RCSP) a lancé une initiative visant à améliorer la formation liée aux compétences numériques pour les forces de l'ordre canadiennes. Financé en partie par le Programme de coopération en matière de cybersécurité de Sécurité publique Canada, le projet *Formation en cybercriminalité et développement des compétences numériques pour les forces de l'ordre canadiennes* a engagé la communauté policière canadienne à appliquer une approche fondée sur les compétences pour :

1. Élaborer un dictionnaire de compétences numérique pour divers rôles et grades au sein des organismes d'application de la loi canadiens; et
2. Mettre à jour/développer une formation bilingue pour améliorer la capacité du personnel de première ligne à répondre aux incidents de cybercriminalité.

1.1. L'approche du cadre de gestion par compétences

Le cadre de gestion basé sur les compétences se concentre sur la gestion des ressources humaines en définissant les compétences, les connaissances et les attributs qui contribuent à une performance efficace dans un rôle spécifique. Dans un contexte policier canadien, le cadre de gestion basé sur les compétences classe les compétences comportementales, techniques et de leadership/gestion associées aux rôles de service général, d'enquête et de commandement. (Canadian Police Knowledge Network, 2020, p. 1; Greenwood, 2020).

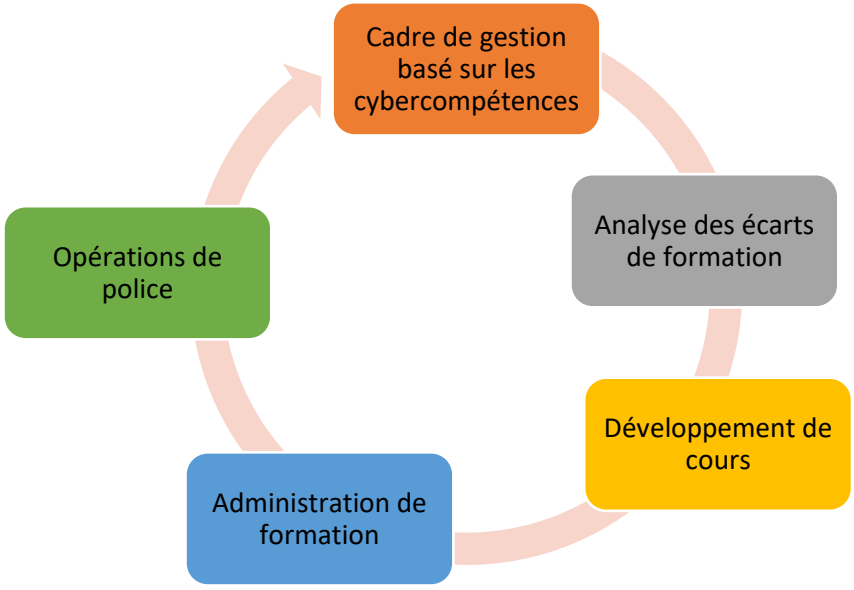
Le développement d'un cadre de gestion par compétences mature joue un rôle essentiel pour :

- répondre à l'attente du public selon laquelle, quelle que soit la province ou la communauté, tous les policiers soient formés à un niveau constant et approprié de connaissances et de compétences;
- permettre aux services de police d'utiliser les ressources de manière plus efficace;
- identifier les écarts ou les lacunes dans le rendement des services de police et fournir des points de repère grâce auxquels les services de police peuvent renforcer leurs capacités, améliorer la prise de décision et s'adapter stratégiquement aux besoins particuliers de leurs communautés;
- veiller à ce que les agents aient les compétences et les connaissances nécessaires pour s'acquitter efficacement de leurs tâches, y compris dans les situations difficiles qui dépassent souvent les limites traditionnelles du travail policier;
- apporter des améliorations mesurables des performances ;
- diminuer les risques organisationnels et des agents, en particulier dans les environnements à haut risque ;
- améliorer le moral et le bien-être des employés (c.-à-d. augmenter la confiance, réduire le stress au travail et fournir une voie claire pour l'avancement professionnel);
- renforcer les résultats généraux en matière de police et de sécurité publique;
- réduire le dédoublement des efforts (et des coûts) entre les différents services de police qui conçoivent et utilisent des modèles de gestion axée sur les compétences;

- améliorer la transparence, la responsabilisation et la confiance du public dans les services de police; et
- identifier les opportunités de partenariat avec des organisations sociales et de santé pour améliorer l'approche globale de la sécurité et du bien-être de la communauté (Canadian Police Knowledge Network, 2020, p. 2).

Comme l'illustre la figure 1, le cadre de compétences numériques basé sur les rôles permet une analyse plus approfondie pour identifier les lacunes en matière de formation, répertorier la formation existante et, finalement, mener à l'élaboration et à la prestation de nouvelles formations qui assurent que les organismes d'application de la loi canadiens sont mieux placés pour faire face aux changements dans le paysage numérique et cybernétique.

Figure 1. Cadre de gestion basé sur les cybercompétences



1.2. Méthodologie

Ce projet comprenait plusieurs phases pour créer un dictionnaire de compétences et faire des recommandations concernant le développement et/ou la mise à niveau de la formation existante.

Phase 1: Examen des pratiques mondiales

Une revue de la littérature ciblée a été entreprise pour fournir une base pour le développement des compétences et pour créer une compréhension des meilleures pratiques mondiales. Une revue de la littérature ciblée a cherché à définir le terme « cybercriminalité » et à découvrir les compétences numériques existantes pour les forces de l'ordre.

Phase 2: Consultation

Basé sur la revue de la littérature, un texte de discussion qui a consolidé les meilleures pratiques mondiales a été rédigé pour encadrer les conversations des groupes de discussion.

Le plan initial prévoyait réunir divers experts en cybercriminalité et enquêteurs sur la cybercriminalité pour un atelier de plusieurs jours afin de définir et de développer un dictionnaire de compétences numériques et des profils de compétences numériques pour les forces de l'ordre canadiennes. La pandémie mondiale et les restrictions de voyage qui en ont résulté ont empêché l'atelier d'avoir lieu. À sa place, le RCSP a organisé une série de groupes de discussion virtuels avec des groupes de gouvernance et des praticiens de divers organismes d'application de la loi.

À la suite des consultations, une feuille de route existait pour l'élaboration d'un dictionnaire de compétences numériques et de profils de compétences numériques.

Phase 3: Création d'un dictionnaire de compétences et de profils de compétences

La phase de consultation a fourni le contexte canadien aux meilleures pratiques mondiales et a identifié à la fois les cyber-acteurs de l'application de la loi et les compétences qui n'avaient pas été identifiées auparavant.

L'information et les connaissances accumulées au cours de la revue de la littérature, de la phase de consultation et de la phase de développement ont été combinées pour créer une ébauche de compétences numériques pour les forces de l'ordre canadiennes. Cela comprenait un dictionnaire de compétences décrivant les compétences essentielles à travers les niveaux 1 à 5 et des profils de compétences qui identifiaient les niveaux de compétence recommandés pour les différents cyber-acteurs chargés de l'application de la loi.

Phase 4: Enquête sur la formation et analyse des écarts

Une fois les profils de compétences terminés, un sondage sur la formation facilement disponible et accessible a été entreprise. Bien qu'il ne s'agisse pas d'un inventaire exhaustif de la formation disponible, le sondage donne de l'information sur les lacunes potentielles dans le paysage de la formation et identifie les opportunités de création de nouveaux programmes d'études ou des programmes d'études améliorés basés sur les compétences.

2. Bilan des pratiques mondiales

2.1 Crime numérique, cybercriminalité, ou tout simplement crime?

Lorsque l'on considère les compétences numériques, il est important de comprendre le contexte de leur utilisation. Il peut être naturel de considérer les compétences numériques comme étant directement liées aux compétences dont les policiers ont besoin pour lutter contre la cybercriminalité. Cependant, la définition générale de la cybercriminalité, associée à la croissance exponentielle des preuves numériques, pourrait amener à repenser la portée des compétences numériques.

Au Canada, il n'y a pas de définition légale ou unique de ce qui constitue un cybercrime. La plupart des organismes d'application de la loi du pays utilisent une définition élaborée par le Collège canadien de police et adoptée par le Centre canadien de la statistique juridique et le Programme de déclaration uniforme de la criminalité (Mazowita & Vezina, 2014) où la cybercriminalité est définie comme :

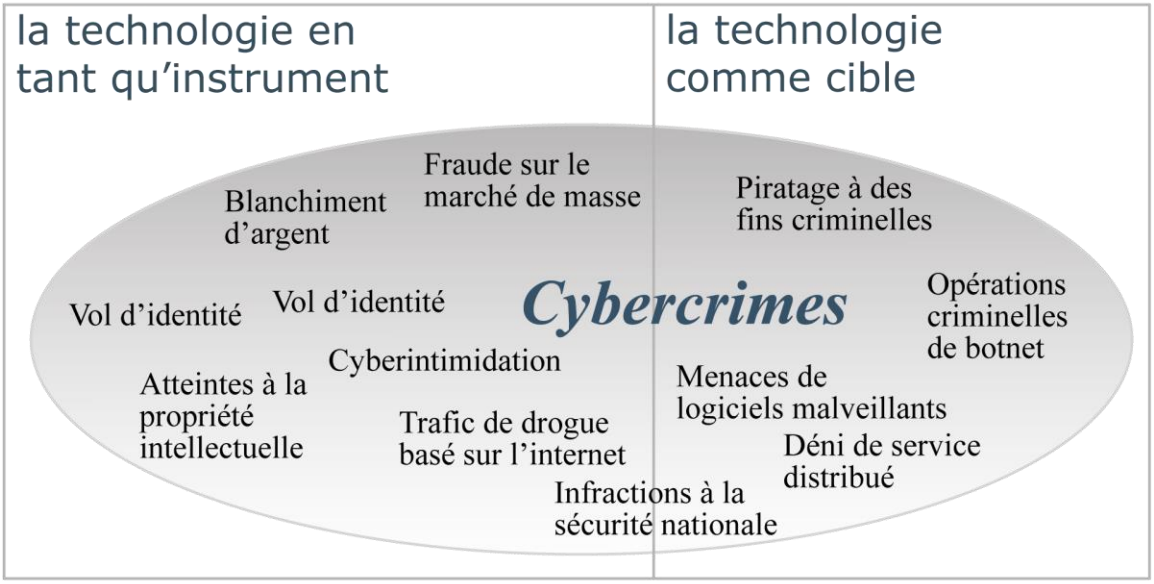
> *« une infraction pénale impliquant un ordinateur comme objet d'un crime ou l'outil utilisé pour commettre une composante matérielle de l'infraction »* (Kowalski, 2002)

Les cybercrimes sont généralement considérés comme ayant deux volets distincts :

1. Les cybercrimes **ciblés par la technologie** sont des infractions où la technologie de l'information, y compris les appareils et les réseaux, est la cible de l'infraction. Les exemples incluent l'utilisation non autorisée d'ordinateurs, les attaques de déni de service et les méfaits liés aux données informatiques.

2. Les infractions de cybercriminalité **utilisant la technologie en tant qu'instrumen**t sont commis à l'aide des technologies de l'information. Ceux-ci sont souvent considérés comme des « *crimes traditionnels* », et les exemples incluent le harcèlement criminel via les médias sociaux ou les SMS, la distribution et la vente de pornographie juvénile et le vol d'identité à l'aide des technologies de l'information ou d'Internet. (Ontario Provincial Police (2), 2016; Royal Canadian Mounted Police, 2021; Royal Canadian Mounted Police, 2015)

Figure 2. Catégories de cyberciminalité



Source: (Royal Canadian Mounted Police, 2021)

Bien qu'il y ait des nuances, il semble y avoir une cohérence dans l'approche à multiples facettes pour définir la cybercriminalité dans le monde.

La Convention du Conseil de l'Europe sur la cybercriminalité, également connue sous le nom de Convention de Budapest, définit la cybercriminalité comme un large éventail d'activités, y compris l'interception et l'interférence illégales de données, les infractions informatiques telles que la fraude et les infractions liées au contenu telles que la création ou distribution de pornographie juvénile[1] (Council of Europe, 2001). Europol différencie la cybercriminalité en délits cyberdépendants et délits cybernétiques, où les technologies de l'information et de la communication sont la cible dans le premier cas et où elles font partie du *modus operandi* du délinquant dans le dernier. (Europol, 2018, p. 15)

[1]. Le Canada est l'un des soixante-cinq signataires de la Convention de Budapest.

La nature diversifiée de la définition de la cybercriminalité est illustrée par l'expérience canadienne. Lors de la compilation des données sur les infractions liées à la cybersécurité, Statistique Canada conclut que,

> *« La violation de la cybercriminalité représente la violation pénale spécifique dans le cadre d'un incident au cours duquel un ordinateur ou l'Internet a été la cible du crime, ou l'instrument utilisé pour commettre le crime. »* (Statistics Canada, 2021)

Le tableau 2 montre que la plupart des infractions liées à la cybersécurité signalées à Statistique Canada sont généralement considérées comme des crimes dans lesquels la technologie est un instrument ou une partie du *modus operandi* de l'infraction; un bon nombre de ces incidents classés comme des cybercrimes sont généralement considérés comme des crimes traditionnels.

Tableau 2. Cybercriminalité déclarée par la police selon l'infraction reliée à la cybercriminalité, Canada (certains services de police)

Infraction liée à la cybersécurité	2015	2016	2017	2018	2019
Total des infractions	**17 887**	**23 996**	**27 829**	**33 893**	**44 136**
Homicide	0	0	1	1	3
Incitation à des contacts sexuels	109	77	101	104	118
Exploitation sexuelle	15	14	17	21	27
Leurre d'un enfant au moyen d'un ordinateur	850	1108	1132	1280	1450
Voyeurisme	67	58	80	77	88
Distribution non consensuelle d'images intimes	97	295	516	569	718
Extorsion	709	797	893	1863	1410
Harcèlement criminel	1001	1058	1291	1396	1715
Communications indécentes ou harcelantes	1202	1655	2302	2708	4933
Menaces	1139	1356	1674	2224	3122
Autres infractions avec violence	69	149	195	251	300
Fraude	8429	11 383	13 426	16 641	21 047
Vol d'identité	191	260	280	284	388
Fraude à l'identité	695	828	1082	1369	1920
Méfaits	167	156	166	152	169
Autres infractions non violentes	8	27	66	181	270
Défaut de se conformer à une ordonnance	156	225	318	473	553
Actions indécentes	10	19	23	20	35
Pornographie juvénile	1753	1278	1041	621	1130
Production ou distribution de pornographie juvénile	850	2886	2868	3113	4174
Corruption des moeurs	20	33	28	20	30
Manquement aux conditions de la probation	39	68	74	98	120
Menacer des biens ou des animaux	45	48	51	82	107

Infractions contre la personne et la réputation (Partie VIII, *Code criminel*)	110	89	82	142	118
Autres Code *criminel*	141	95	106	136	161
Autres infractions (infractions provinciales)	15	34	16	67	30

Source: (Statistics Canada, 2021)

Les éléments numériques sont de plus en plus courants dans l'éventail des infractions pénales. Cette expérience n'est pas uniquement canadienne. Par exemple, le bureau du procureur du district de Manhattan a noté que plus d'un quart des inculpations pour crime à Manhattan en 2019 impliquaient une composante numérique (Manhattan District Attorney's Office, 2021). Alors que la Commission européenne a estimé qu'au cours de la même période, 85 % des enquêtes pénales incluaient des preuves électroniques. (European Commission, 2019)

Statistique Canada rapporte que 91,3 % des Canadiens utilisent régulièrement l'Internet, (Statistics Canada, 2021; Statistics Canada, 2019) et que plus de 80 % de la population utilise des téléphones intelligents (Statistics Canada, 2021) il est difficile d'imaginer un acte criminel ou ce qu'on appelle le « crime traditionnel » sans potentiel de preuves numériques. Ce sentiment est partagé par la Police provinciale de l'Ontario qui déclare,

> *« Chaque aspect d'une enquête policière est déjà affecté d'une manière ou d'une autre par les technologies numériques, et les modèles traditionnels de traitement des preuves numériques n'ont pas la capacité de gérer les volumes de preuves numériques saisies dans le cadre des enquêtes policières et de les traiter en temps opportun. »* (Ontario Provincial Police (2), 2016, p. 3)

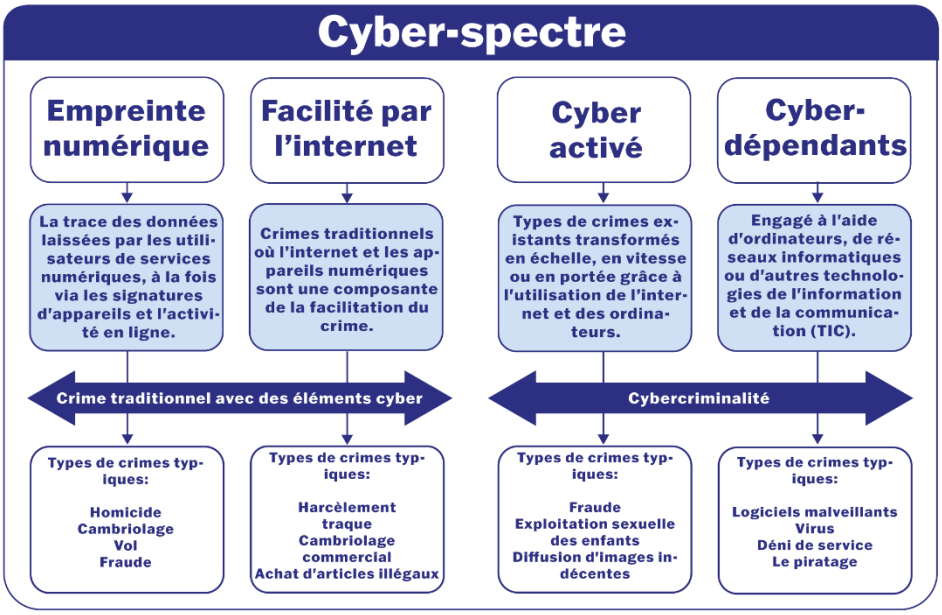
Pour illustrer davantage ce point, la stratégie numérique de la police nationale du Royaume-Uni reconnaît que :

> *« La nature des menaces 'traditionnelles' a évolué avec les plateformes et la technologie numériques. Presque tous les crimes traditionnels ont maintenant un élément numérique, en termes de la façon dont ils ont été commis et de la manière dont nous pouvons enquêter dessus. »* (Association of Police and Crime Commissioners, 2020, p. 4)

On pourrait soutenir que les compétences numériques doivent s'étendre au-delà de la définition générale de la cybercriminalité. Les réalités de la police et de la réponse policière aux éléments cybernétiques et numériques nécessitent une perspective élargie des compétences numériques. Cela nécessite une perspective qui tienne compte de l'empreinte croissante des preuves numériques que les agents de police sont censés comprendre et collecter de manière criminalistique.

Her Majesty's Inspectorate of Constabulary (HMCI) du Royaume-Uni a reconnu que la portée des activités cybernétiques et numériques liées à la police et à la criminalité comporte quatre éléments distincts : Empreinte numérique, faciliter par l'Internet, Cyber activé et Cyber dépendant (Her Majesty's Inspectorate of Constabulary, 2015, p. 7).. Alors que HMCI fait référence à ces composants en utilisant le terme « criminalité numérique », la police du Lincolnshire a affiné et illustré le concept en inventant les composants de la criminalité numérique sous le nom de *cyber-spectre*.

Figure 3. Le spectre de la cybercriminalité



Source: *CITATION Lin21 \l 1033* (Lincolnshire Constabulary, 2021)

Bien que les 'crimes facilités par l'Internet' soient pris en compte dans la partie 'la technologie en tant qu'instrument' de la définition canadienne, la reconnaissance de 'l'empreinte numérique' en tant que composante du spectre cybernétique est un ajout important et nécessaire au renforcement des compétences numériques. Comme l'a observé le Bureau fédéral d'investigation,

> *« Il est impératif que les organismes chargés de l'application des lois à travers le pays, en particulier les premiers intervenants sur une scène de crime, aient une connaissance pratique de la façon d'étudier et de sécuriser les preuves électroniques en plus des preuves physiques auxquelles ils sont plus habitués, comme les empreintes digitales et l'ADN. »* (Federal Bureau of Investigation, 2016)

2.2 La division du travail et les compétences de base

Le Cadre de gestion axé sur les compétences s'efforce de s'assurer que tous les membres canadiens de l'application de la loi sont formés à un niveau uniforme et approprié de connaissances et de compétences. De toute évidence, un membre d'un service de police engagé dans un domaine de spécialité requiert des compétences avancées.

