prompt

Portrait du secteur de la cybersécurité au Québec

8 octobre 2024

Mis à jour: février 2025

En collaboration avec

IN·SEC·M
LA GRAPPE CANADIENNE DE LA CYBERSÉCURITÉ

cyber eco
Écosystème en cybersécurité

Table des matières

Mot de la directrice générale 4
COLLABORATEURS 5
INTRODUCTION 6
Présentation de l'initiative et de ses objectifs 6
Mise en contexte 6
L'industrie de la cybersécurité 7
1. PORTRAIT DE LA CYBERSÉCURITÉ DANS LE MONDE ET AU QUÉBEC (REVUE DE LITTÉRATURE) .. 11
1.1 Sources des données et méthodologie 11
1.2 Le marché mondial de la cybersécurité et les trois méga-grappes 12
1.3 La demande de cybersécurité au Canada et au Québec 13
1.4 Retombées économiques de l'industrie de la cybersécurité au Canada et au Québec 15
1.5 La main-d'œuvre en cybersécurité 16
2. PORTRAIT DES ENTREPRISES QUÉBÉCOISES DE CYBERSÉCURITÉ 18
2.1 L'offre des entreprises et leurs domaines d'activités 18
2.2 Nombre d'employés et caractéristiques de la main d'œuvre 22
2.3 Répartition géographique des entreprises 24
2.4 Historique des entreprises et profitabilité de leurs activités 24
2.5 Intensité des activités de recherche et de développement (R&D) 26
3. ÉCOSYSTÈME INSTITUTIONNEL DE LA CYBERSÉCURITÉ AU QUÉBEC 27
3.1 Entreprises de cybersécurité 28
3.2 Acheteurs privés 29
3.3 Assureurs 30
3.4 Acheteurs publics 31
3.5 Investisseurs & infrastructures d'incubation et d'accélération 32
3.6 Organismes de soutien à la cybersécurité 33
3.7 Organismes de formation et de recherche (monde académique) 34
3.8 Autorités régulatrices 35
3.9 Associations professionnelles et initiatives bénévoles 38
3.10 Quelques éléments de comparaison avec des écosystèmes de calibre mondial 39
4. DÉFIS ET OPPORTUNITÉS POUR L'INDUSTRIE DE LA CYBERSÉCURITÉ AU QUÉBEC 42
4.1 Talents et main-d'œuvre qualifiée 42

4.2 La recherche et l'innovation en cybersécurité au Québec 44
4.3 Le financement de l'innovation 44
4.4 Commercialisation : enjeux et défis 46
4.5 Portrait FFOM synthèse 47
5. SIX PISTES DE RÉFLEXION 49
5.1 Fragmentation de l'écosystème 49
5.2 Données incomplètes sur l'industrie et l'écosystème 49
5.3 Accès des PME de l'industrie aux marchés publics 50
5.4 Le soutien et la valorisation internationale des entreprises locales 51
5.5 Un ciblage de l'aide gouvernementale 51
5.6 Collaborations entre industriels et universitaires 52
CONCLUSION 53
RÉFÉRENCES 54
ANNEXE 1 : écosystèmes de la cybersécurité à l'international 57
Écosystème israélien 57
Écosystème français 60
Écosystème américain 62
Écosystème allemand 65
ANNEXE 2 : cartographie de l'écosystème du Québec 69

Mot de la directrice générale

Les études indiquent que la cybersécurité souffre d'une pénurie de 4 millions de talents au niveau mondial[1] et que le coût de la