Les compétences avancées reposent sur une base de compétences et de connaissances attendues. Considérons, par exemple, l'identification criminalistique. Tous les policiers reçoivent une formation en identification criminalistique; ils apprennent à conserver les preuves, l'importance de la chaîne de continuité des preuves, etc. Certains policiers reçoivent une formation complémentaire en examen de scène de crime où ils peuvent apprendre à relever les empreintes digitales et à prendre des photographies de scène de crime. Les agents de police chargés de l'identification criminalistique reçoivent une formation hautement spécialisée dans des domaines tels que l'analyse des empreintes digitales, la photographie, la collecte d'ADN et l'analyse des traces de sang. Ils sont considérés comme les experts en techniques d'identification criminalistique.

Il en va de même pour les compétences numériques. La technologie est en train de remodeler le crime, comme le reconnaît le Groupe d'experts sur l'avenir des modèles de police canadiens,

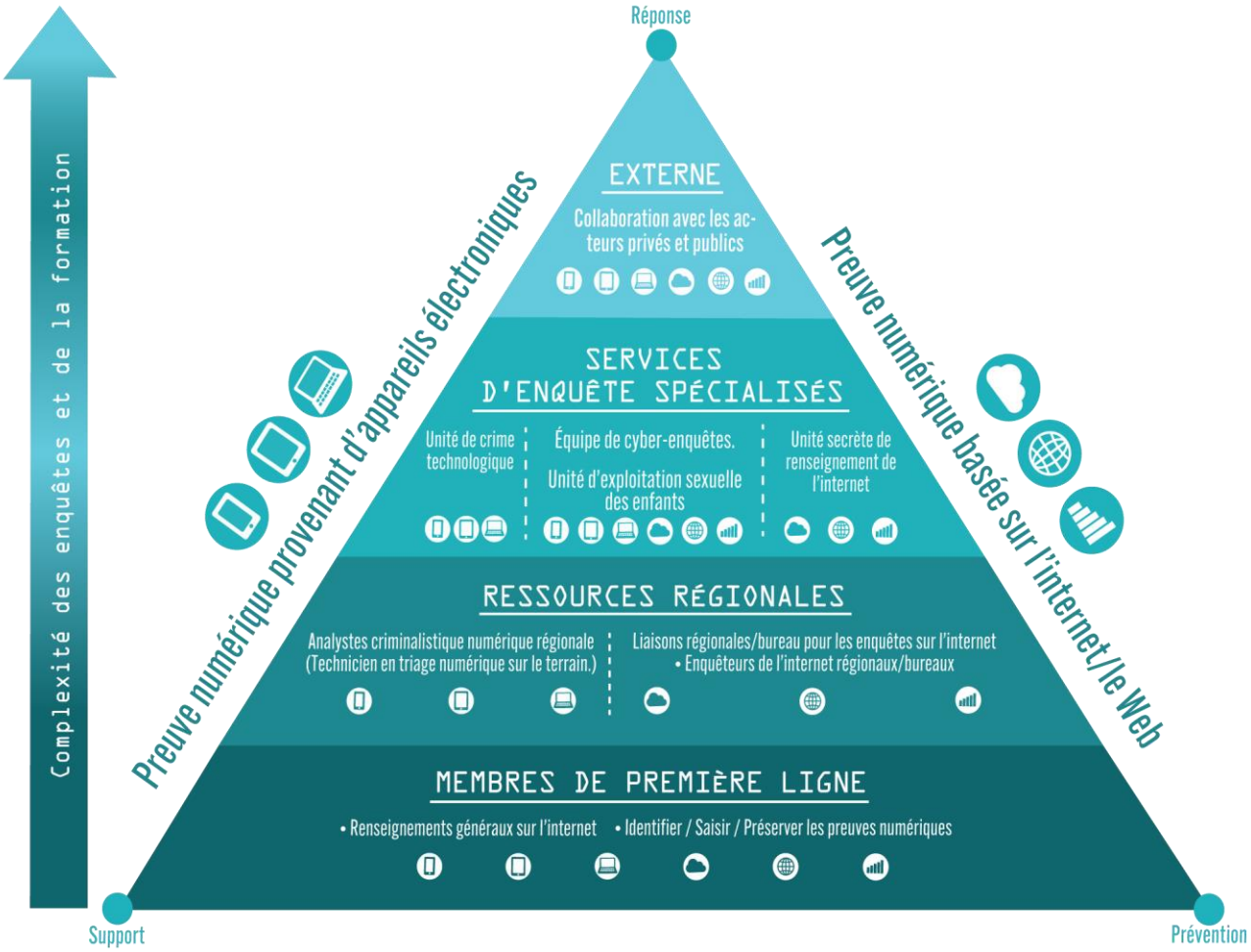
> *« Les services de police répondent de plus en plus à des problèmes sociaux pour lesquels ils ont une formation et des ressources limitées. La demande est influencée par une population plus âgée, plus diversifiée et plus connaissante numériquement. »* (The Expert Panel on the Future of Canadian Policing Models, 2014, p. 14)

Compte tenu de l'omniprésence des preuves numériques et de l'essor des crimes technologiques, il est raisonnable de s'attendre à ce que chaque membre d'un service de police possède un niveau de base de compétences numériques. Bien entendu, les personnes spécialisées dans l'analyse criminalistique numérique ou la criminalité purement technologique doivent acquérir et maintenir des compétences avancées.

Bien que de nombreux organismes canadiens d'application de la loi exploitent des unités spécialisées dans des domaines tels que la criminalistique numérique, l'exploitation sexuelle des enfants et la criminalité liée à la technologie, on estime que moins de 100 personnes sont assignées exclusivement à la cybercriminalité liée à la technologie au Canada (Baron & Le Khac, 2021). En tant que tel, une réponse à plusieurs niveaux aux incidents avec des éléments cyber ou numériques est de plus en plus courante dans les services de police canadiens (Royal Canadian Mounted Police, 2015; Ontario Provincial Police (2), 2016, p. 8; Kowalski, 2002).

Le modèle d'intervention à plusieurs niveaux, comme celui élaboré par la Police provinciale de l'Ontario (PPO) illustré à la figure 4, identifie les rôles que jouent les membres des services de police en cas d'incident impliquant des éléments cyber ou numériques. La base représente les compétences fondamentales requises par tous les membres du service, tandis que le sommet représente les activités et les compétences au-delà de la capacité du service. Au fur et à mesure que l'on monte dans la pyramide, le volume d'événements liés à la cybercriminalité diminue tandis que la complexité des enquêtes augmente. La complexité des enquêtes correspond à des compétences et à une formation avancée.

Figure 4. Compétences numériques hiérarchisées par rôle 1



Source: CITATION Ont16 \l 1033 (Ontario

Un aspect important du modèle de réponse à plusieurs niveaux est qu'il adopte une approche à l'échelle de l'entreprise de l'activité numérique et à la cybersécurité et des compétences corollaires. Il est irréaliste de s'attendre à ce que quelques personnes hautement qualifiées répondent à chaque appel de service ayant un aspect numérique ou cybernétique.

Pour garantir que les services de police peuvent répondre de manière appropriée à la prolifération des preuves numériques et de la cybercriminalité, y compris les crimes à grand volume qui laissent une empreinte numérique ou utilisent la technologie dans le cadre du *modus operandi*, le développement de compétences numériques qui couvrent l'ensemble du spectre cybernétique est essentiel. Plusieurs auteurs ont identifié le besoin de cyber-connaissances dans tous les rôles au sein d'une organisation policière (Robertson, 2019, p. 37).

Le modèle de réponse à plusieurs niveaux implique que les compétences sont requises à l'échelle de l'entreprise, en commençant par les compétences fondamentales communes à tous les membres, et

représentent de nouvelles opportunités de diversification des ressources (The Expert Panel on the Future of Canadian Policing Models, 2014, p. 99) Donner aux premiers intervenants les moyens de faire face aux crimes sur le spectre cybernétique en obtenant des preuves numériques, en menant des enquêtes préliminaires et en faisant des renvois appropriés dans des enquêtes plus complexes, est essentiel pour améliorer la capacité des forces de l'ordre canadiennes dans un monde de plus en plus numérique.

Par exemple, considérons un scénario courant dans lequel un policier est envoyé pour une agression qui a été capturée sur les réseaux sociaux. Si les compétences d'une unité spécialisée étaient nécessaires pour saisir les preuves numériques de tous ces appels, la charge de travail de l'unité spécialisée serait certainement insoutenable et néfaste à l'investigation sur des enquêtes de cybercriminalité pures, plus complexes, plus longues. mais moins courantes pour lesquelles l'unité spécialisée est formée.

Bien qu'il existe peu ou pas de données sur le nombre de premiers intervenants formés au Canada pour faire face aux problèmes de ce qu'on appelle le spectre cybernétique, les recherches suggèrent que le public s'attend à ce que la police réagisse de la même manière à la criminalité en ligne et à la criminalité physique, que les petits services de police sont censés réagir à la criminalité numérique avec le même niveau de service que les grands organismes, et que les services qui traitent efficacement les composantes du spectre cybernétique ont connu une plus grande satisfaction du public (Robertson, 2019, p. 29).

2.3 Quelles compétences sont nécessaires?

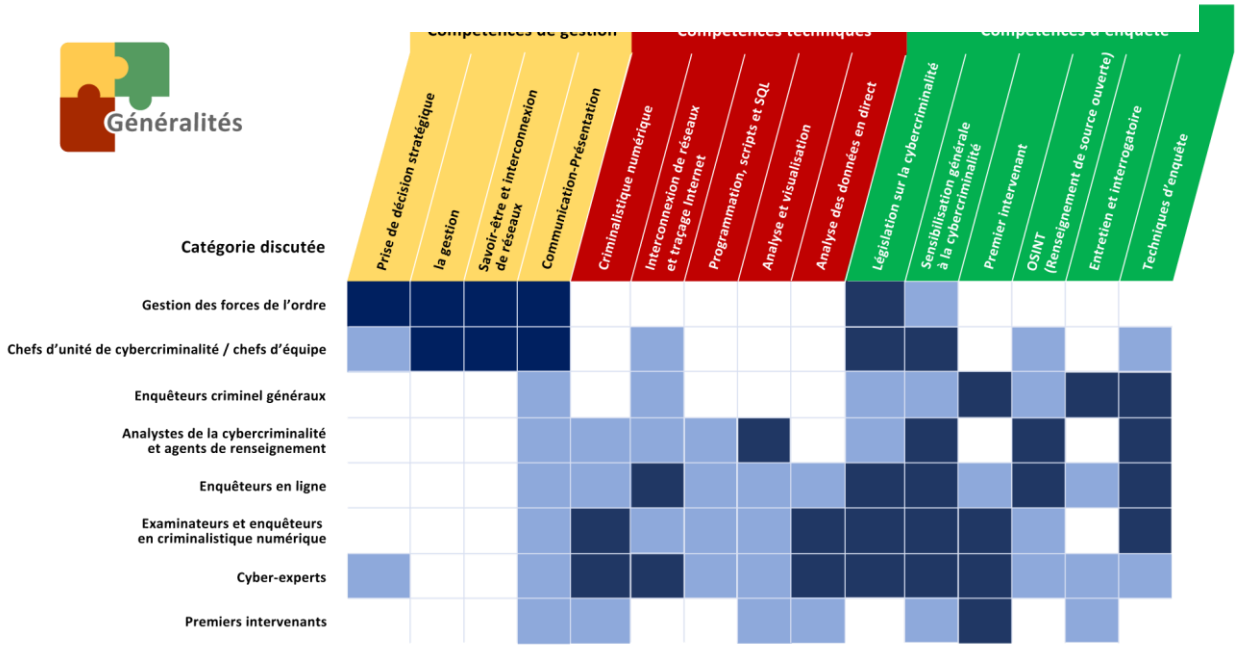
Il existe plusieurs exemples internationaux de développement des compétences numériques qui peuvent servir de guide dans le développement des compétences numériques pour les forces de l'ordre canadiennes.

La Convention de Budapest sur la cybercriminalité est le seul traité international contraignant sur cette question. Il sert de guide à tout pays développant une législation contre la cybercriminalité et de cadre de coopération internationale (The Council of Europe, 2020).

Découlant de la Convention de Budapest et illustré à la figure 5 [2], l'Agence de l'Union européenne pour la formation des services répressifs, par l'intermédiaire de son Groupe européen de formation et d'éducation en matière de cybercriminalité, a créé des compétences numériques pour les différents « acteurs » chargés de l'application des lois impliqués dans la réponse aux crimes commis sur le cyber-spectre (European Cybercrime Training and Education Group, 2020).

[2] Le bleu clair représente la formation de base. Le bleu foncé représente la formation de niveau avancé.

Figure 5. Matrice des compétences requises pour les acteurs de l'application de la loi



Source: ***CITATION Eur20 \l 1033*** (European Cybercrime Training and Education Group, 2020)

Cette matrice identifie les acteurs chargés de l'application de la loi en termes de rôles d'une manière similaire au modèle de réponse à plusieurs niveaux. Il sert de point de départ utile dans le développement d'un Cadre de gestion axé sur les compétences pour la plupart des quadrants du modèle de réponse à plusieurs niveaux. Les compétences numériques du Groupe européen de formation et d'éducation en matière de cybercriminalité sont résumées dans le tableau 3.

Tableau 3. Rôles et compétences numériques

Rôle	Description	Compétences numériques
Chef d'unité de cybercriminalité/ **Chef d'équipe**	Il traite directement avec les cyber-enquêteurs et experts. Ils devraient prendre des décisions éclairées dans les affaires de cybercriminalité ou dans d'autres enquêtes complexes impliquant des éléments de cybercriminalité.	• Connaissance approfondie de la cybercriminalité et des infractions de cybercriminalité • Connaissance approfondie des questions juridiques et juridictionnelles • Connaissance du cadre institutionnel de la coopération internationale • Connaissance des procédures d'enquête pertinentes • Connaissance de haut niveau des outils d'investigation et de criminalistique • Connaissance des besoins de formation et des ressources disponibles • Compétences en gestion du personnel • Compétences en gestion budgétaire

		• Compétences en rédaction de proposition de projet • Gestion des relations et savoir-être • Compétences en communication
Cyber-experts	Cette catégorie comprend les professionnels impliqués en tant que représentants tactiques de l'application de la loi dans les cyberattaques qui coopèrent avec d'autres acteurs (agence de cybersécurité, équipe de réponse aux incidents de sécurité informatique, services informatiques et direction concernés) pour lancer des contre-mesures techniques coercitives, ainsi que pour acquérir, préserver, analyser et documenter des traces (numérique) complexes et des preuves électroniques.	• Identification des preuves électroniques et prise de contrôle des bonnes pratiques • Sensibilisation avancée à la cybercriminalité • Réseau criminalistique avancé • Analyse stratégique et opérationnelle de la cybercriminalité • Outils d'analyse et de visualisation • Script • Compétences en rédaction de rapports et présentation de preuves • Coopération judiciaire internationale en matière de cybercriminalité
Examinateur criminalistique numérique	Ces professionnels effectuent des examens criminalistiques détaillés des preuves numériques informatisées.	• Sensibilisation avancée à la cybercriminalité • Connaissance approfondie des enjeux juridiques et juridictionnelles • Traitement des preuves numériques tout en maintenant la chaîne des preuves • Connaissances approfondies dans un ou plusieurs domaines criminalistiques • Familiarité avec différents systèmes d'exploitation et applications • Connaissance des outils commerciaux et à source ouverte pertinents • Connaissance des scripts/programmation et des requêtes de bases de données (SQL) • Compréhension des artefacts criminalistiques et de la gravure de données • Connaissance de l'analyse des données *post-mortem* et en direct • Compétences en rédaction de rapports • Présentation des preuves

Analyste de la cybercriminalité	Ces professionnels se concentrent sur l'analyse stratégique, la recherche, l'analyse et la présentation des dernières menaces et la fourniture d'aperçus situationnels ou sont plus engagés dans l'analyse opérationnelle pour trouver des modèles, des tendances et des points chauds et créer des liens entre les cas réels.	• Analyse stratégique et opérationnelle de la criminalité • Gestion et analyse des mégadonnées • Sensibilisation avancée à la cybercriminalité • Outils d'analyse et de visualisation • Enquête source ouverte • Enquête sur les réseaux sociaux • Script/programmation • Réseau criminalistique • Compétences en rédaction de rapports • Présentation des preuves • Principes fondamentaux des enquêtes secrètes
Enquêteur en ligne	Ces agents sont chargés de surveiller le monde numérique et de proposer de nouveaux sujets et dossiers à enquêter, ainsi que de mener ou d'accompagner les enquêtes.	• Sensibilisation avancée à la cybercriminalité • Connaissance approfondie des enjeux juridiques et juridictionnelles • Traitement des preuves numériques tout en maintenant la chaîne des preuves • Enquête source ouverte avancée • Enquête sur les réseaux sociaux • Réseau criminalistique avancé • Compétences en rédaction de rapports • Enquêtes secrètes • Script/programmation • Techniques de mener un entretien • Présentation des preuves
Enquêteur criminel général	Les enquêteurs ordinaires confrontés à l'utilisation de l'internet et des outils numériques par des criminels.	• Sensibilisation avancée à la cybercriminalité • Connaissance approfondie des enjeux juridiques et juridictionnelles • Traitement des preuves numériques tout en maintenant la chaîne des preuves • Enquête source ouverte avancée • Enquête sur les réseaux sociaux • Réseau criminalistique avancé • Compétences en rédaction de rapports • Enquêtes secrètes • Script/programmation • Techniques de mener un entretien • Présentation des preuves
Premier intervenant	Un acteur de premier intervenant fait référence aux agents de la force publique qui	• Normes et meilleures pratiques en matière d'identification et prise de contrôle de preuves électroniques

	sont les premiers à entrer en contact avec des preuves électroniques potentielles. Les policiers patrouilleurs, les détectives, les contrôleurs des frontières et des impôts sont tous des exemples de premiers intervenants.	• Acquisition de données de base en criminalistique en direct • Connaissances de base sur la criminalistique numérique (outils, techniques, méthodes et meilleures pratiques), y compris la technologie Internet, le dark web et les crypto-monnaies • Gestion de scène de crime • Techniques d'entretien • Sensibilisation générale à la cybercriminalité

Source: (European Cybercrime Training and Education Group, 2020)

Aux États-Unis, le National White Collar Crime Center (NW3C) dispose de certifications spécialisées pour les examinateurs et les enquêteurs en cybercriminalité qui identifient spécifiquement les ensembles de connaissances requises (NW3C, 2021). Le processus de certification NW3C, détaillé dans le tableau 4, peut également être un guide utile dans le développement de compétences avancées pour les activités de police du cyber-spectre.

Table 4. Organisme de cyber-certification NW3C des connaissances requises

Examinateur certifié de cybercriminalité (3CE)	Enquêteur certifié en cybercriminalité (3CI)
Applique les meilleures pratiques en matière de techniques criminalistiques numériques pour imager, documenter et rapporter des preuves numériques solides.	Détecte, répondre et enquête sur les cybercrimes et les crimes facilités par la communication en ligne.
Connaissances 3CE:	Connaissances 3CI:
1. Technologies 2. Traitement des preuves numériques 3. Imagerie criminalistique 4. La criminalistique du système de fichiers 5. Concepts criminalistiques 6. Cadre législatif, juridique et réglementaire	1. Théorie et histoire 2. Cybercriminalité courante et délits facilités par l'internet 3. Collecte et analyse des preuves détenues par les fournisseurs de services électroniques 4. Enquête sur la cybercriminalité et les crimes facilités par l'internet 5. Cybersécurité, atténuation de la cybercriminalité et cyber-hygiène 6. Cadre législatif, juridique et réglementaire

Source: (NW3C, 2021)

Dans une perspective à l'échelle de l'entreprise, la recherche canadienne met l'accent sur l'importance de la cyber hygiène et de la littératie numérique dans la formation des recrues policières (Robertson, 2019, pp. 112-114).

D'autres recherches centrées sur le Canada (Baron & Le Khac, 2021) ont identifié des compétences techniques, d'enquête et de renseignement pour les enquêteurs en cybercriminalité et les spécialistes des examinateurs judiciaires numériques:

Technologie

- Préservation et acquisition de malware, ICS-SCADA, VM. cryptage/obscursissement/stéganographie
- Analyse RAM, base de données, sauvegarde, malware, ICS-SCADA, VM et chiffrement/obscurcissement/ stéganographie
- Examen des preuves numériques telles que RAM, base de données, sauvegarde, etc.
- Examen des preuves numériques telles que les logiciels malveillants, ICS-SCADA, VM et cryptage/obscurcissement/stéganographie
- Programmation (SQL, Script, Java. Python, etc.)
- Concept de sécurité du réseau, menaces, vulnérabilités, impact, etc.
- Enquête sur le réseau, réponse aux incidents et détection d'intrusion
- Analyse des journaux (Accès, Pare-feu, IDS, IPS, etc.)
- Outils et ressources (Arcsight, Splunk, Wireshark, TDR, Netflow, etc.)
- Interception des capacités de données en direct
- Analyse des données en direct 5.04 Paysage de malware

Investigation

• Témoignage et témoignage d'expert

Intélligence

- Crypto-monnaies
- Ressources et outils de renseignement
- Contre-espionnage et contre-mesures

L'importance des compétences numériques pour les premiers intervenants, cependant, ne peut pas être surestimée comme l'a souligné la mort tragique de Rehtaeh Parsons,

> *"Après l'affaire Rehtaeh Parsons, il y avait un besoin identifié pour une meilleure éducation… Les membres en première ligne ne savaient tout simplement pas par où commencer."* (Thatcher, 2017, p. 17)

Bien que les versions antérieures de la matrice du Groupe européen de formation et d'éducation en matière de cybercriminalité aient négligé les compétences numériques des premiers intervenants (Sobusial-Fischanaller & Vandermeer, 2016; European Cybercrime Training and Education Group, 2020), le groupe a récemment développé E-FIRST, le « forfait d'apprentissage des premiers intervenants » à travers lequel il espère former des milliers de premiers intervenants aux compétences numériques suivantes :

- Capacité d'identifier et de saisir des preuves électroniques potentielles, y compris la criminalistique des données en direct
- Sensibilisation à la cybercriminalité, à l'internet, au cryptage, au dark web et aux crypto-monnaies
- Aider les victimes de crimes facilités par les technologies lors d'une plainte et du commencement d'un dossier criminel (European Cybercrime Training and Education Group, 2021)

Une base solide de compétences numériques pour tous les membres du service de police est également reconnue comme un élément clé de la cyber stratégie de la Police provinciale de l'Ontario :

- L'agent de première ligne connaîtra et suivra la politique de la police provinciale de l'Ontario sur le traitement des enquêtes sur les preuves numériques
- Sera capable de parler avec des membres du public d'une manière professionnelle et significative sur les questions de cybercriminalité
- Connaîtra les services spécialisés de la Police provinciale de l'Ontario qui peuvent aider aux enquêtes sur la cybercriminalité et saura comment et quand les contacter pour obtenir une aide supplémentaire dans les enquêtes
- Aura des connaissances sur la façon d'identifier, de saisir et de protéger l'intégrité des appareils numériques afin qu'ils puissent être correctement examinés par les services spécialisés de la Police provinciale de l'Ontario
- Sera responsable de la création du rapport de niche pour le système de gestion des dossiers initial (y compris l'ajout des biens saisis et la notation des codes DUC appropriés pour une enquête sur les preuves numériques) et la soumission d'un formulaire de demande de service à l'Unité de la criminalité technique
- Le premier point de contact pour obtenir de l'aide avec un appareil numérique sera l'analyste régional de la criminalistique numérique, qui sera en mesure de conseiller l'agent sur le niveau approprié de service spécialisé requis. (Ontario Provincial Police (1), 2016, p. 16)

Le besoin de compétences numériques pour les premiers intervenants et le manque de formation abordable sont reconnus comme un problème par l'Association internationale des chefs de police (IACP) (Federal Bureau of Investigation, 2016). En réponse, l'IACP s'est associé au bureau fédéral d'enquête (FBI) pour lancer un programme en ligne visant à améliorer les connaissances techniques des premiers intervenants sur la façon d'étudier et de sécuriser les artefacts numériques (Carnegie Mellon University, 2018).

La GRC en Colombie-Britannique a été la pionnière du développement du triage numérique sur le terrain pour former les membres des premiers intervenants à récupérer des preuves numériques, tandis que les membres de la GRC en Nouvelle-Écosse sont formés pour répondre directement aux cas avec un élément cyber ou technologique, y compris la fraude, le vol d'identité, l'exploitation des enfants en ligne et la cyberintimidation (Siden, 2017; Thatcher, 2017).

Bien que les compétences numériques des premiers intervenants dans ces dernières initiatives ne soient pas explicitement définies, la notion et l'intention d'améliorer la capacité des premiers intervenants à répondre efficacement aux crimes avec des éléments cyber et numériques sont cohérentes.

3. Phase de consultation

3.1. Mise en place d'un groupe de discussion

Le plan de projet initial prévoyait divers experts en cyber-matière et praticiens des enquêtes sur la cybercriminalité se réunissant pour un atelier de plusieurs jours afin de définir et de développer un dictionnaire de compétences numériques et des profils de compétences numériques pour les forces de l'ordre canadiennes. Cependant, la pandémie mondiale et les restrictions de voyage qui en ont résulté ont empêché la tenue de l'atelier. Au lieu de cela, le RCSP a organisé une série de groupes de discussion virtuels.

En mars et avril 2021, une série de groupes de discussion virtuels de deux heures ont été organisés avec des praticiens et des experts de la lutte contre la cybercriminalité de l'industrie et des services de police de partout au Canada.[3] Les groupes de discussion comprenaient le Comité sur la cybercriminalité des Services nationaux de police et le Comité sur la cybercriminalité de l'Association canadienne des chefs de police et son sous-comité de la cybercriminalité en tant que principaux groupes de gouvernance de la cybercriminalité.

Un document de discussion basé sur la revue de la littérature a permis de consolider les approches globales des compétences numériques dans le maintien de l'ordre et de structurer les discussions avec les groupes de discussion. Les participants aux groupes de discussion ont reçu le document de discussion avant leur séance. Le document de discussion demandait aux lecteurs de considérer ces questions :

1. Existe-t-il un besoin de compétences numériques dans la police ?
2. S'il y a un besoin, doivent-ils être à l'échelle de l'entreprise ou limités à des équipes spécialisées?
3. Le Cadre de gestion axé sur les compétences est-il la bonne approche pour développer des compétences numériques ?
4. Est-ce qu'une approche élargie (au-delà de la cybercriminalité) des compétences numériques est-elle appropriée ?
5. Le modèle d'intervention à plusieurs niveaux et la division du travail sont-ils un modèle viable sur le plan opérationnel pour les services de police canadiens?
6. Pouvons-nous utiliser le modèle du Groupe européen de formation et d'éducation en matière de cybercriminalité comme point de départ ?
7. Votre agence possède-t-elle des compétences numériques qui peuvent être partagées ?
8. Quelles compétences numériques sont uniques à l'expérience canadienne?
9. Est-ce que les compétences numériques notées dans le document sont pertinentes à l'expérience canadienne?

De plus, les participants aux groupes de discussion ont reçu des instructions de connexion qui leur ont fourni un contexte et des informations sur les objectifs du projet de compétence numérique. Les instructions d'adhésion comprenaient un ensemble de compétences préliminaires à discuter.

Les instructions d'adhésion demandaient également aux participants d'effectuer les tâches suivantes avant leur groupe de discussion :

1. Lisez, s'il vous plaît, le document de travail de RCSP. Le document est conçu pour structurer la conversation et présente des concepts sur lesquels nous nous appuierons pendant les groupes de discussion.
2. Considérez les rôles identifiés dans le document de discussion. Sont-ils complets ? Y a-t-il quelque chose qui manque ? Y a-t-il des rôles identifiés qui ne sont pas nécessaires ?
3. Examinez les ébauches de profils de compétences. Sont-ils complets ? Y a-t-il quelque chose qui manque ? Y a-t-il des rôles identifiés qui ne sont pas nécessaires ?

4. Votre organisation a-t-elle déjà des profils de compétences pour ces rôles ou un rôle similaire ? Pouvez-vous les partager avec le RCSP?

3.2 Conclusions du groupe de discussion

Bien que la discussion du groupe de discussion ait été organique, les modérateurs du RCSP ont saisi les points saillants concernant les questions ci-dessus. Voici les principales conclusions des groupes de discussion :

1. Un consensus s'est dégagé sur la nécessité d'une formation supplémentaire sur la cybercriminalité pour les agents de police et les professionnels de la police.
2. Une formation à la cybercriminalité est requise à tous les niveaux, du niveau de base au niveau avancé.
3. De nombreux participants ne connaissaient pas les cadres de gestion fondés sur les compétences.
4. Il a été convenu que les compétences devraient guider le développement de la formation.
5. Les participants ont convenu que les compétences numériques devraient porter sur la technologie en tant que criminalité ciblée, la technologie en tant qu'instrument pour commettre des infractions et les preuves de l'empreinte numérique et qu'une définition plus générale de la cybercriminalité était appropriée.
6. Un consensus s'est dégagé sur le fait que les unités spécialisées en cybercriminalité n'ont pas la capacité de traiter les cybercrimes à grand volume tels que la fraude sur l'internet et les preuves de l'empreinte numérique. La plupart des organismes au Canada ont déjà un modèle d'intervention à plusieurs niveaux formel ou informel.
7. Il a été reconnu que la plupart des membres d'une organisation policière sont exposés à des activités sur le spectre cybernétique régulièrement.
8. De l'avis général, les généralistes tels que les premiers intervenants et les détectives de détachement devraient posséder des compétences numériques, mais pas nécessairement à un niveau avancé.
9. Bien que le modèle du Groupe européen de formation et d'éducation en matière de cybercriminalité ait été perçu comme un cadre intéressant, il n'y a pas eu de consensus sur son adoption dans le contexte canadien. Les principales raisons étaient que des acteurs et des compétences supplémentaires étaient nécessaires et que les niveaux de compétence devaient être mieux définis.
10. Aucun des participants n'a été en mesure de fournir les compétences numériques existantes. La GRC, la Police provinciale de l'Ontario, le service de police de Calgary, le service de police de Saskatoon et le service de police de Vancouver ont été en mesure de fournir des descriptions de poste ou des programmes de formation pour les unités spécialisées dans lesquelles les compétences étaient implicitement incluses.
11. Il y a eu une discussion approfondie sur les divers rôles dans un contexte d'application de la loi. Il y avait un accord sur les rôles spécialisés des examinateurs criminalistiques numériques, des enquêteurs sur la cybercriminalité et des enquêteurs de source ouverte en ligne.

12. Les modérateurs ont orienté la discussion vers les rôles de non-spécialiste et les rôles de spécialiste supplémentaires. La plupart des participants ont convenu que tous les membres du service de police, les premiers intervenants, les détectives généralistes et les services d'approche et d'aide aux victimes étaient des rôles appropriés et nécessaires dans l'espace de la police numérique.

13. Les participants aux groupes de discussion ont identifié de manière indépendante le rôle des cyber-enquêteurs intermédiaires comme le technicien en criminalistique numérique de la GRC ou l'analyste en criminalistique numérique régional de la Police provinciale de l'Ontario. De même, les participants ont noté que le rôle des analystes du renseignement tactique et stratégique était essentiel pour comprendre les tendances de la cybercriminalité et identifier les personnes d'intérêt.

14. Il y avait moins d'accord concernant le rôle de gestion et de leadership. Certains gestionnaires de police ont noté qu'étant donné que la cybercriminalité n'était qu'une partie de leur portefeuille, il serait difficile d'atteindre le niveau d'expertise. D'autres ont souligné que le rôle des gestionnaires et des superviseurs des unités dédiées à la cybercriminalité devrait être inclus dans le profil de compétences, car les gestionnaires sont souvent affectés sans expérience préalable en matière de cybercriminalité.

15. Une large discussion a eu lieu sur les compétences appropriées. Bien que la plupart des participants aient convenu que les compétences identifiées dans le modèle du Groupe européen de formation et d'éducation en matière de cybercriminalité ont une application générale dans le contexte canadien, le consensus était que les compétences devaient être mieux décrites et délimitées par niveaux de compétence.

16. Parmi les compétences incluses dans le modèle du Groupe européen de formation et d'éducation en matière de cybercriminalité, les participants ont convenu que malgré leurs préoccupations concernant la description et la délimitation des niveaux de compétence, la criminalistique numérique, la criminalistique des données en direct, la programmation et les scripts, l'analyse de données, la sensibilisation à la cybercriminalité et le renseignement source ouverte étaient tous des compétences très pertinentes dans le contexte canadien.

17. Outre les compétences pertinentes du modèle du Groupe européen de formation et d'éducation en matière de cybercriminalité, les thèmes de l'alphabétisation numérique, de la cyber hygiène, de la cybersécurité, de la sensibilisation à la cybercriminalité, de la prévention de la cybercriminalité et de l'assistance aux cyber victimes ont été identifiés par divers participants comme des compétences essentielles dans la lutte contre la cybercriminalité.

18. Il y a eu une discussion animée sur la loi changeante et évolutive relative aux preuves numériques et à la criminalistique numérique. Il y avait un consensus sur le fait que tous les membres des services de police devraient comprendre la jurisprudence et les lois relatives aux preuves numériques, y compris les perquisitions et saisies et la présentation des preuves.

19. L'importance et l'utilisation croissantes des crypto-monnaies, associées à un manque général de connaissances, ont été soulevées par les participants à plusieurs reprises dans plus d'un groupe de discussion. Il a été convenu que les policiers devaient au moins être sensibilisés aux crypto-monnaies et à leurs utilisations potentielles dans des activités criminelles.

20. En raison des compétences requises et de l'omniprésence potentielle des appareils de l'internet des objets, les participants ont suggéré que la criminalistique des réseaux (Cloud) devrait être une compétence distincte et séparer de celle de la criminalistique numérique.

4. Profils des compétences numériques

4.1. À propos des compétences

La composante principale du Cadre de gestion axé sur les compétences du RCSP est un dictionnaire de compétences qui détaille quarante-deux compétences policières. Le dictionnaire des compétences divise les compétences d'enquête spécialisées en cinq niveaux (Canadian Police Knowledge Network, 2020). Pour assurer la cohérence avec cette approche, les niveaux de compétence prédéfinis pour les compétences d'enquête seront utilisés pour construire les profils de compétences de la police numérique.

Tableau 5. Niveaux des compétences d'enquête spécialisées, dictionnaire des compétences du RCSP

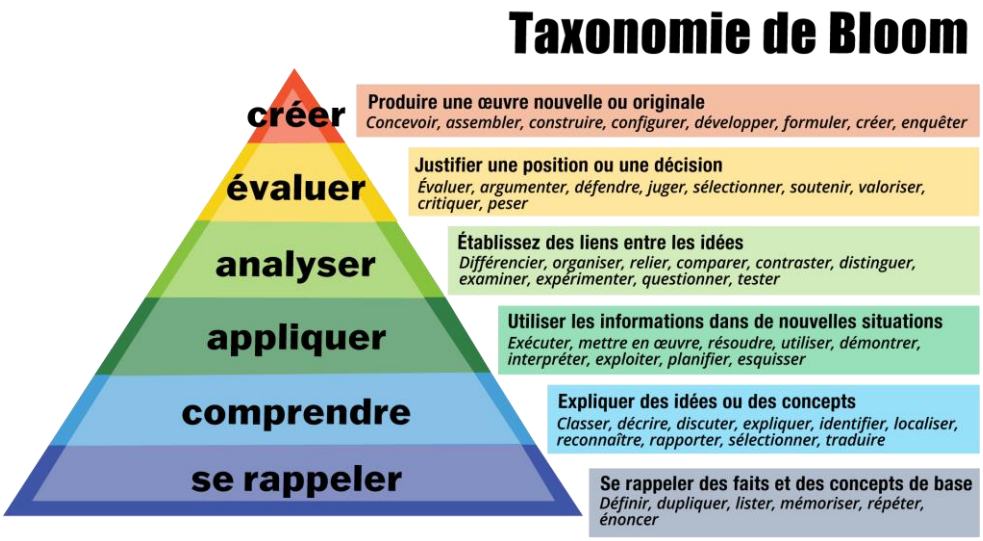
Niveau 1	Niveau 2	Niveau 3	Niveau 4	Niveau 5
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.

Source: (Canadian Police Knowledge Network, 2020)

Bien que la délimitation des cinq niveaux de compétence suive le cadre utilisé dans le Dictionnaire de compétences du RCSP, l'attribution des niveaux de compétence dans la création des profils de compétences numériques est grandement informée par la taxonomie révisée de Bloom. En termes simplifiés, les niveaux de maîtrise des compétences sont conçus pour correspondre aux six étapes de la taxonomie révisée de Bloom, comme illustré à la figure 6. [3]

[3] Pour plus d'informations sur la taxonomie de Bloom (révisée), voir https://uwaterloo.ca/centre-for-teaching-excellence/teaching-resources/teaching-tips/planning-courses-and-assignments/course-design/blooms-taxonomy

Figure 6. Révision d'Anderson et Krathwohl (2001) de la hiérarchie cognitive de Bloom



Source: (Armstrong, 2021)

Emploi et Développement social Canada définit les compétences comme *« l'utilisation combinée des capacités et attributs personnels, des compétences et des connaissances pour accomplir efficacement un travail, un rôle, une fonction, une tâche ou un devoir »* (Government of Canada, 2020). L'acquisition des compétences va au-delà de la participation aux cours. Par exemple, en plus de la réussite du programme criminalistique du Technological Crime Learning Institute, la GRC exige que les examinateurs criminalistiques numériques suivent un programme d'étude de deux ans (Baron & Le Khac, 2021, p. 15). La Police provinciale de l'Ontario a un programme d'étude similaire pour ses analystes criminalistique numériques.

À des niveaux inférieurs, cependant, l'acquisition des compétences peut être atteinte grâce au rappel, à la sensibilisation et à la compréhension (University of Waterloo, 2021). Dans ces circonstances, il est concevable qu'une compétence qui exige une maîtrise des niveaux 1 ou 2 puisse être atteinte simplement par éducation.

Des en-têtes de compétences générales et des descriptions simplifiées comme celles utilisées dans la matrice du Groupe européen de formation et d'éducation en matière de cybercriminalité permettent un « renouvellement » des compétences. Par exemple, si une compétence avec un en-tête général comme « Renseignements et collecte de données à source ouverte » capture l'essence des connaissances et des compétences requises à chacun des cinq niveaux de compétence, elle évite d'avoir à mettre à jour et à modifier la compétence à mesure que les techniques et les technologies évoluent. Ce projet vise à développer des compétences faciles à comprendre et durables pour éclairer les programmes de formation axés sur les compétences. Bien qu'un programme d'études ou un programme de formation puisse avoir besoin d'être ajusté, la compétence restera valide ou « à perpétuité » quels que soient les changements dans la technologie, les techniques d'enquête et de criminalistique, ou la loi.

4.2. Dictionnaire des compétences

Basé sur les réponses des groupes de discussion, de l'examen des pratiques mondiales et de la prise en compte de la taxonomie de Bloom, un dictionnaire de compétences et des profils de compétences numériques ont été élaborés.

Dix compétences numériques ont été identifiées comme les compétences numériques requises pour les forces de l'ordre canadiennes :

1. **Compétences numériques et l'internet**
   La capacité de trouver, d'évaluer, d'utiliser, de partager et de créer du contenu à l'aide des technologies de l'information et de l'internet.

2. **Cyber-hygiène et cybersécurité**
   Pratiques et étapes que les utilisateurs d'ordinateurs et d'autres appareils prennent pour maintenir la santé du système et améliorer la sécurité en ligne.

3. **Sensibilisation à la cybercriminalité, prévention et assistance aux victimes**
   Sensibilisation aux éléments du spectre cyber (empreinte numérique, facilité par Internet, cyber activé, cyberdépendant), prévention de la victimisation et assistance aux victimes de la cybercriminalité.

4. **Renseignement de source ouverte et collecte de preuves**
   Surveiller et rechercher des sites internet connus (sites de médias sociaux, forums sur l'internet, blogs, microblogs, podcasts, photographies ou images, vidéos, signets sociaux, etc.) pour recueillir des informations à partager en tant que preuves ou renseignements.

5. **Cyber légalités**
   Questions juridiques propres aux preuves numériques, y compris les considérations relatives à la *Charte canadienne des droits et libertés*, la jurisprudence, le droit écrit et le droit international, la présentation au tribunal et la préparation aux poursuites.

6. **Analyse des cyber données et du renseignement**
   L'examen des ensembles de données pour trouver des tendances et tirer des conclusions sur les informations qu'ils contiennent.

7. **Crypto-monnaie et Blockchain**
   L'utilisation de la crypto-monnaie pour acheter des biens et des services, l'utilisation du grand livre de cryptographie en ligne pour sécuriser les transactions en ligne.

8. **Programmation et scripts**
   Concevoir et construire un programme informatique exécutable pour accomplir un résultat informatique spécifique ou pour effectuer une tâche spécifique.

9. **La criminalistique numérique**
   Collecte et analyse de preuves dans les médias numériques pour appuyer les enquêtes.

10. **La criminalistique du réseau (Cloud)**
    Analyse des réseaux et des preuves des médias numériques stockées sur les réseaux pour soutenir l'enquête.

Une description détaillée de chaque compétence et des éléments de chacun des cinq niveaux est fournie ci-dessous.

Compétences numériques et l'internet				
La capacité de trouver, d'évaluer, d'utiliser, de partager et de créer du contenu à l'aide des technologies de l'information et de l'internet.		• L'internet • Outils de recherche Internet • Utilisation de matériel et de technologies communs		
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.
Connaissance du matériel informatique et des logiciels couramment utilisés Sensibilisation au fonctionnement du matériel informatique Comprend la recherche, la récupération et le stockage de données, d'informations et de contenus dans des environnements numériques	Comprend les périphériques informatiques et leurs procédures de fonctionnement Connaissance des protocoles Internet courants Applique une variété d'outils pour rechercher, récupérer et stocker des données, des informations et du contenu dans des environnements numériques	Reste à jour avec les technologies nouvelles et émergentes Fournit des orientations et des conseils sur les applications matérielles et logicielles couramment utilisées dans le contexte de l'application de la loi	Entraîne et forme les membres du service de police en matière des compétences numériques Fournit des conseils sur des questions complexes Donne des conseils sur les questions liées à la compétence numérique dans un contexte d'application de la loi	Crée des outils, des méthodes et des techniques pour l'analyse criminalistique numérique Fournit des conseils d'experts sur les problèmes liés à la compétence numérique dans un contexte d'application de la loi aux niveaux national et international

Capacité à interagir via une variété de moyens de communication numériques, y compris le courrier électronique pour un contexte donné Adhère aux politiques et procédures relatives à l'utilisation d'ordinateurs, d'appareils numériques et de réseaux Demande l'avis d'experts en la matière si nécessaire	Utilise des logiciels courants de traitement de texte et de tableur. Utilise une variété de logiciels pour compléter des rapports et des présentations Utilise divers logiciels pour faciliter les enquêtes Comprend les empreintes numériques dans un environnement en ligne Connaissance du matériel et des logiciels du réseau privé virtuel, des pare-feu, des applications d'infrastructure à clé publique	Connaissance de l'internet, des intranets, du commerce en ligne, du magasin en ligne et des technologies convergentes, des protocoles de communication réseau, de l'architecture et de la topologie du réseau, de l'environnement virtualisé, des technologies portatives, des bases de données et des logiciels de test et de surveillance spécialisés Comprend et accède aux marchés en ligne, y compris les marchés criminels ou ceux liés au crime en tant que service Comprend le Dark Web, les marchés criminels TOR et les tendances	Évalue l'environnement opérationnel et fournit des conseils stratégiques à la direction Assurer la liaison avec les agences externes et les autres parties prenantes Identifie le besoin de recherche et de développement de nouvelles techniques et technologies Comprend les protocoles de communication de données	Agit à titre d'expert en la matière dans l'élaboration et la prestation de formations spécialisées Agit en tant qu'expert en la matière dans l'élaboration de lois, de règlements ou de politiques liés à l'utilisation des technologies Participe à des associations professionnelles Publie des recherches et des livres blancs Présente à des conférences nationales et internationales

Cyber-hygiène et cybersécurité				
Pratique les étapes que les utilisateurs d'ordinateurs et d'autres appareils prennent pour maintenir la santé du système et améliorer la sécurité en ligne.		• Mots de passe • Matériel • Hameçonnage	• Logiciels malveillants • Empreinte numérique • Services numériques « Politique de confidentialité »	
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.
Sensibilisation à la cyber-hygiène et aux bonnes pratiques en matière de cybersécurité Sensibilisation à l'ingénierie sociale et à l'hameçonnage en tant que cible potentielle Connaissance des techniques de protection des appareils et du contenu numérique Sensibilisation aux risques et menaces dans les environnements numériques	Comprend la sécurité et la confidentialité sur l'internet Prise de conscience de la nécessité de protéger les identités en ligne Applique des politiques et des protocoles pour protéger les informations personnelles et d'entreprise et la cybersécurité	Reste à jour avec la cybersécurité émergente et les cybermenaces émergentes Fournit des conseils aux membres du service sur la cyber-hygiène et la cybersécurité, y compris la réduction de l'empreinte numérique Comprend les technologies et les composants de l'infrastructure du réseau	Comprendre l'environnement de sécurité complexe, y compris l'architecture, l'infrastructure, la gestion physique, des identités et des accès, et les technologies en évolution avec la participation de plusieurs parties prenantes Appliquer des techniques de conception de systèmes, d'intégration technologique et d'analyse, y compris des méthodes de test et des	Crée de nouveaux outils, méthodes et techniques pour l'analyse criminalistique numérique post-attaque Donne des conseils d'experts sur les problèmes liés à la cyber-hygiène et à la cybersécurité dans un contexte d'application de la loi au niveau national et international

Connaissance des pratiques et des politiques de cybersécurité de l'entreprise, y compris l'utilisation autorisée du matériel informatique et des logiciels Comprend le concept d'empreinte numérique dans un contexte d'application de la loi Comprend les politiques de mot de passe et l'intégrité du mot de passe Demande l'avis d'experts en la matière si nécessaire	Comprend et applique des techniques pour traiter et limiter les données d'identification personnelle produites par le biais d'outils et d'environnements numériques Comprend l'utilisation de l'ingénierie sociale et des techniques d'hameçonnage couramment utilisées	Applique les principes de cybersécurité en utilisant des technologies de surveillance du réseau Applique des techniques pour créer une analyse d'attribution post-exploitation	pratiques de recherche et de reconnaissance détaillées Évalue et recommande des changements aux pratiques et politiques de cybersécurité de l'entreprise Agit à titre d'expert en la matière dans l'élaboration et la prestation de formations spécialisées Utilise des outils et des techniques de test d'intrusion courants dans l'industrie pour tester la cybersécurité	Agit en tant qu'expert en la matière dans l'élaboration de réglementations ou de politiques liées à la cybersécurité et à la sécurité de l'information Participe à des associations professionnelles Publie des recherches et des livres blancs Présente à des conférences nationales et internationales

Sensibilisation à la cybercriminalité, prévention et assistance aux victimes				
Sensibilisation aux éléments du cyber-spectre (empreinte numérique, facilité par l'internet, cyber activé, cyberdépendant), prévention de la victimisation et assistance aux victimes de la cybercriminalité		● Types de cybercriminalité ● Durcissement ciblé ● Prévention de la cybercriminalité		● Services aux victimes ● Orientation communautaire
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.
Reconnaît les éléments du cyber-spectre (empreinte numérique, facilité par l'internet, cyber activé, cyberdépendant) Sensibilisation aux ressources nationales sur la cybercriminalité (CAFC, Senior Busters, NC3) Connaissance des services disponibles pour les victimes Demande l'avis d'experts en la matière si nécessaire	Reconnaît les cybercrimes courants et les crimes cybernétiques Comprend les informations requises lors de la prise de rapports de cybercriminalité et de crime cyber activé Comprendre et faciliter l'orientation des victimes de la cybercriminalité et du crime cyber activé vers les services et ressources appropriés pour les victimes	Comprend la criminalité basée sur la technologie, la cybercriminalité et les techniques utilisées par les délinquants Fournit des conseils à la police et à la communauté (particuliers et entreprises) sur la cybercriminalité et la prévention de la criminalité informatique	Évalue les tendances émergentes en matière de cybercriminalité et du crime cyber activé et fournit des conseils sur la prévention de la victimisation Évalue l'environnement opérationnel et fournit des conseils stratégiques aux dirigeants sur les questions liées à la prévention de la cybercriminalité et à la réponse/aux services aux victimes	Donne des conseils d'experts sur la prévention de la cybercriminalité et les services aux victimes aux niveaux national et international Agit en tant qu'expert en la matière dans la création et la prestation de formations spécialisées concernant la prévention de la cybercriminalité et les services aux victimes

	Sensibilisation aux techniques de prévention de la cybercriminalité et de la victimisation liée à la cybercriminalité	Comprend et anticipe les besoins des victimes de la cybercriminalité et du crime cyber activé Fournit des conseils concernant les services disponibles pour les victimes de la cybercriminalité et du crime cyber activé Comprend la victimologie périphérique des cyberattaques contre des entités tierces	Assure la liaison avec des agences externes et d'autres parties prenantes pour évaluer et créer des programmes de prévention et améliorer les services aux victimes de la cybercriminalité Assure la liaison avec les responsables de la cybersécurité et de la sécurité de l'information des entreprises des secteurs public et privé concernant le paysage des cybermenaces Fournit une formation sur la prévention de la cybercriminalité et les services aux victimes	Agit en tant qu'expert en la matière dans l'élaboration de lois, de règlements ou de considérations politiques concernant la prestation de programmes de prévention de la cybercriminalité et l'amélioration des services aux victimes

Renseignement de source ouverte et collecte de preuves				
Surveiller et rechercher des sites Internet connus (sites de médias sociaux, forums Internet, blogs, microblogs, podcasts, photographies ou images, vidéos, signets sociaux, etc.) pour recueillir des informations à partager comme preuves ou renseignements		• Moteurs de recherche • Méta robots d'exploration • Dark Web • Des médias sociaux	• Géolocalisation • Surveillance Web • Bavarder pair-à-pair	
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.
Comprend le terme « source ouverte » Utilise les moteurs de recherche Internet courants Connaissance des adresses Internet, y compris la navigation Internet Utilise des sites communs de médias sociaux et de marché Sensibilisation à l'empreinte numérique	Comprend l'utilisation de l'internet comme outil de recherche d'investigation Comprend les concepts fondamentaux de la recherche, de l'investigation et du renseignement en ligne, y compris les outils et techniques essentiels Comprend le profil d'attribution de l'empreinte numérique et les proxys IP	Analyse des métadonnées Applique des techniques avancées de recherche sur l'internet, y compris la géolocalisation et la dé-anonymisation des utilisateurs dans un contexte réel et historique Applique des techniques et des logiciels de recherche avancés pour rechercher le dark web et TOR.	Entraîne Évalue les technologies émergentes et les changements législatifs relatifs aux preuves et au renseignement de source ouverte Évalue et fournit des conseils sur les plans de recherche et de collecte	Donne des conseils d'expert sur les problèmes liés à la collecte de preuves et de renseignements à la source aux niveaux national et international Agit à titre d'expert en la matière dans la création et la prestation de formations spécialisées

Demande l'avis d'experts en la matière si nécessaire et comprend comment et où demander conseil Comprend la loi et la politique dans l'utilisation des preuves de médias sociaux à source ouverte Comprend comment documenter les recherches sur Internet et se présenter dans les procédures judiciaires	Comprend les problèmes de confidentialité et de sécurité liés à la collecte d'informations à source ouverte Sensibilisation au dark web et aux TOR	Applique des outils pour préserver et assurer l'intégrité des documents en ligne Comprend la loi et les politiques relatives à la création et à l'utilisation de comptes et de « pots de miel » d'enquêteurs sur les réseaux sociaux Fournit des conseils et évalue les techniques source ouvertes, l'utilisation de comptes proxy, la confidentialité et les considérations de sécurité Utilise et accède aux marchés en ligne, y compris les marchés criminels ou ceux liés au crime en tant que service Applique les principes d'approvisionnement dans la création de rapports Témoigne	Évalue et fournit des conseils sur les problèmes complexes de source ouverte et l'utilisation des comptes d'enquêteurs et des pots de miel Évalue l'environnement d'exploitation et fournit des conseils stratégiques aux dirigeants sur les questions liées au renseignement de source ouverte et à la collecte de preuves Assure la liaison avec les agences externes et les autres parties prenantes Fournit une formation sur la collecte de preuves et le renseignement de source ouverte Effectue une évaluation par les pairs des rapports et de l'approvisionnement Assure le respect des politiques et de la législation en matière de confidentialité et de sécurité	Agit en tant qu'expert en la matière dans l'élaboration de considérations législatives, réglementaires ou politiques dans l'utilisation des preuves des médias sociaux et la création de comptes d'enquêteurs non secrets et secrets et de pots de miel

Cyber légalités				
Questions juridiques propres aux preuves numériques, y compris les considérations relatives à la Charte, la jurisprudence, le droit écrit et le droit international. Présentation au tribunal et préparation aux poursuites.		• Application pratique du droit des perquisitions et saisies concernant les données et les appareils numériques • Présentation des preuves • Continuité des preuves • Rapports et notes • Confidentialité et archivage • Traités et accès aux données internationales		
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.
Sensibilisation aux exigences et politiques de confidentialité, de liberté d'information et d'archivage régissant l'utilisation des réseaux informatiques et la conservation des informations	Comprend la chaîne de contrôle en ce qui concerne les appareils numériques et les preuves numériques Applique les principes de rédaction des ordonnances judiciaires pour les enquêtes impliquant des preuves numériques	Évalue et fournit des conseils sur la recherche et la saisie des appareils numériques, des données et d'autres preuves numériques Évalue les plans et fournit des conseils sur les attentes raisonnables en matière de confidentialité dans les appareils numériques et les données connexes	Tenir à jour la jurisprudence et les lois relatives à la recherche et à la saisie d'appareils numériques, de données et de preuves numériques Comprend et maintient une connaissance actuelle des traités internationaux relatifs à la preuve numérique	Agit en tant qu'expert en la matière dans l'élaboration de considérations législatives, réglementaires ou politiques concernant la recherche et la saisie d'appareils numériques et de preuves numériques

Sensibilisation aux principes de gestion des preuves Applique des pouvoirs accessoires pour la perquisition et la saisie d'appareils numériques et de preuves numériques Comprend la documentation des actions liées aux preuves numériques Comprend l'articulation des autorités juridiques pour les actions Demande l'avis d'experts en la matière si nécessaire	Comprend les exigences en matière de documentation et de divulgation concernant les preuves numériques. Comprend comment présenter des preuves numériques dans les procédures judiciaires	Applique des techniques pour prouver l'authenticité et la continuité des artefacts numériques Connaissance des traités internationaux sur les preuves numériques et leur application aux enquêtes nationales Comprend les questions et les complexités juridictionnelles liées au mouvement transfrontalier des données et des données stockées sur les réseaux (stockage en nuage) Évalue et fournit des conseils sur la rédaction d'ordonnances judiciaires complexes, y compris les demandes d'entraide juridiques (MLAT) et les mandats généraux	Assurer la liaison avec des agences externes et d'autres parties prenantes pour assurer la connaissance de la jurisprudence et de la loi en ce qui concerne les preuves numériques Applique les critères relatifs à l'utilisation de témoins experts et fournit des preuves d'opinion au besoin Évalue les plans et fournit des conseils aux gestionnaires de cas sur l'utilisation et les limites des experts et des témoins experts dans une enquête Crée et donne une formation sur les ordonnances judiciaires en ce qui concerne les appareils numériques et les preuves numériques	Agit en tant qu'expert en la matière dans l'élaboration de considérations politiques concernant le rôle et la participation des témoins experts en preuves numériques

Analyse des cyberdonnées et du renseignement				
L'examen des ensembles de données pour trouver des tendances et tirer des conclusions sur les informations qu'ils contiennent.		• Bases de données • Analyses statistiques • Science des données • Analyse des liens • Logiciel d'analyse		
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.
Connaissance des bases de données policières et de leur application aux problèmes du cyber-spectre Demande l'avis d'experts en la matière si nécessaire	Comprend les problèmes associés aux activités criminelles liées au cyber-spectre Liens de sensibilisation et autres analyses de données pour appuyer les enquêtes Utilise des outils facilement disponibles pour rechercher des informations dans les bases de données	Évalue les tendances émergentes et les activités criminelles du cyber-spectre Produit des rapports de renseignement stratégique concernant la cybercriminalité émergente et les tendances émergentes Utilise un logiciel approprié pour interroger les données afin d'aider les enquêtes en cours en créant des graphiques de liaison	Entraîne Applique les principes de la science des données, y compris l'analyse statistique, pour produire des rapports stratégiques Fournit des conseils sur la gestion des données et l'utilisation de l'analyse statistique et recommande l'utilisation de logiciels appropriés	Crée de nouveaux outils, méthodes, techniques pour les exécutables intégrés et autonomes Donne des conseils d'expert sur les problèmes d'analyse de données relatives à la cybercriminalité et aux tendances émergentes aux niveaux national et international

	Effectue une analyse routinière des ensembles de données	Produit des rapports tactiques et opérationnels liés à l'analyse des données Applique des techniques d'analyse de données et des applications logicielles appropriées Intègre les principes d'analyse du renseignement aux cadres standard de l'industrie pour l'évaluation des cybermenaces et des acteurs de la menace Témoigne	Évalue et fournit des conseils sur les techniques d'analyse Assure la liaison avec les agences externes et les parties prenantes sur l'analyse des données liées aux activités criminelles sur le cyber-spectre Identifie et évalue les menaces et les acteurs impliqués dans des activités criminelles sur le cyber-spectre Crée des évaluations des menaces Identifie et évalue les moyens d'infiltrer, d'enquêter, de détecter, de prévenir, de dissuader et/ou de perturber les réseaux cybercriminels Applique les concepts associés à l'analyse Big Data et aux logiciels associés	Agit en tant qu'expert en la matière dans l'élaboration d'analyses de données liées aux questions d'application de la loi du spectre numérique Participe à des associations professionnelles Publie des recherches et des livres blancs Présente à des conférences nationales et internationales

Crypto-monnaie et Blockchain				
L'utilisation de la crypto-monnaie pour acheter des biens et des services, l'utilisation de la cryptographie en ligne pour sécuriser les transactions en ligne.		• Diverses devises • Portefeuilles • Blockchain	• Réseaux distribués • Codes QR • Exploitation minière	
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.
Sensibilisation aux crypto-monnaies Sensibilisation à l'anonymat des transactions de crypto-monnaie Demande l'avis d'experts en la matière si nécessaire	Comprend les principes fondamentaux du fonctionnement des crypto-monnaies Connaissance des mécanismes de transaction de crypto-monnaie, y compris les adresses Bitcoin Comprend comment et où les crypto-monnaies sont converties en espèces	Applique le vocabulaire et les concepts clés liés à la blockchain et aux crypto-monnaies Comprend l'utilisation criminelle de la crypto-monnaie Comprend comment acquérir, disposer et récupérer diverses crypto-monnaies Utilise la crypto-monnaie	Comprend la structure, les utilisations et les applications de la technologie blockchain Comprend l'utilisation de la blockchain au-delà de la crypto-monnaie Assure la liaison avec les agences externes et les parties prenantes sur les questions liées à la crypto-monnaie dans un contexte d'application de la loi	Crée de nouveaux outils, méthodes, techniques d'analyse criminalistique des crypto-monnaies et des technologies de la chaîne de blocs Donne des conseils d'expert sur les questions liées aux crypto-monnaies dans un contexte d'application de la loi

	Comprend les signes de crypto-monnaie, y compris les codes QR et les portefeuilles numériques Sensibilisation aux réseaux distribués et à la blockchain	Utilise et applique les meilleures pratiques de sécurité pour les portefeuilles crypto dans un contexte d'application de la loi Applique des techniques pour tracer les portefeuilles de crypto-monnaie Applique les exigences de stockage et de sécurité de la crypto-monnaie Évalue et fournit des conseils sur la saisie et le stockage de la crypto-monnaie Témoigne	Identifie et évalue les problèmes émergents liés à la crypto-monnaie et à la blockchain dans un contexte d'application de la loi Évalue l'environnement opérationnel et fournit des conseils stratégiques à la direction Comprend la législation et les réglementations relatives aux crypto-monnaies et à la blockchain Crée et dispense des formations sur la crypto-monnaie et la blockchain dans un contexte d'application de la loi	Agit à titre d'expert en la matière dans la création et la prestation de formations spécialisées Agit en tant qu'expert en la matière dans l'élaboration de lois, de réglementations ou de politiques relatives aux crypto-monnaies et à la blockchain Participe à des associations professionnelles Publie des recherches et des livres blancs Présente à des conférences nationales et internationales

Programmation et scripts				
Concevoir et construire un programme informatique exécutable pour accomplir un résultat informatique spécifique ou pour effectuer une tâche spécifique.		• Langages de programmation • Compétences en codage • SQL • Opérateurs booléens		
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.
Sensibilisation au codage et aux scripts en tant que principal moyen de personnaliser les logiciels et de rechercher efficacement des données Utilise des outils de recherche d'interface graphique Demande l'avis d'experts en la matière si nécessaire	Utilise des opérateurs booléens dans les moteurs de recherche; peut demander des conseils sur la syntaxe et l'ordre des opérations Utilisation du code, des scripts et des commandes SQL pré-écrits en tant qu'exécutables autonomes ou en tant que macros dans le logiciel et comprendre leurs opérations	Utilise un ou plusieurs langages de programmation et de script sans guide pour créer des exécutables autonomes et intégrés de base Lit le code et interprète la fonction du programme, y compris le débogage des erreurs Fournit des conseils sur booléen et SQL	Effectue une analyse approfondie du code et des scripts Utilise divers langages et scripts informatiques pour créer des exécutables complexes autonomes et intégrés Entraîne sur les fondamentaux de l'écriture de scripts ou du codage	Crée de nouveaux outils, méthodes et techniques pour les exécutables intégrés et autonomes Donne des conseils d'expert sur les problèmes liés aux scripts et au codage liés aux activités d'application de la loi du spectre numérique aux niveaux national et international Agit en tant qu'expert en la matière dans le développement de logiciels

		Fournit des conseils sur les utilisations appropriées du script intégré	Assurer la liaison avec les agences externes et les parties prenantes sur des solutions logicielles personnalisées liées aux questions d'application de la loi sur le spectre numérique Identifie et évalue les langages de codage et les solutions appropriés pour le développement de logiciels liés aux activités d'application de la loi sur le spectre numérique	liés aux enquêtes et à l'application de la loi Agit en tant qu'expert en la matière dans le développement de logiciels liés aux questions d'application de la loi du spectre numérique Participe à des associations professionnelles Publie des recherches et des livres blancs Présente à des conférences nationales et internationales

La criminalistique numérique				
Collecte et analyse de preuves des médias numériques pour appuyer les enquêtes.		• Analyse des données mortes • Analyse des données en direct • Systèmes d'exploitation	• Réseaux • Cryptage et obscurcissement	
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.
Comprend les sources potentielles de preuves numériques Comprend la nécessité de préserver et la valeur des preuves numériques Adhère aux politiques et procédures du service pertinent à la recherche, la saisie et le traitement des preuves numériques Demande l'avis d'experts en la matière si nécessaire	Comprend le stockage multimédia numérique, y compris : - l'ordinateur - téléphone portable - l'internet - caméra	Se tient au courant des technologies émergentes Évalue les plans d'enquête et fournit des conseils aux membres de première ligne et aux enquêteurs Identifie et évalue les preuves d'artefacts criminalistiques Fournit un soutien sur place lors de l'exécution de mandats de perquisition	Entraîneurs Fournit des conseils sur des problèmes complexes Évalue l'environnement opérationnel et fournit des conseils stratégiques à la direction Assure la liaison avec les agences externes et les autres parties prenantes	Crée de nouveaux outils, méthodes, techniques pour l'analyse criminalistique numérique Donne des conseils d'expert sur les questions liées à l'analyse criminalistique numérique au niveau national et international Agit à titre d'expert en la matière dans l'élaboration et la prestation de formations spécialisées

	Comprend les preuves numériques potentielles liées à la cybercriminalité courante et aux crimes cybernétiques, notamment : - logiciels malveillants - pourriel - fraude - vol d'identité - Harcèlement sur l'internet - l'exploitation des enfants - sexto Utilise des outils criminalistique de base pour collecter des preuves numériques facilement accessibles Comprend la législation relative à la recherche, la saisie et le traitement des preuves numériques Comprend comment documenter et présenter des preuves numériques Connaissance des protocoles de cryptage couramment utilisés et des signes de cryptage	Applique les principes criminalistiques dans l'acquisition, la conservation et l'examen des preuves numériques mortes et vivantes Comprend les techniques typiques de désobscurcissement et de traçage Comprend les systèmes de fichiers et les principales caractéristiques distinctives des systèmes d'exploitation Utilise des protocoles de cryptage et des techniques de décryptage courants Témoigne en tant qu'expert	Évalue et mène des enquêtes de réseau complexes Effectue une évaluation par les pairs des preuves numériques pour l'admissibilité légale dans les affaires pénales Identifie et évalue le besoin de recherche et de développement de nouvelles techniques et technologies Comprend la législation relative à l'analyse criminalistique numérique Gère l'acquisition d'outils d'analyse des médias numériques	Agit en tant qu'expert en la matière dans l'élaboration de lois, de règlements ou de politiques en matière d'analyse criminalistique numérique Participe à des associations professionnelles Publie des recherches et des livres blancs Présente à des conférences nationales et internationales

La criminalistique du réseau				
Analyse des réseaux et des preuves des médias numériques stockées sur les réseaux pour soutenir les enquêtes.		• Architecture de réseau • Traçage du réseau • Nuage (Cloud) • Cryptage et obscurcissement		
Niveau 1	**Niveau 2**	**Niveau 3**	**Niveau 4**	**Niveau 5**
Applique les connaissances de base dans des situations routinières et prévisibles avec conseils.	Applique les connaissances de base dans une gamme de situations typiques qui présentent des défis limités. Orientation requise. Une certaine autonomie ou responsabilité individuelle.	Applique de solides connaissances dans une gamme complète de situations non typiques de complexité modérée avec un minimum de conseils ou pas de conseils.	Applique des connaissances avancées dans un large éventail de situations complexes. Guide d'autres professionnels.	Applique des connaissances avancées dans les situations les plus complexes et imprévisibles. Développe de nouvelles approches, méthodes ou politiques dans le domaine. Fournit des conseils au niveau national et international.
Sensibilisation aux réseaux et au Cloud en tant qu'utilisateur Comprend la législation relative à la recherche, la saisie et le traitement des preuves numériques obtenues à partir du stockage en nuage de d'autres réseaux distants	Comprend les principes fondamentaux des composants, du matériel et des paquets de réseau informatique Connaissance des types d'adresses réseau, des protocoles TCP et UDP, des possibilités de recherche directe et inversée des adresses courriels	Se tient au courant des technologies de réseau nouvelles et émergentes Évalue les plans et fournit des conseils aux membres de première ligne et aux enquêteurs concernant le nuage et les réseaux Fournit un soutien sur place lors de l'exécution de mandats de perquisition	Entraîne Fournit une analyse et une évaluation de l'architecture du réseau Fournit des conseils sur des problèmes complexes impliquant l'architecture du réseau et leur analyse criminalistique Évalue l'environnement opérationnel et fournit des conseils stratégiques à la direction	Développe de nouveaux outils, méthodes, techniques pour l'analyse judiciaire des réseaux Donne des conseils d'expert sur les problèmes liées à la criminalistique des réseaux aux niveaux national et international Agit à titre d'expert en la matière dans l'élaboration et la prestation de formations spécialisées

Adhère aux politiques et procédures du service relatives à la recherche, la saisie et le traitement des preuves numériques obtenues à partir du nuage ou d'autres réseaux distants Demande l'avis d'experts en la matière si nécessaire	Connaissance des preuves généralement disponibles à partir de l'empreinte numérique du réseau (Cloud) Connaissance des artefacts numériques (mots de passe, codes QR, clés PKI) qui permettent d'accéder au stockage en nuage ou au stockage en réseau à distance	Applique des techniques criminalistique pour localiser, acquérir, préserver et examiner les preuves numériques stockées sur des réseaux ou des centres de données distants Applique des techniques criminalistiques pour identifier les artefacts qui aident à la gestion des identités et des accès Applique les principes criminalistiques à la désobscurcissement et au traçage du réseau Applique les principes de la cryptographie et des techniques de décryptage Auteur les rapports techniques criminalistiques pour le tribunal Témoigne	Assure la liaison avec les agences externes et les autres parties prenantes Évalue les options de réponse aux incidents et supervise la réponse aux incidents Évalue les enquêtes de réseau criminalistiques proposées Identifie le besoin de recherche et de développement de nouvelles techniques et technologies Possède une compréhension approfondie de la législation relative à l'analyse criminalistique numérique des réseaux, y compris le mouvement transfrontalier de données Gère l'acquisition d'outils d'analyse de réseau Fournit un témoignage d'expert	Agit en tant qu'expert en la matière dans l'élaboration de lois, de règlements ou de politiques en matière d'analyse criminalistique numérique Participe à des associations professionnelles Publie des recherches et des livres blancs Présente à des conférences nationales et internationales

4.3. Cyber-acteurs

En complément des compétences numériques, ces dix cyber-acteurs ou rôles ont été identifiés comme ceux qui sont régulièrement engagés dans l'application de la loi et exercent des activités sur le cyber-spectre :

Tous les membres du service de police

Tout employé ou bénévole d'un service de police ayant accès au réseau informatique. Ces compétences servent de base de compétences pour tous les autres rôles.

Premiers intervenants

Les membres des services de police qui répondent aux appels de service. Ce sont généralement les premières personnes à réagir à des activités criminelles et à travailler en uniforme. Ces compétences servent également de fondement à tous les autres rôles.

Fonctions générales des enquêteurs/détectives

Les enquêteurs de police qui travaillent principalement dans les sections d'enquêtes générales, les bureaux d'enquête criminelle, les unités criminelles ou les bureaux de détective divisionnaire. Ils sont généralement communautaires et s'occupent d'enquêtes sur des activités criminelles dépassant les capacités des premiers intervenants en uniforme.

Enquêteurs intermédiaires (liés à la cybersécurité)

Des professionnels de la police dotés d'une capacité et d'une formation supplémentaires pour saisir des preuves électroniques et soutenir les enquêtes comportant des éléments numériques, y compris l'extraction de données de base, la capture de données et la saisie de données. Ils fournissent des conseils et une assistance locale sur les interrogatoires et les ordonnances judiciaires pour les enquêtes avec des éléments numériques. Ils préparent des expositions qui nécessitent un examen plus avancé ou technique et assurent la liaison avec des acteurs ayant des connaissances avancées ou expertes.

Professionnels de la sensibilisation/de la liaison avec les victimes

Professionnels de la police qui s'engagent à fournir à leur communauté des conseils en matière de prévention du crime. Ce groupe peut comprendre des agents de service communautaire, des agents de liaison avec les écoles et des agents de liaison avec les victimes. Les tâches de niveau avancé peuvent inclure la prestation de programmes de sensibilisation, de prévention et d'éducation en matière de cybersécurité à l'industrie, aux entreprises et au gouvernement (par exemple, les municipalités, les conseils scolaires, etc.).

Enquêteurs en ligne

Enquêteurs de police qui mènent des enquêtes principalement par internet. Ils peuvent inclure des enquêteurs spécialisés engagés dans des rôles de lutte contre l'exploitation (l'exploitation sexuelle des enfants et le trafic d'êtres humains), des enquêteurs de la sécurité nationale et des agents de renseignement criminel. Ils surveillent l'internet comme une sorte d'officiers de « patrouille numérique ». Ils identifient et proposent de nouvelles enquêtes et ils sont formés aux techniques de renseignement de source ouverte et aux domaines techniques tels que le traçage, l'obscurcissement, le cryptage et la contre-expertise judiciaire.

Analystes de la cybercriminalité (tactique et stratégique)

Les professionnels de la police se sont engagés dans des analyses stratégiques pour identifier et rechercher les dernières menaces et activités de cybercriminalité ou fournir un soutien tactique aux enquêtes en cours en identifiant les modèles, les points chauds et les liens dans les activités criminelles. Les personnes engagées dans ce rôle doivent être capables de traiter de grandes quantités de données diverses pour produire des rapports concis et exploitables.

Examinateurs criminalistiques numériques

Professionnels de la police qui effectuent des examens criminalistiques experts concernant les données au repos et récupèrent des artefacts numériques à partir de divers matériels informatiques et réseaux.

Enquêteurs sur la cybercriminalité

Professionnels de la police qui enquêtent et atténuent les cyberattaques, y compris, mais sans s'y limiter, le DOS, l'intrusion de données et les extorsions ransomware; ils obtiennent et préservent les preuves électroniques et surmontent l'obscurcissement de l'origine.

Cybergestionnaires et dirigeants

Professionnels de la police qui s'occupent d'enquêtes complexes sur la cybercriminalité à titre de leader. Ils conseillent la direction sur les initiatives stratégiques et les tendances liées à la cybercriminalité, supervisent les aspects opérationnels de leur unité et fournissent des conseils aux autres secteurs du service de police concernant la cybercriminalité et/ou les preuves numériques.

4.4. Profils de compétences numériques

Le profil de compétences numériques décrit les compétences et le niveau de maîtrise dont les différents cyber acteurs ont besoin pour accomplir les éléments essentiels de leur travail. Les profils de compétences sont résumés dans le tableau 6 suivis d'une description détaillée pour chacun des profils de compétences du cyber acteur.[4]

[4] The profiles also include some non-digital competencies that are part of the existing CPKN-CBMF competency dictionary.

Tableau 6: Matrice de profils de compétences numériques pour les forces de l'ordre canadiennes

** Compétences non numériques supplémentaires également recommandées - voir les profils détaillés*

	Compétences numérique et l'Internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Tous les membres	1	1								
Premier intervenant *	1	2	2	1	1	1	1		2	1
Détective général*	2	2	2	2	2	2	2		2	2
Enquêteur intermédiaire*	3	3	3	2	2	2	2	3	3	3
Sensibilisation/liaison avec les victimes*	2	2	4	2	2	1	2		2	2
Enquêteur en ligne*	4	3	2	4	3	3	3	3	2	3
Analyste de la cybercriminalité*	3	3	2	3	2	4	4	4	2	3
Examinateur médico-légal numérique*	4	4	2	3	3	3	4	3	5	5
Enquêteur sur la cybercriminalité*	4	3	3	3	4	3	4	2	2	2
Cyber gestionnaire et dirigeant*	3	3	3	2	4	2	2		2	2

Tous les membres du service de police qui ont accès aux réseaux informatiques et/ou aux systèmes de messagerie			
Description du role	**Exigences de formation essentielles**	**Compétence numérique**	**Niveau**
Tout employé ou bénévole d'un service de police ayant accès au réseau informatique. Ces compétences servent de base de compétences pour tous les autres rôles.	Compétence numérique fondamentale Cyber-hygiène fondamentale Cybersécurité personnelle et organisationnelle fondamentale Législation et politique fondamentales en matière de confidentialité et d'archivage Où et comment demander l'aide de ressources spécialisées	Compétence numérique et l'internet Cyber-hygiène et sécurité	1 1

Premiers intervenants (généralement une patrouille en uniforme)			
Description du role	**Exigences de formation essentielles** ***Tous les membres du Service de police PLUS :***	**Compétence numérique**	**Niveau**
Les membres des services de police qui répondent aux appels de service. Ce sont généralement les premières personnes à réagir à des activités criminelles et à travailler en uniforme. Ces compétences servent également de fondement à tous les autres rôles.	Littératie numérique fondamentale Identification des preuves électroniques Sensibilisation à la criminalistique numérique Saisie et conservation des appareils numériques avant l'examen criminalistique Consentement éclairé pour la collecte de preuves	Compétence numérique et l'internet Cyber-hygiène et sécurité Cybercriminalité, prévention et assistance aux victimes Source ouverte Cyber Légalités Analyse des données et du renseignement	1 2 2 1 1 1

	Techniques fondamentales de capture Web Collecte de preuves numériques fondamentales Gestion numérique fondamentale des scènes de crime Sensibilisation générale à la cybercriminalité et au crime cyber activé Cybersécurité personnelle et organisationnelle fondamentale Besoins des victimes et services disponibles Présentation au tribunal de preuves numériques Sensibilisation à la crypto-monnaie Où et comment demander l'aide de ressources spécialisées	Crypto-monnaie et Blockchain La criminalistique numérique La criminalistique du réseau (Cloud) *Compétences non numériques existantes du RCSP :* • *Témoignage au tribunal* • *Gestion des scènes de crime* • *Entretiens* •*Prendre des notes*	1 2 1

Enquêteur/détective de fonctions générales			
Description du role	**Exigences de formation essentielles** ***Premiers intervenants PLUS :***	**Compétence numérique**	**Niveau**
Les enquêteurs de police qui travaillent principalement dans les sections d'enquêtes générales, les bureaux d'enquête criminelle, les unités criminelles ou les	Techniques fondamentales de cyberinvestigation Cybercriminalité et sensibilisation à la criminalité informatique	Compétence numérique et l'internet Cyber-hygiène et sécurité Cybercriminalité, prévention et assistance aux victimes	2 2 2

bureaux de détective divisionnaire. Ils sont généralement communautaires et s'occupent d'enquêtes sur des activités criminelles dépassant les capacités des premiers intervenants en uniforme.	Fondamentaux des preuves disponibles à partir des empreintes numériques Autorités légales, exigences et procédures Principes fondamentaux de la collecte de preuves et de renseignements de source ouverte Fondamentaux de l'enquête sur les réseaux sociaux Fondamentaux de la crypto-monnaie Besoins des victimes et services disponibles Entretien Où et comment demander l'aide de ressources spécialisées	Source ouverte Cyber légalités Analyse des données et des renseignements Crypto-monnaie et Blockchain La criminalistique numérique La criminalistique du réseau (Cloud) *Compétences non numériques existantes du RCSP-Cadre de gestion axé sur les compétences :* • *Témoignage au tribunal* • *Gestion des scènes de crime* • *Entretiens* • *Obtention des autorisations judiciaires* • *Prendre des notes*	2 2 2 2 2 2

Enquêteur intermédiaire (liés à la cybersécurité)			
Description du role	**Exigences de formation essentielles**	**Compétence numérique**	**Niveau**
Des professionnels de la police dotés d'une capacité et d'une formation supplémentaires pour saisir des preuves électroniques et soutenir les enquêtes comportant des éléments numériques, y compris l'extraction de données	Sensibilisation avancée à la cybercriminalité et au crime cyber activé Connaissance avancée spécialisée (appareils mobiles, ordinateur, réseau) Application pratique des principes de gestion de scènes de crime	Compétence numérique et l'internet Cyber-hygiène et sécurité Cybercriminalité, prévention et assistance aux victimes Source ouverte Cyber légalités	3 3 3 2 2

de base, la capture de données et la saisie de données. Ils fournissent des conseils et une assistance locale sur les interrogatoires et les ordonnances judiciaires pour les enquêtes avec des éléments numériques. Ils préparent des expositions qui nécessitent un examen plus avancé ou technique et assurent la liaison avec des acteurs ayant des connaissances avancées ou expertes.	Application pratique de principes de traçage de réseau et IP Programmation et script Autorités légales, exigences et procédures Rédaction de rapports techniques et judiciaires Témoignage techniques et judiciaires Application pratique de crypto-monnaie Où et comment demander l'aide de ressources spécialisées ou expertes	Analyse des données et des renseignements Crypto-monnaie et Blockchain Programmation et scripts La criminalistique numérique La criminalistique du réseau (Cloud) *Compétences non numériques existantes du RCSP-Cadre de gestion axé sur les compétences :* ● *Témoignage au tribunal* ● *Gestion des scènes de crime* ● *Prendre des notes*	2 2 3 3 3

Professionnel de la sensibilisation/de la liaison avec les victimes			
Description du role	**Exigences de formation essentielles**	**Compétence numérique**	**Niveau**
Professionnels de la police engagés à fournir à leur communauté des conseils en matière de prévention du crime. Ce groupe peut comprendre des agents de service communautaire, des agents de liaison avec les écoles et des agents de liaison avec les victimes. Au niveau avancé, les tâches peuvent inclure la prestation de programmes de	Sensibilisation avancée à la cybercriminalité et au crime cyber activé Techniques de prévention de la cybercriminalité à grand volume Cyber-hygiène avancée Besoins des victimes et services disponibles Modèles de mobilisation communautaire	Compétence numérique et l'internet Cyber-hygiène et sécurité Cybercriminalité, prévention et assistance aux victimes Source ouverte Cyber légalités Analyse des données et des renseignements Crypto-monnaie et Blockchain	2 2 3/4 2 2 1 2

sensibilisation, de prévention et d'éducation en matière de cybersécurité à l'industrie, aux entreprises et au gouvernement (par exemple, les municipalités, les conseils scolaires, etc.).	Prévention du développement de ressources et de réseaux en matière de cybercriminalité Application pratique de la crypto-monnaie Crime as a Service (CaaS) et marchés criminels Où et comment demander l'aide de ressources spécialisées ou expertes	La criminalistique numérique La criminalistique du réseau (Cloud) *Compétences non numériques existantes du RCSP-Cadre de gestion axé sur les compétences :* ● *Entretiens (victimes)* ● *Prendre des notes* ● *Favoriser les partenariats* ● *Relations communautaires et gestion des médias*	2 2

Enquêteur en ligne			
Description du rôle	**Exigences de formation essentielles**	**Compétence numérique**	**Niveau**
Enquêteurs de police qui mènent des enquêtes principalement par internet. Cela peut inclure des enquêteurs spécialisés engagés dans des rôles de lutte contre l'exploitation (l'exploitation sexuelle des enfants et le trafic d'êtres humains), des enquêteurs de la sécurité nationale et des agents de renseignement criminel. Ils surveillent l'internet comme une sorte d'officiers de « patrouille numérique ». Ils identifient et proposent de nouvelles enquêtes et sont formés aux techniques de renseignement source	Sensibilisation avancée à la cybercriminalité et au crime cyber activé Autorités légales, exigences et procédures Programmation et script Enquête source ouverte avancée Techniques avancées de recherche sur internet Enquête sur les réseaux sociaux dark web, TOR, marchés criminels en ligne et Crime as a Service (CaaS) Désobscurcissement avancé en ligne	Compétence numérique et l'internet Cyber-hygiène et sécurité Cybercriminalité, prévention et assistance aux victimes Source ouverte Cyber légalités Analyse des données et des renseignement Crypto-monnaie et Blockchain Programmation et scripts La criminalistique numérique	3/4 3 1 4 3 3 3 2/3 2

ouverte, aux domaines techniques tels que le traçage, l'obscurcissement, le cryptage et la contre-expertise judiciaire.	La criminalistique du réseau Application pratique de la crypto-monnaie Rédaction de rapports techniques et judiciaires Principes fondamentaux des opérations d'infiltration en ligne Présentation des témoignages d'experts Où et comment demander l'aide de ressources spécialisées ou expertes	Lsa criminalistique du réseau (Cloud) *Compétences non numériques existantes du RCSP-Cadre de gestion axé sur les compétences :* ● *Témoignage au tribunal* ● *Gestion des scènes de crime* ● *Prendre des notes* ● *Analyste du renseignement criminel*	2/3

Analyste de la cybercriminalité (tactique et stratégique)			
Description du rôle	**Exigences de formation essentielles**	**Compétence numérique**	**Niveau**
Les professionnels de la police se sont engagés dans une analyse stratégique pour identifier et rechercher les dernières menaces et activités de cybercriminalité ou fournir un soutien tactique aux enquêtes en cours en identifiant les modèles, les points chauds et les liens dans les activités criminelles. Les personnes engagées dans ce rôle doivent être capables de traiter de grandes quantités de données diverses pour	Analyse stratégique et tactique de la criminalité Analyse de données Big data Analyses statistiques Sensibilisation avancée à la cybercriminalité et au crime cyber activé Enquête source ouverte Réseaux sociaux La criminalistique du réseau Script et codage	Compétence numérique et l'internet Cyber-hygiène et sécurité Cybercriminalité, prévention et assistance aux victimes Source ouverte Cyber légalités Analyse des données et des renseignements Crypto-monnaie et Blockchain Programmation et scripts La criminalistique numérique	3 3 2 3 2 4 3/4 2/3 2

produire des rapports concis et exploitables.	Présentation des preuves Crypto-monnaie Dark Web, TOR, marchés criminels en ligne et Crime as a Service (CaaS) Rédaction de rapports techniques et judiciaires Présentation des témoignages d'experts Où et comment demander l'aide de ressources spécialisées ou expertes	La criminalistique du réseau (Cloud) *Compétences non numériques existantes du RCSP-Cadre de gestion axé sur les compétences :* ● *Témoignage au tribunal* ● *Gestion des scènes de crime* ● *Prendre des notes* ● *Analyste du renseignement criminel*	3

Examinateur criminalistique numérique			
Description du rôle	**Exigences de formation essentielles** ***Enquêteurs intermédiaires et avancés PLUS :***	**Compétence numérique**	**Niveau**
Professionnels de la police qui effectuent des examens criminalistiques expertes concernant les données au repos et récupèrent des artefacts numériques à partir de divers matériels et réseaux.	Connaissances numériques et de matériel informatique avancées Sensibilisation avancée à la cybercriminalité et au crime cyber activé Expertise dans le domaine de la spécialisation criminalistique (appareils mobiles, ordinateur, réseau) Autorités légales, exigences et procédures liées aux preuves numériques Rédaction de rapports techniques et judiciaires	Compétence numérique et l'internet Cyber-hygiène et sécurité Cybercriminalité, prévention et assistance aux victimes Source ouverte Cyber légalités Analyse des données et des renseignements Crypto-monnaie et Blockchain Programmation et scripts La criminalistique numérique	4 4 2 3 3 3 3/4 3 4/5

	Systèmes d'exploitation et applications avancés Désobscurcissement et cryptage avancés Connaissance avancée des artefacts criminalistique et de la gravure de données Crypto-monnaies avancées Présentation de la preuve d'expert, y compris la compréhension du rôle et des limites des témoins experts Où et comment demander l'aide de ressources spécialisées ou expertes	La criminalistique du réseau (Cloud) *Compétences non numériques existantes du RCSP-Cadre de gestion axé sur les compétences :* ● *Témoignage au tribunal* ● *Gestion des scènes de crime* ● *Entretiens* ● *Obtention des autorisations judiciaires* ● *Prendre des notes*	4/5

Enquêteur sur la cybercriminalité			
Description du rôle	**Exigences de formation essentielles** **Enquêteur aux fonctions générales PLUS :**	**Compétence numérique**	**Niveau**
Professionnels de la police qui enquêtent et atténuent les cyberattaques, y compris, mais sans s'y limiter, le DOS, l'intrusion de données et les extorsions de ransomware. Ils acquièrent et préservent des preuves électroniques, y compris le traçage et surmontent l'obscurcissement de l'origine.	Sensibilisation avancée aux menaces de cybercriminalité Sensibilisation avancée à la cybercriminalité et au crime cyber activé La criminalistique des réseaux et du numérique Script et codage Crypto-monnaies avancées Rédaction de rapports techniques et judiciaires	Compétence numérique et l'internet Cyber-hygiène et sécurité Cybercriminalité, prévention et assistance aux victimes Source ouverte Cyber légalités Analyse des données et des renseignements Crypto-monnaie et Blockchain	4 3 3 3 3/4 2/3 3/4

	Techniques de mener un entretien Autorités légales, exigences et procédures Présentation des témoignages d'experts Où et comment demander l'aide de ressources spécialisées ou expertes	Programmation et scripts La criminalistique numérique La criminalistique du réseau (Cloud) *Compétences non numériques existantes du RCSP-Cadre de gestion axé sur les compétences :* ● *Témoignage au tribunal* ● *Gestion des scènes de crime* ● *Entretiens* ● *Obtention des autorisations judiciaires* ● *Prendre des notes*	2 2 2

Cybergestionnaire et dirigeant			
Description du rôle	**Exigences de formation essentielles**	**Compétence numérique**	**Niveau**
Professionnels de la police qui s'occupent d'enquêtes complexes sur la cybercriminalité à titre de leader. Ils conseillent la direction sur les initiatives stratégiques et les tendances liées à la cybercriminalité, supervisent les aspects opérationnels de leur unité et fournissent des conseils aux autres secteurs du service de police concernant la cybercriminalité et/ou les preuves numériques.	Sensibilisation de haut niveau de à la cybercriminalité et au crime cyber activé Autorités légales, exigences et procédures Principes fondamentaux des techniques d'enquête sur la cybercriminalité Besoins des victimes et services disponibles Compétences en gestion du changement technologique et en gestion de la qualité	Compétence numérique et l'internet Cyber-hygiène et sécurité Cybercriminalité, prévention et assistance aux victimes Source ouverte Cyber légalités Analyse des données et des renseignements Crypto-monnaie et Blockchain La criminalistique numérique	3 3 3-4 2 3-4 2 2 2

	Gestion financière – budgétisation, acquisition de technologie La gestion des incidents Principes de gestion de projet Gestion des ressources humaines des professionnels techniques Gestion du changement Gestion de la technologie de l'information Gestion stratégique	La criminalistique du réseau (Cloud) *Compétences non numériques existantes du RCSP-Cadre de gestion axé sur les compétences :* ● *Compétences de performance* ● *Compétences en partenariat* ● *Compétences en matière de responsabilité*	2

5. L’état de la formation actuellement disponible au Canada

5.1. Sondage de formation

Une enquête de source ouverte pour identifier les formations qui correspondent aux profils de compétences a suivi l'élaboration des profils de compétences numériques. Le sondage sur la formation sert uniquement à fournir des exemples de cyberformation actuellement disponibles. Les limites suivantes s'appliquent au sondage sur la formation:

1. Le sondage ne tient compte que de la formation facilement disponible (c.-à-d. une formation que tout organisme canadien d'application de la loi peut identifier rapidement et être en mesure d'inscrire ses membres). Cela n'inclut pas la formation qui a été développée « à l'interne » qui n'est pas annoncée ou facilement accessible par l'ensemble de la communauté canadienne de l'application de la loi.

2. Le sondage est basé sur des recherches de source ouverte sur l’internet et ne prétend pas être exhaustive ou complète. Il ne fournit que des exemples de formation facilement accessible.

3. Il ne prend pas en compte les frais de scolarité, les frais de déplacement et ne fournit pas d'évaluation de l'optimisation des ressources.

Malgré ces limites, le sondage sur la formation donne un aperçu des formations à lesquelles les chefs de police canadiens ou les sections de formation peuvent facilement accéder pour répondre à certaines ou à toutes les exigences de formation qui complètent les profils de compétences. Il fournit également des conseils sur les thèmes et les possibilités d'amélioration de la formation qui sont examinés ci-dessous.

Les tableaux ci-dessous identifient les niveaux de compétence suggérés requis pour chacun des cyberacteurs, la formation facilement disponible et les commentaires généraux.

Tableau 7. Sondage sur la formation actuellement disponible pour les compétences relatives à tous les membres des services de police

	Compétences numérique et l'internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Tous les membres	**1**	**1**								

Cours et compétences numériques : tous les membres des services de police
Compétences numériques et l'internet (1) ● Divers cours de courte durée sont largement disponibles à la fois en ligne et en personne, y compris une formation de sensibilisation non structurée gratuite via Microsoft à Digital Literacy | Microsoft. ● Enquêtes de base en ligne (RCSP – Service de police de Calgary) **Cyber-hygiène et cybersécurité (1)** ● La cybersécurité au GC et le paysage de la cybercriminalité (Centre canadien pour la cybersécurité) ● Cybersécurité de l'Internet des objets (IoT) (Centre canadien pour la cybersécurité)
Notes complémentaires: ● Il n'y a pas suffisamment de formations et de cours pour les compétences numériques rudimentaires et l'internet et la cyber-hygiène et la cybersécurité. Les cours en ligne de plateformes d'apprentissage virtuelles telles que Udemy, Coursera et Edx proposent des cours de base sur la culture numérique. ● Une grande partie de la formation en compétences numérique et de l'internet au niveau de base s'adresse aux personnes âgées. ● Il existe de nombreux matériels de lecture et des ressources sur le sujet couvrant des concepts fondamentaux et de base sur un large éventail de sujets liés à la cybersécurité. Par exemple, le Centre canadien pour la cybersécurité La cybersécurité à la maison et au bureau – Sécuriser vos dispositifs, vos ordinateurs et vos réseaux (ITSAP.00.007) - Centre canadien pour la cybersécurité et Pratiques exemplaires en cybersécurité - Centre canadien pour la cybersécurité

Table 8. Sondage sur la formation actuellement disponible pour les compétences relatives aux premiers intervenants

	Compétences numérique et l'internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Premier intervenant *	1	2	2	1	1	1	1		2	1

Cours et compétences numériques – Premiers intervenants

Compétences numériques et l'internet (1)

- Divers cours de courte durée sont largement disponibles à la fois en ligne et en personne, y compris une formation de sensibilisation non structurée gratuite via Microsoft à Digital Literacy | Microsoft.
- Enquêtes de base en ligne (RCSP – Service de police de Calgary)

Cyber-hygiène et cybersécurité (2)

- La cybersécurité au GC et le paysage de la cybercriminalité (Centre canadien pour la cybersécurité)
- Cybersécurité de l'Internet des objets (IoT) (Centre canadien pour la cybersécurité)
- Enquêtes sur la cybercriminalité de niveau 1 (RCSP – Police régionale d'Halifax)
- Cybersécurité au GC pour les employés non informaticiens (Centre canadien pour la cybersécurité)

Sensibilisation à la cybercriminalité, prévention et assistance aux victimes

- Enquêtes de base en ligne (RCSP – Service de police de Calgary)

Source ouverte (1)

- Enquêtes sur la cybercriminalité niveau 1 (RCSP - Police régionale d'Halifax) *Niveau 1/2

Cyber légalités (1)

- Preuve numérique : Enquêtes de première ligne (RCSP– Police régionale de York) – Niveau 1/2
- Améliorer le signalement de la cybercriminalité grâce à l'Enquête sur la déclaration uniforme de la criminalité (Statistique Canada)
- Pas de formation spécifique à la cyber légalité au niveau de compétence 1 bien que la formation générale de la police (formation des recrues) identifie généralement les concepts.

Analyse des cyber données et du renseignement (1)

- Bien qu'aucune formation spécifique n'ait été identifiée, tous les services de police offrent une formation aux membres de leur service sur divers systèmes de gestion des dossiers.

Crypto-monnaie et Blockchain (1)

- Bien que diverses plateformes en ligne et établissements d'enseignement en personne proposent des cours de sensibilisation à la crypto-monnaie, aucune n'est orientée vers l'application de la loi.

La criminalistique numérique (2)

- Preuve numérique : Enquêtes de première ligne (RCSP – Police régionale de York) – Niveau 1/2
- L'essentiel de la criminalistique numérique (SANS)
- Imagerie numérique criminalistique : documentation et présentation de visuels (Justice Institute of British Columbia)
- Divers fournisseurs de logiciels d'investigation numérique tels que Cellebrite et Magnet Forensics proposent une formation sur l'utilisation de leurs produits utilisés par les premiers intervenants.

La criminalistique du réseau (1)

- Aucune formation spécifique identifiée pour le niveau de compétence 1. La formation commence au niveau de compétence 2 et plus par le biais de prestataires tels que SANS et CompTIA.

Notes supplémentaires:

- Il n'y a pas suffisamment de formations et de cours disponibles pour les compétences numériques de base et de l'internet, la cyber-hygiène et la sécurité, la crypto-monnaie et la blockchain, et la criminalistique des réseaux.
- Les plateformes en ligne comme Udemy, Coursera et Edx proposent de nombreux cours en ligne qui fournissent des informations d'introduction ou de niveau 1 sur ces sujets.
- Une grande partie de la formation en compétences numérique et de l'internet au niveau de base s'adresse aux personnes âgées.
- Moins de formation disponible pour les compétences numériques de niveau inférieur ; au lieu de cela, davantage offrent des ressources telles que des PDFS et des vidéos YouTube partageant des informations de base.

Tableau 9. Sondage sur la formation actuellement disponible pour les compétences relatives aux fonctions générales d'enquêteurs ou de détectives

	Compétences numérique et l'internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Détective général*	2	2	2	2	2	2	2		2	2

Cours et compétences numériques Fonctions générales des Enquêteurs/Détectives

Compétences numériques et l'internet (2)

- Divers cours de courte durée sont largement disponibles à la fois en ligne et en personne. La formation la plus courante est fournie par l'achèvement du CompTIA IT Fundamentals (ITF +).

Cyber-hygiène et cybersécurité (2)

- La cybersécurité au GC et le paysage de la cybercriminalité (Centre canadien pour la cybersécurité)
- Cybersécurité de l'Internet des objets (IoT) (Centre canadien pour la cybersécurité)
- Enquêtes sur la cybercriminalité de niveau 1 (RCSP – Police régionale d'Halifax)
- Cybersécurité au gouvernement du Canada pour les employés non informaticiens (Centre canadien pour la cybersécurité)

Cybercriminalité, prévention et assistance aux victimes (2)

- Enquêtes de base en ligne (RCSP – Service de police de Calgary)
- Aucune formation spécifique identifiée concernant l'assistance aux victimes et la prévention

Source ouverte (2)

- Utilisation de l'internet comme outil de renseignement (INTINT) (Collège canadien de police)
- Enquêtes sur la cybercriminalité de niveau 1 (RCSP – Police régionale d'Halifax)
- Enquêtes sur l'internet - Niveau 2 (Holland College)
- Enquêtes sur l'internet - LITE (Holland College)
- Le guide Facebook pour les enquêteurs (Holland College)

Cyber légalités (2)

- Droit de la sécurité des données et des enquêtes (SANS) - Niveau 2/3
- Enquêtes sur l'internet - Niveau 1 - 2021 SYR APA-III-0812 (Collège de police de l'Atlantique)
- Technologies numériques pour les enquêteurs (Collège canadien de police) – Niveau 2/3
- Cours d'enquêteurs sur la cybercriminalité (Collège canadien de police)

Analyse des cyber données et du renseignement (2)

- Introduction à l'analyse du renseignement (Toddington) - Niveau 2/3
- Renseignements criminels (Analyse 202Eca) (Toddington) – Niveau 2/3
- Renseignement stratégique (Analyse 203E SA) (Toddington) – Niveau 2/3

Crypto-monnaie et Blockchain (2)

- Bien que les plateformes en ligne et les établissements d'enseignement en personne proposent des cours de sensibilisation et de compréhension de la crypto-monnaie, aucun n'est destiné aux forces de l'ordre.

La criminalistique numérique (2)

- Preuve numérique : Enquêtes de première ligne (RCSP – Police régionale de York) – Niveau 1/2
- L'essentiel de la criminalistique numérique (SANS)
- Imagerie numérique criminalistique : documentation et présentation de visuels (Justice Institute of British Columbia)
- Divers fournisseurs de logiciels d'investigation numérique tels que Cellebrite et Magnet Forensics proposent une formation sur l'utilisation de leurs produits utilisés par les premiers intervenants.

La criminalistique du réseau (Cloud) (2)

- Sécurité de base du réseau et de la base de données (IBM by Edx)
- Introduction aux réseaux et au matériel informatique (Association internationale des chefs de police)
- Réseau CompTIA + * Niveaux 2/3

Notes supplémentaires:

- L'analyse des données et du renseignement via Toddington contient deux parties le reliant à un niveau 2/3
- La formation sur la cybercriminalité, la prévention et l'assistance aux victimes, la crypto-monnaie et la chaîne de blocs et la criminalistique des réseaux à ces niveaux est insuffisante.

Tableau 10. Formation actuellement disponible pour les compétences relatives aux techniciens intermédiaires liés à la cybersécurité

	Compétences numérique et l'internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Enquêteur intermédiaire*	3	3	3	2	2	2	2	3	3	3

Cours et compétences numériques Enquêteur intermédiaires en cybersécurité

Compétences numériques et l'internet (3)

- CompTIA A+ (CompTIA)

Cyber-hygiène et cybersécurité (3)

- Cybersécurité dans le camp d'entraînement GC (Centre canadien pour la cybersécurité) * le camp d'entraînement progresse rapidement des concepts de base aux concepts avancés (niveau 2/3)
- Fondations – Informatique, technologie et sécurité (SANS) *Niveau 2/3 – propose des concepts informatiques, des principes de base des réseaux, des concepts de cybersécurité, une introduction à la criminalistique.
- Introduction à la cybersécurité (SANS)* Niveaux 2/3
- CompTIA Security + (CompTIA)

Cybercriminalité, prévention et assistance aux victimes (3)

- • Aucune formation spécifique identifiée

Source ouverte (2)

- Utilisation de l'internet comme outil de renseignement (INTINT) (Collège canadien de police)
- Enquêtes sur la cybercriminalité de niveau 1 (RCSP – Police régionale d'Halifax)
- Enquêtes sur l'internet - Niveau 2 (Holland College)
- Enquêtes sur l'internet - LITE (Holland College)
- Le guide Facebook pour les enquêteurs (Holland College)

Cyber légalités (2)

- Droit de la sécurité des données et des enquêtes (SANS) - Niveau 2/3
- Enquêtes sur l'internet - Niveau 1 - 2021 SYR APA-III-0812 (Collège de police de l'Atlantique)
- Technologies numériques pour les enquêteurs (Collège canadien de police) – Niveau 2/3
- Cours d'enquêteurs sur la cybercriminalité (Collège canadien de police)

Analyse des cyber données et du renseignement (2)

- Introduction à l'analyse du renseignement (Toddington) *Niveau 2/3
- Renseignements criminels (Analyse 202Eca) (Toddington) *Niveau 2/3
- Renseignement stratégique (Analyse 203E SA) (Toddington) *Niveau 2/3

Programmation et scripts (3)

- ICS/SCADA Security Essentials (SANS)
- Fondamentaux de Blue Team : Opérations et analyse de sécurité (SANS)
- L'éducation et la formation à la programmation et au script sont largement disponibles auprès des fournisseurs de cyber éducation privés et publics.

Crypto-monnaie et Blockchain (2)

- Bien que les plateformes en ligne et les établissements d'enseignement en personne proposent des cours de sensibilisation et de compréhension de la crypto-monnaie, aucun n'est destiné aux forces de l'ordre.

La criminalistique numérique (3)

- L'essentiel de la criminalistique numérique (SANS)
- Acquisition et analyse d'appareils mobiles (Collège canadien de police)

La criminalistique du réseau (Cloud) (3)

- Analyse des preuves internet (Collège canadien de police)
- Cours sur les techniques d'enquête en réseau (Collège canadien de police)
- Acquisition et analyse d'appareils mobiles (Collège canadien de police)
- Cloud Security Essentials (SANS)
- Atelier d'analyse en direct (Collège canadien de police) – Niveau 3

Notes supplémentaires:

- La disponibilité des formations et des cours en crypto-monnaie et blockchain est insuffisante.
- L'analyse des données et du renseignement via Toddington contient deux parties le reliant à un niveau 2/3
- De nombreux cours de niveau collégial offrent des cours de programmation et de script qui satisferaient aux exigences de compétence. Par exemple, cours offert à l'Université McMaster : Python for Advanced collection.

Tableau 11. Formation actuellement disponible pour les compétences relatives à la sensibilisation, à la prévention et à l'assistance aux victimes

	Compétences numérique et l'internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Sensibilisation/ liaison avec les victimes*	2	2	4	2	2	1	2		2	2

Cours et compétences numériques Professionnels de la Sensibilisation de la liaison avec les victimes

Compétences numériques et l'internet (2)

- Divers cours de courte durée sont largement disponibles à la fois en ligne et en personne. La formation la plus courante est fournie par l'achèvement du CompTIA IT Fundamentals (ITF +).

Cyber-hygiène et cybersécurité (2)

- La cybersécurité au GC et le paysage de la cybercriminalité (Centre canadien pour la cybersécurité)
- Cybersécurité de l'Internet des objets (IoT) (Centre canadien pour la cybersécurité)
- Enquêtes sur la cybercriminalité de niveau 1 (RCSP – Police régionale d'Halifax)
- Cybersécurité au GC pour les employés non informaticiens (Centre canadien pour la cybersécurité)

Cybercriminalité, prévention et assistance aux victimes (4)

- Conduire le changement en matière de cybersécurité : Construire une culture basée sur la sécurité (SANS)
- Aucune formation spécifique identifiée pour les questions d'assistance aux victimes liées à la cybercriminalité.

Source ouverte (2)

- Utilisation de l'internet comme outil de renseignement (INTINT) (Collège canadien de police)
- Enquêtes sur la cybercriminalité de niveau 1 (RCSP – Police régionale d'Halifax)
- Enquêtes sur l'internet - Niveau 2 (Holland College)
- Enquêtes sur l'internet - LITE (Holland College)
- Le guide Facebook pour les enquêteurs (Holland College)

Cyber légalités (2)

- Preuve numérique : Enquêtes de première ligne (RCSP – Police régionale de York) – Niveau 1/2
- Droit de la sécurité des données et des enquêtes (SANS) - Niveau 2/3
- Enquêtes sur l'internet - Niveau 1 - 2021 SYR APA-III-0812 (Collège de police de l'Atlantique)
- Technologies numériques pour les enquêteurs (Collège canadien de police) – Niveau 2/3
- Cours d'enquêteurs sur la cybercriminalité (Collège canadien de police)

Analyse des cyber données et du renseignement (1)

- Bien qu'aucune formation spécifique n'ait été identifiée, tous les services de police offrent une formation aux membres de leur service sur divers systèmes de gestion des dossiers.

Crypto-monnaie et Blockchain (2)

- Bien que les plateformes en ligne et les établissements d'enseignement en personne proposent des cours sur l'utilisation de la crypto-monnaie, aucune n'est destinée à l'application de la loi.

La criminalistique numérique (2)

- Preuve numérique : Enquêtes de première ligne (RCSP – Police régionale de York) – Niveau 1/2
- L'essentiel de la criminalistique numérique (SANS)
- Imagerie numérique criminalistique : documentation et présentation de visuels (Justice Institute of British Columbia)
- Divers fournisseurs de logiciels d'investigation numérique tels que Cellebrite et Magnet Forensics proposent une formation sur l'utilisation de leurs produits utilisés par les premiers intervenants.

La criminalistique du réseau (Cloud) (2)

- Sécurité de base du réseau et de la base de données (IBM by Edx)
- Introduction aux réseaux et au matériel informatique (Association internationale des chefs de police)

Notes supplémentaires:

- Il n'y a pas suffisamment de formations et de cours disponibles pour l'alphabétisation numérique et de l’internet, la prévention de la cybercriminalité et l'assistance aux victimes, l'analyse des données et du renseignement, et la crypto-monnaie et la blockchain.
- De nombreux cours de niveau collégial offrent des cours de programmation et de scénarisation qui satisferaient aux exigences de compétence. Par exemple, les cours offerts à l'Université McMaster : Python for Basic Collection et Python for Advanced collection.

Tableau 12. Formation actuellement disponible pour les compétences relatives à l'enquêteur en ligne

	Compétences numérique et l'internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Enquêteur en ligne*	4	3	2	4	3	3	3	3	2	3

Cours et compétences numériques Enquêteur en ligne

Compétences numériques et l'internet (4)

- Diverses cours Comp TIA y compris A+, Network+ et Security+

Cyber-hygiène et cybersécurité (3)

- Cybersécurité dans le camp d'entraînement GC (Centre canadien pour la cybersécurité) * le camp d'entraînement progresse rapidement des concepts de base aux concepts avancés (niveau 2/3)
- Fondations – Informatique, technologie et sécurité (SANS) *Niveau 2/3 – propose des concepts informatiques, des principes de base des réseaux, des concepts de cybersécurité, une introduction à la criminalistique.
- Introduction à la cybersécurité (SANS)* Niveaux 2/3
- CompTIA Security + (CompTIA)

Cybercriminalité, prévention et assistance aux victimes (1)

- Enquêtes de base en ligne (RCSP – Service de police de Calgary)
- Aucune formation spécifique identifiée concernant l'assistance aux victimes et la prévention

Source ouverte (4)

- Renseignement de source ouverte avancée (AOSINT) (Collège canadien de police)
- Automatisation de l'analyse du renseignement de source ouverte pratique (OSINT) (SANS)
- Expert certifié en renseignement des médias sociaux (McAfee Institute)
- Analyste certifié en renseignement des médias sociaux (McAfee Institute)

Cyber légalités (3)

- Droit de la sécurité des données et des enquêtes (SANS) - Niveau 2/3
- Enquêtes sur l'internet - Niveau 1 - 2021 SYR APA-III-0812 (Collège de police de l'Atlantique)
- Technologies numériques pour les enquêteurs (Collège canadien de police) – Niveau 2/3
- Cours d'enquêteurs sur la cybercriminalité (Collège canadien de police)

Analyse des cyber données et du renseignement (3)

- Introduction à l'analyse du renseignement (Toddington) * Niveau 2/3
- Renseignements criminels (Analyse 202Eca) (Toddington) *Niveau 2/3
- Renseignement stratégique (Analyse 203E SA) (Toddington) *Niveau 2/3
- Renseignement sur les cybermenaces (SANS) * Niveau 3-4

Crypto-monnaie et Blockchain (3)

- Blockchain et Smart Contract Security (SANS) – Niveau 3
- Bien que les plateformes en ligne et les établissements d'enseignement en personne proposent des cours sur l'utilisation de la crypto-monnaie, aucune n'est destinée à l'application de la loi.

La criminalistique numérique (2)

- Preuve numérique : Enquêtes de première ligne (RCSP – Police régionale de York) – niveau 1-2
- L'essentiel de la criminalistique numérique (SANS)
- Imagerie numérique criminalistique : documentation et présentation de visuels (Justice Institute of British Columbia)
- Divers fournisseurs de logiciels d'investigation numérique tels que Cellebrite et Magnet Forensics proposent une formation sur l'utilisation de leurs produits utilisés par les premiers intervenants.

La criminalistique du réseau (3)

- Analyse des preuves Internet (Collège canadien de police)
- Cours sur les techniques d'enquête en réseau (Collège canadien de police)
- Acquisition et analyse d'appareils mobiles (Collège canadien de police)
- Cloud Security Essentials (SANS)
- Atelier d'analyse en direct (Collège canadien de police)
- ICS Cybersecurity In-Depth (SANS) *niveau 3

Notes supplémentaires:

- Formation largement disponible qui complète les profils de compétences.

Tableau 13. Formation actuellement disponible pour les compétences relatives aux analystes de la cybercriminalité

	Compétences numérique et l'internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Analyste de la cybercriminalité*	3	3	2	3	2	4	4	4	2	3

Cours et compétences numériques Analystes de la cybercriminalité

Compétences numériques et l'internet (3)

- CompTIA A+ (CompTIA)

Cyber-hygiène et cybersécurité (3)

- Cybersécurité dans le camp d'entraînement du GC (Centre canadien pour la cybersécurité) * le camp d'entraînement progresse rapidement des concepts de base aux concepts avancés (niveau 2-3)
- Fondations – Informatique, technologie et sécurité (SANS) *Niveau 2/3 – propose des concepts informatiques, des principes de base des réseaux, des concepts de cybersécurité, une introduction à la criminalistique.
- Introduction à la cybersécurité (SANS)
- CompTIA Security + (CompTIA)

Cybercriminalité, prévention et assistance aux victimes (2)

- Enquêtes de base en ligne (RCSP – Service de police de Calgary)
- Aucune formation spécifique identifiée concernant l'assistance aux victimes et la prévention

Source ouverte (3)

- Utilisation de l'internet comme outil de recherche d'investigation (Toddington)
- Renseignement et enquête sur les médias sociaux (Toddington)
- Collecte et analyse de renseignements de source ouverte (OSINT) (SEC487) – SANS

Cyber légalités (2)

- Droit de la sécurité des données et des enquêtes (SANS) - Niveau 2/3
- Enquêtes sur l'internet - Niveau 1 - 2021 SYR APA-III-0812 (Collège de police de l'Atlantique)
- Technologies numériques pour les enquêteurs (Collège canadien de police) – Niveau 2/3
- Cours d'enquêteurs sur la cybercriminalité (Collège canadien de police)

Analyse des cyber données et du renseignement (4)

- Renseignements sur les cybermenaces (SANS)

Crypto-monnaie et Blockchain (3/4)

- Blockchain et Smart Contract Security (SANS) – Niveau 3
- Bien que les plateformes en ligne et les établissements d'enseignement en personne proposent des cours sur l'utilisation de la crypto-monnaie, aucune n'est destinée à l'application de la loi.

Programmation et scripts (2/3)

- Sécurité de base du réseau et de la base de données (IBM avec Edx)
- Fondamentaux de Blue Team : Opérations et analyse de sécurité (SANS)
- Principes de sécurité ICS/SCADA (SANS)
- L'éducation et la formation à la programmation et au script sont largement disponibles auprès des fournisseurs de cyberéducation privés et publics.

La criminalistique numérique (2)

- Preuve numérique : Enquêtes de première ligne (RCSP – Police régionale de York) – Niveau 1/2
- L'essentiel de la criminalistique numérique (SANS)
- Imagerie numérique criminalistique : documentation et présentation de visuels (Justice Institute of British Columbia)
- Divers fournisseurs de logiciels d'investigation numérique tels que Cellebrite et Magnet Forensics proposent une formation sur l'utilisation de leurs produits utilisés par les premiers intervenants.

La criminalistique du réseau (3)

- Analyse des preuves Internet (Collège canadien de police)
- Cours sur les techniques d'enquête en réseau (Collège canadien de police)
- Acquisition et analyse d'appareils mobiles (Collège canadien de police)
- Cloud Security Essentials (SANS)
- Atelier d'analyse en direct (Collège canadien de police)
- ICS Cybersecurity In-Depth (SANS) *Niveau 3

Notes complémentaires:

- Formation largement disponible qui complète les profils de compétences.

Tableau 14. Formation actuellement disponible pour les compétences relatives à l'examinateur criminalistique numérique

	Compétences numérique et l'internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Examinateur criminalistique numérique	4	4	2	3	3	3	4	3	5	5

Cours et compétences numériques Examinateur criminalistique numérique

Compétences numériques et l'internet (4)

- Divers cours Comp TIA, y compris A+, Network+ et Security+

Cyber-hygiène et cybersécurité (4)

- Tests de pénétration du réseau et piratage éthique (SANS)

Cybercriminalité, prévention et assistance aux victimes (2)

- Enquêtes de base en ligne (RCSP – Service de police de Calgary)
- Aucune formation spécifique identifiée concernant l'assistance aux victimes et la prévention

Source ouverte (3)

- Utilisation de l'internet comme outil de recherche d'investigation (Toddington)
- Renseignement et enquête sur les médias sociaux (Toddington)
- Collecte et analyse de renseignement source ouverte (OSINT) (SEC487) - SANS

Cyber légalités (3)

- Droit de la sécurité des données et des enquêtes (SANS) - Niveau 2/3* Droit américain, pas de cours de droit canadien équivalent
- Enquêtes sur l'internet - Niveau 1 - 2021 SYR APA-III-0812 (Collège de police de l'Atlantique)
- Technologies numériques pour les enquêteurs (Collège canadien de police) – Niveau 2/3
- Cours d'enquêteurs sur la cybercriminalité (Collège canadien de police)

Analyse des cyber données et du renseignement (3)

- Introduction à l'analyse du renseignement (Toddington) - Niveau 2/3
- Renseignements criminels (Analyse 202Eca) (Toddington) – Niveau 2/3
- Renseignement stratégique (Analyse 203E SA) (Toddington) – Niveau 2/3
- Renseignements sur les cybermenaces (SANS) - Niveau ¾

Crypto-monnaie et Blockchain (3/4)

- Blockchain et Smart Contract Security (SANS) – Niveau 3
- Bien que les plateformes en ligne et les établissements d'enseignement en personne proposent des cours sur l'utilisation de la crypto-monnaie, aucune n'est destinée à l'application de la loi.

Programmation et scripts (3)

- Sécurité de base du réseau et de la base de données (IBM avec Edx)
- Fondamentaux de Blue Team : Opérations et analyse de sécurité (SANS)
- Principes de sécurité ICS/SCADA (SANS)
- L'éducation et la formation à la programmation et au script sont largement disponibles auprès des fournisseurs de cyberéducation privés et publics.

La criminalistique numérique (4/5)

- Examinateurs en informatique judiciaire (Collège canadien de police)
- Champ de bataille et acquisition de données (SANS)
- Examinateur judiciaire en informatique (CMPFOR) (Collège canadien de police)
- Analyse criminalistique approfondie des smartphones (SANS)
- Formation avancée en criminalistique mobile JTAG (Justice Institute of British Columbia)
- Extraction Cellebrite JTAG et Décodage (Justice Institute of British Columbia)
- Examen TEEL Cellebrite sur appareil mobile de 5 jours (Justice Institute of British Columbia)

La criminalistique du réseau (Cloud) (4/5)

- Analyse avancée des réseaux et réponse aux incidents (SANS)
- Essentiels de sécurité avancés – Défenseur d'entreprise (SANS)
- Surveillance de la sécurité du cloud et détection des menaces (SANS)
- Tests de pénétration du réseau et piratage éthique (SANS)
- Développement d'exploits avancés pour la pénétration (SANS)

Notes supplémentaires:

- Formations et cours suffisants sur les compétences numériques de niveau supérieur en criminalistique numérique et en criminalistique de réseau. **Seul un petit échantillon des offres disponibles est répertorié ci-dessus.**

Tableau 15. Formation actuellement disponible pour les compétences relatives à l'enquêteur en matière de cybercriminalité

	Compétences numérique et l'internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Enquêteur de la cybercriminalité*	4	3	3	3	4	3	4	2	2	2

Cours et compétences numériques Enquêteur sur la cybercriminalité

Compétences numériques et l'internet (4)

- Divers cours Comp TIA, y compris A+, Network+ et Security+

Cyber-hygiène et cybersécurité (3)

- Cybersécurité dans le camp d'entraînement GC (Centre canadien pour la cybersécurité) * le camp d'entraînement progresse rapidement des concepts de base aux concepts avancés (niveau 2/3)
- Fondations – Informatique, technologie et sécurité (SANS) *Niveau 2/3 – propose des concepts informatiques, des principes de base des réseaux, des concepts de cybersécurité, une introduction à la criminalistique.
- Introduction à la cybersécurité (SANS)* Niveaux 2/3
- CompTIA Security + CompTIA

Cybercriminalité, prévention et assistance aux victimes (3)

- Expert certifié en cyber-enquêtes (McAfee Institute) *remarque : aborde certains sujets qui peuvent ne pas être aussi pertinents, par exemple la criminalité dans le commerce de détail.
- Aucune formation identifiée traitant spécifiquement de l'assistance aux victimes de la cybercriminalité.

Source ouverte (3)

- Utilisation de l'Internet comme outil de recherche d'investigation (Toddington)
- Renseignement et enquête sur les médias sociaux (Toddington)
- Collecte et analyse de renseignements de source ouverte (OSINT) (SEC487) – SANS

Cyber légalités (4)

- Droit de la sécurité des données et des enquêtes (SANS) - Niveau 2/3 * Droit américain, pas de cours de droit canadien équivalent
- Enquêtes sur l'internet - Niveau 1 - 2021 SYR APA-III-0812 (Collège de police de l'Atlantique)
- Technologies numériques pour les enquêteurs (Collège canadien de police) – Niveau 2/3
- Cours d'enquêteurs sur la cybercriminalité (Collège canadien de police)

Analyse des cyber données et du renseignement (3)

- Introduction à l'analyse du renseignement (Toddington) * Niveau 2/3
- Renseignements criminels (Analyse 202Eca) (Toddington) *Niveau 2/3
- Renseignement stratégique (Analyse 203E SA) (Toddington) *Niveau 2/3
- Renseignement sur les cybermenaces (SANS) * Niveau 3/4

Crypto-monnaie et Blockchain (3/4)

- Blockchain et Smart Contract Security (SANS) *Niveau 3
- Bien que les plateformes en ligne et les établissements d'enseignement en personne proposent des cours sur l'utilisation de la crypto-monnaie, aucune n'est destinée à l'application de la loi.

Programmation et scripts (2)

- Sécurité de base du réseau et de la base de données (IBM with edx)
- L'éducation et la formation à la programmation et au script sont largement disponibles auprès des fournisseurs de cyberéducation privés et publics.

La criminalistique numérique (2)

- Preuve numérique : Enquêtes de première ligne (RCSP – Police régionale de York) – Niveau 1/2
- L'essentiel de la criminalistique numérique (SANS)
- Imagerie numérique criminalistique : documentation et présentation de visuels (Justice Institute of British Columbia)
- Divers fournisseurs de logiciels d'investigation numérique tels que Cellebrite et Magnet Forensics proposent une formation sur l'utilisation de leurs produits utilisés par les premiers intervenants.

La criminalistique du réseau (Cloud) (2)

- Sécurité de base du réseau et de la base de données (IBM by Edx)
- Introduction aux réseaux et au matériel informatique (Association internationale des chefs de police)
- Réseau+ CompTIA *Niveau 2/3

Notes complémentaires:

- Formation largement disponible qui complète les profils de compétences.

Tableau 16. Formation actuellement disponible pour les compétences relatives aux gestionnaires et aux dirigeants

	Compétences numérique et l'internet	Cyber Hygiène – Cyber sécurité	Sensibilisation à la cybercriminalité, prévention et assistance aux victimes	Renseignement de source ouverte et collecte de preuves	Cyber légalités	Analyse des cyber données et du renseignement	Crypto-monnaie et Blockchain	Programmation et scripts	La criminalistique numérique	La criminalistique du réseau (Cloud)
Gestionnaire/dirigeant *	3	3	3	2	4	2	2		2	2

Cours et compétences numériques Cybergestionnaires et dirigeants

Compétences numériques et l'internet (3)

- CompTIA A+ (CompTIA)

Cyber-hygiène et cybersécurité (3)

- Cybersécurité dans le camp d'entraînement GC (Centre Canadien pour la cybersécurité) *le camp d'entraînement progresse rapidement des concepts de base aux concepts avancés (Niveau 2/3)
- Fondations – Informatique, technologie et sécurité (SANS) *Niveau 2/3 – propose des concepts informatiques, des principes de base des réseaux, des concepts de cybersécurité, une introduction à la criminalistique.
- Introduction à la cybersécurité (SANS)* Niveaux 2/3
- CompTIA Security + CompTIA

Cybercriminalité, prévention et assistance aux victimes (4)

- Conduire le changement en matière de cybersécurité : Construire une culture basée sur la sécurité (SANS)
- Aucune formation identifiée traitant spécifiquement de l'assistance aux victimes de la cybercriminalité

Source ouverte (2)

- Utilisation de l'internet comme outil de renseignement (UIOR) (Collège canadien de police)
- Enquêtes sur la cybercriminalité de niveau 1 (RCSP – Police régionale d'Halifax)
- Enquêtes sur l'internet - Niveau 2 (Holland College)
- Enquêtes sur l'internet - LITE (Holland College)
- Le guide Facebook pour les enquêteurs (Holland College)

Cyber légalités (3/4)

- Droit de la sécurité des données et des enquêtes (SANS) – niveau 2/3 *Droit américain, pas de cours de droit canadien équivalent
- Enquêtes sur l'internet – Niveau 1 – 2021 SYR APA-III-0812 (Collège de police de l'Atlantique)
- Technologies numériques pour les enquêteurs (Collège canadien de police) – Niveau 2/3
- Cours d'enquêteurs sur la cybercriminalité (Collège canadien de police)

Analyse des cyber données et du renseignement (2)

- Introduction à l'analyse du renseignement (Toddington) *Niveau 2/3
- Renseignements criminels (Analyse 202Eca) (Toddington) *Niveau 2/3
- Renseignement stratégique (Analyse 203E SA) (Toddington) *Niveau 2/3

Crypto-monnaie et Blockchain (2)

- Bien que les plateformes en ligne et les établissements d'enseignement en personne proposent des cours de sensibilisation et de compréhension de la crypto-monnaie, aucun n'est destiné aux forces de l'ordre.

La criminalistique numérique (2)

- Preuve numérique : Enquêtes de première ligne (RCSP – Police régionale de York) – Niveau 1/2
- L'essentiel de la criminalistique numérique (SANS)
- Imagerie numérique criminalistique : documentation et présentation de visuels (Justice Institute of British Columbia)
- Divers fournisseurs de logiciels d'investigation numérique tels que Cellebrite et Magnet Forensics proposent une formation sur l'utilisation de leurs produits utilisés par les premiers intervenants.

La criminalistique du réseau (Cloud) (2)

- Sécurité de base du réseau et de la base de données (IBM by Edx)
- Introduction aux réseaux et au matériel informatique (Association internationale des chefs de police)
- Réseau + CompTIA * Niveau 2/3

Notes complémentaires:

- Formation insuffisante en compétences numérique et de l'internet, prévention de la cybercriminalité et assistance aux victimes, crypto-monnaie et blockchain et criminalistique des réseaux au niveau prescrit.

5.2. Analyse des écarts de formation

Malgré les limites du sondage sur la formation, un examen des formations facilement disponibles a identifié les thèmes suivants pour chacune des compétences numériques :

Compétences numériques et l'internet

- Il existe un large éventail de formations disponibles, notamment sur les plateformes en ligne.
- Une grande partie de la formation en ligne dans le domaine des compétences numériques n'est pas structurée.
- La formation en Compétences numérique n'exige pas un objectif d'application de la loi à des niveaux de compétence inférieurs.
- Il y a des manques de formations au niveau de base.

Cyber-hygiène et cybersécurité

- Des ressources en ligne autodirigées sont offertes à un niveau de base.
- La formation disponible en cyber-hygiène avec un objectif d'application de la loi fait défaut, en particulier aux niveaux de compétence inférieurs.
- La formation formelle semble se limiter aux niveaux supérieurs de cybersécurité.
- La formation coûte cher.
- Le secteur privé et les établissements d'enseignement publics offrent une certification de formation en cybersécurité.

Cyber légalités

- Peu de formation offerte à tous les niveaux – portant spécifiquement sur le droit canadien.
- La formation sur les témoins experts est offerte uniquement par le Collège canadien de police - Institut d'apprentissage technique sur la criminalité.

Assistance aux victimes

- Peu de formation offerte à tous les niveaux.
- Certains des cours fondamentaux d'enquête et d'entretien traitent de la manière de parler aux victimes et aux témoins. Aucun, cependant, n'est spécifiquement destiné aux victimes de la cybercriminalité.
- Aucun des cours offerts par les établissements d'enseignement de la police canadienne ne comprend de programme d'études sur l'aide aux victimes.

La criminalistique numérique

- La formation et les cours font défaut aux niveaux les plus élémentaires.

- Formation approfondie offerte à des niveaux de compétence plus élevés par des établissements de formation de la police et des prestataires de formation du secteur privé.

Analyse des cyber données et du renseignement

- La formation et les cours font défaut aux niveaux les plus élémentaires.
- Formation avancée offerte par les établissements de formation de la police et les prestataires de formation du secteur privé.
- Les collèges et universités offrent une vaste gamme de cours et de programmes en analyse de données.

Crypto-monnaie et Blockchain

- Il y a un manque à tous les niveaux dans la formation de l'utilisation et des connaissances à la crypto-monnaie et à la blockchain dans un contexte de l'application de la loi.
- De nombreux collèges et universités, y compris des plateformes d'apprentissage en ligne (Udemy, Coursera, etc.), proposent des cours sur la théorie et l'utilisation de la crypto-monnaie et de la blockchain aux niveaux débutant à avancé.

Programmation et scripts

- Des cours sur la programmation et le script à tous les niveaux sont largement disponibles dans les universités, les collèges et les prestataires du secteur privé.

La criminalistique numérique

- Peu d'opportunités de formation à des niveaux de compétence inférieurs
- Large gamme de formations offertes par les établissements de formation de la police, les établissements d'enseignement publics et les prestataires du secteur privé.

La criminalistique du réseau

- Peu d'opportunités de formation à des niveaux de compétence inférieurs
- Large gamme de formations offertes par les établissements de formation de la police, les établissements d'enseignement publics et les prestataires du secteur privé.

Il semble qu'il existe de nombreuses possibilités de formation pour ces rôles considérés comme spécialistes. Plus précisément, les techniciens intermédiaires liés à la cybercriminalité, les examinateurs criminalistiques numériques, les enquêteurs sur la cybercriminalité, les analystes de la cybercriminalité et les enquêteurs en ligne. Le Collège canadien de police (CCP), par exemple, par l'intermédiaire de L'institut d'apprentissage en criminalité informatique (IACI), offre une formation hautement spécialisée en examen criminalistique numérique, en enquête sur la cybercriminalité et en collecte de renseignements à source ouverte. Ces cours satisfont à la plupart des exigences de formation des rôles de spécialiste mentionnés ci-dessus. Les cours IACI constituent les principales exigences de formation du programme de doublure d'examinateur judiciaire en informatique de la GRC.

Tableau 17. Cours spécialisés offerts par l'institut d'apprentissage technique du crime du collège canadien de police

Criminalistique	Cybercriminalité – Crime cyber activé
● Examinateur judiciaire en informatique ● Analyse des preuves Internet ● Techniques d'enquête de réseau ● Acquisition et analyse d'appareils mobiles ● Atelier d'analyse en direct ● Atelier d'analyse du registre ● Expert du tribunal technique et témoignage	● Technologies numériques pour les enquêteurs ● Cours d'enquêteurs sur la cybercriminalité ● Utilisation de l'internet comme outil de renseignement ● Cours avancé d'intelligence à source ouverte ● Exploitation des enfants sur l'internet au Canada ● Exploitation avancée des enfants sur l'internet ● Cours de chercheur pair à pair

Source: (Canadian Police College, 2021)

Les cours spécialisés offerts par le CCP-IACI sont complétés par de nombreux fournisseurs du secteur privé tels que l'Institute SANS, qui offre également de nombreux cours techniques spécialisés.

L'acquisition de compétences dans les rôles cybernétiques spécialisés va au-delà de la participation à des cours. Les rôles hautement spécialisés tels que les examinateurs criminalistiques numériques nécessitent également un mentorat (Baron & Le Khac, 2021, p. 15). Des rôles moins spécialisés, cependant, peuvent éventuellement atteindre le niveau de compétence 1 ou 2 grâce à l'éducation seulement. Néanmoins, c'est dans ces domaines que les possibilités de formation sont insuffisantes ou incomplètes.

Considérez les rôles du premier intervenant et de l'enquêteur/détective général : l'omniprésence des preuves numériques, associée à la nature changeante de la criminalité, signifie qu'en termes de volume, les agents de première ligne sont sans doute les plus exposés aux incidents qui se situent sur le cyber-spectre. . Bien que les services de police individuels en partenariat avec le RCSP aient élaboré une cyberformation destinée aux premiers intervenants, il n'existe pas d'options de formation largement et facilement disponibles pour les premiers intervenants ou les détectives aux fonctions générales qui remplissent la totalité de la compétence identifiée par le biais d'un cours unique ou d'une offre de cours modulaire.

Présentement, les organismes canadiens d'application de la loi doivent envoyer leurs premiers intervenants et détectives aux fonctions générales suivre plusieurs cours pour atteindre les niveaux de compétence recommandés, un exploit qui dépasse sans aucun doute la capacité physique et financière de tout service.

6. Recommandations

Les recommandations suivantes sont basées sur la recherche concernant la pratique mondiale, les consultations des groupes de discussion, l'enquête sur les opportunités de formation et l'analyse des lacunes en matière de formation :

1. **Renforcer les capacités de formation pour les cyber-rôles non spécialisés.**

   La formation liée à la cybersécurité pour les cyber-rôles non spécialisés nécessite des investissements pour améliorer la capacité de formation et l'acquisition de compétences. L'omniprésence des preuves numériques et la nature changeante de la criminalité nécessitent une approche unifiée de la part des forces de l'ordre canadiennes pour renforcer la capacité de première ligne à faire face aux problèmes liés à la cybersécurité.

   Principalement dirigée par le CPC-TCLI et des prestataires du secteur privé tels que le SANS Institute, la formation pour des rôles spécialisés aux niveaux de compétence 3 et 4 est déjà bien établie.

2. **Créer une formation en cyber-hygiène facilement accessible avec un programme basé sur le profil de compétences de tous les membres du service de police.**

   En se concentrant sur la cyber-hygiène de base, ce cours de courte durée doit être conçu pour une diffusion à haut volume et accessible.

3. **Reconstruire la formation du RCSP sur les enquêtes sur la cybercriminalité avec un programme basé sur le profil de compétences des premiers intervenants.**

   Le profil de compétences pour les premiers intervenants présente des éléments tels que l'assistance aux victimes et la sensibilisation à la crypto-monnaie qui ne sont pas inclus dans la version actuelle Enquêtes sur la cybercriminalité Niveau 1. La version reconstruite pourrait être dispensée sous forme de cours unique ou à travers plusieurs modules axés sur une ou plusieurs compétences. Le programme du module pourrait inclure le cours Digital Evidence: Frontline Investigations en tant que module. L'achèvement des modules requis entraînerait l'achèvement des exigences de compétence des premiers intervenants ou des enquêteurs/détectives aux fonctions générales. Ce cours doit être conçu pour une livraison à haut volume facilement accessible.

4. **Créer une cyberformation facilement accessible avec un programme basé sur le profil de compétences des enquêteurs/détectives des fonctions générales.**

   Les cybercrimes de haut volume et les crimes cyber activés, tels que le vol d'identité et les fraudes en ligne, font généralement l'objet d'enquêtes par des détectives locaux dans des détachements ou des divisions. Le profil de compétences des enquêteurs/détectives aux fonctions générales requiert des compétences au-delà de celles recommandées pour les premiers intervenants. Ce cours devrait s'appuyer sur les concepts et le programme du cours reconstruit de niveau 1 sur les enquêtes sur la cybercriminalité.

5. **Travailler avec des partenaires pour créer des modules d'aide aux victimes avec des programmes basés sur les niveaux de compétence 1 et 2.**

Il existe très peu de formations sur l'assistance aux victimes de la cybercriminalité. Ces modules compléteront à la fois les rôles spécialisés et non spécialisés et introduiront une approche centrée sur la victime pour les cyberenquêtes.

6. **Travailler avec des partenaires pour créer ou identifier une formation en crypto-monnaie et en blockchain pour les forces de l'ordre avec des programmes de compétences de niveaux 1, 2 et 3.**

   Il existe très peu de formations disponibles dans ce domaine qui a une optique d'application de la loi opérationnelle. Cette formation peut être bien adaptée à une approche modulaire pour chaque niveau de compétence.

7. **Continuer d'assurer la liaison avec le Comité des cybercrimes de l'ACCP et le Comité des services de police nationaux sur la cybercriminalité pour l'examen, l'évaluation et la validation annuels du dictionnaire et des profils de compétences numériques.**

   Bien que le dictionnaire de compétences et les profils de compétences aient été conçus pour être évolutifs, l'évaluation continue de la validité et de l'exhaustivité d'une compétence est un élément essentiel de tout cadre de gestion basée sur les compétences. En tant que principaux organes de gouvernance de la cybercriminalité au Canada, le Comité de l'ACCP sur la cybercriminalité et le Comité de la cybercriminalité des Services nationaux de police sont bien placés pour fournir une évaluation et une validation annuelles des profils de compétences numériques.

8. **Poursuivre l'évaluation des cours et de la cyberformation pour s'assurer qu'ils contiennent des programmes d'études valides fondés sur les compétences.**

   Un corollaire de la recommandation 7 est que les modifications apportées au dictionnaire des compétences peuvent nécessiter des modifications au programme de formation ou de cours.

9. **Envisager des partenariats avec des établissements d'enseignement publics ou des prestataires du secteur privé.**

   De nombreux établissements d'enseignement publics et prestataires de formation du secteur privé sont actifs dans le domaine de la cyberformation. Des cours et des formations peuvent déjà exister ou nécessiter des ajustements mineurs pour s'adapter au contexte d'application de la loi. Les partenariats avec les fournisseurs de cyberformation existants peuvent également donner accès à une multitude d'experts en la matière.

7. Références bibliographiques

Armstrong, P. (2021, 06 04). *Center for Teaching - Bloom's Taxonomy*. Retrieved from Vanderbuilt University: https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/

Association of Police and Crime Commissioners. (2020). *National Policing Digital Strategy. Digital, Data and Technology Strategy 2020 - 2030.* London: Association of Police and Crime Commissioners. Retrieved 06 05, 2021, from https://www.apccs.police.uk/media/4886/national-policing-digital-strategy-2020-2030.pdf

Baron, A., & Le Khac, N. A. (2021, 08 08). *Cybercrime Competencies – A Training and Education Perspective.* University College Dublin, School of Computer Science and Infomatics. Dublin: University College Dublin.

Canadian Police College. (2021, 04 22). *Technical Crime Learning Institute*. Retrieved 06 02, 2021, from Canadain Police College: https://www.cpc-ccp.gc.ca/programs-programmes/technological-technologique/index-eng.htm#a1

Canadian Police Knowledge Network. (2020, 03 23). *Competencies Dictionary*. Retrieved 05 25, 2021, from Canadian Police Knowledge Network - Community of Practice: https://lms.cpkn.ca/goto.php?target=wiki_417

Canadian Police Knowledge Network. (2020). *White Paper Competency-Based Policing in Canada: An Integal Component for Transparency and Accountable Policing.* Charlettown, Prince Edward Island: Canadian Police Knowledge Network.

Carnegie Mellon University. (2018). *Cyber Investigator Certificate Program*. Retrieved from FBI - CICP: https://fbi-cicp.cert.org/lms

Council of Europe. (2001, November 23). Convention on Cybercrime. *European Treaty Series - No. 185.* Budapest: Council of Europe.

European Commission. (2019, 06 06). *Press Release: Security Union: Commission receives mandate to start negotiating international rules for obtaining electronic evidence.* Retrieved from European COmmission - Press Corner: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2891

European Cybercrime Training and Education Group. (2020, August 27). *Cybercrime Training Competencies Framework Introduction.* Retrieved from Cybercrime Training Competency Framework: https://www.ecteg.eu/tcf/co/TCG_OpaleModule_4.html

European Cybercrime Training and Education Group. (2021, February 08). *E-FIRST: First Responders E-Learning Package*. Retrieved from European Cybercrime Training and Education Group: https://www.ecteg.eu/running/first-responders/

Europol. (2018). *Internet organized Crime Threat Assessment (IOCTA) 2018.* The Hauge : European Union Agency for Law Enforcemet Cooperations.

Federal Bureau of Investigation. (2016, October 19). *National Cyber Security Awareness Month.* Retrieved from Federal Bureau of Investigation: https://www.fbi.gov/news/stories/online-cyber-training-for-law-enforcement-first-responders

Government of Canada. (2020, 12 02). *Skills and Competencies Taxonomy*. Retrieved 06 04, 2021, from Government of Canada: https://noc.esdc.gc.ca/SkillsTaxonomy/SkillsTaxonomyWelcome

Greenwood, K. (2020, December). Policing, Competencies, and Building a New Normal. *Canadian Police Chief Magazine*, pp. 12-13.

Her Majesty's Inspectorate of Constabulary. (2015). *Real lives, real crimes: A study of digital crime and policing.* London: Her Majesty's Inspectorate of Constabulary. Retrieved from https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf

Kowalski, M. (2002). *Cyber-Crime: Issues, Data Sources, and Feasibility of Collecting Police-Reported Statistics.* Ottawa: Statistics Canada, Canadian Centre for Justice Statistics.

Lincolnshire Constabulary. (2021, February 02). *Lincolnshire Police Cyber Crime Strategy.* Retrieved from Lincolnshire Police: https://www.lincs.police.uk/media/252353/cyber-crime-strategy.pdf

Manhattan District Attorney's Office. (2021, February 01). *Our Work: Cybercrime*. Retrieved from Manhattan District Attoney's Office: https://www.manhattanda.org/our-work/cybercrime/

Mazowita, B., & Vezina, M. (2014, September 25). Police-reported cybercime in Canada, 2012. *Juristat*.

NW3C. (2021, February 9). *NW3C Certifications*. Retrieved from NW3C: https://www.nw3c.org/certifications/AssessmentResults#certificationassessment

Ontario Provincial Police (1). (2016). *From Frontline to Online OPP Cyber Stategy.* Unpublished.

Ontario Provincial Police (2). (2016). *Ontario Provincial Police Cybercrime Strategy: From Frontline to Online.* Orillia, ON: Ontario Provincial Police.

Robertson, J. G. (2019). *The Impact of Digital Society on Police Recuit Training in Canada.* Ontario Tech University, Faculty of Education. Oshawa: Ontairio Technical University.

Royal Canadian Mounted Police. (2015). *Royal Canadian Mounted Police Cybercrime Strategy.* Ottawa: Her Majesty the Queen in Right of Canada as represented by the Royal Canadian Mounted Police.

Royal Canadian Mounted Police. (2021, January 27). *Cybercrime:an overview of incidents and issues in Canada*. Retrieved from Royal Canadian Mounted Police: https://www.rcmp-grc.gc.ca/en/cybercrime-an-overview-incidents-and-issues-canada#sec2

Siden, D. (2017, July 4). Meaningful Evidence. Non-Specialists trained to triage digital devices. *Gazette Magazine Vol 79 No 3.*, p. 16.

Sobusial-Fischanaller, M., & Vandermeer, Y. (2016). *Cybercrime Training Governance Model: Cybercrime Training Competency Framework.* Retrieved from Council of Europe: https://rm.coe.int/3148-2-3-ecteg-16-cy-train-module/1680727f34

Statistics Canada. (2019, November 08). *Canadian Internet Use Survey*. Retrieved from Statistics Canada: https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-eng.htm

Statistics Canada. (2021, January 25). *Police-reported cybercrime, by cyber-related violation, Canada (selected police services)*. Retrieved from Statistics Canada: https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510000101

Statistics Canada. (2021, February 04). *Table 22-10-0083-01 Internet use by province*. Retrieved from Statistics Canada: https://doi.org/10.25318/2210008301-eng

Statistics Canada. (2021, February 02). *Telecommunications: Connecting Canadains*. Retrieved from Statistics Canada: https://www.statcan.gc.ca/eng/subjects-start/digital_economy_and_society/telecommunications

Thatcher, A. (2017, July 4). Cybercime on the front line. *Gazett Magazine*, p. 17.

The Council of Europe. (2020). *Budapest Convention and related standards*. Retrieved from Council of Europe: https://www.coe.int/en/web/cybercrime/the-budapest-convention

The Expert Panel on the Future of Canadian Policing Models. (2014). *Policing Canada in the 21st Century: New Polcing for New Challenges.* Ottawa: The Council of Canadian Academies.

University of Waterloo. (2021, 06 04). *Bloom's Taxonomy. Centre for Teaching Excellence,* . Retrieved from University of Waterloo.

CANADIAN POLICE KNOWLEDGE NETWORK
RÉSEAU CANADIEN DU SAVOIR POLICIER
www.cpkn.ca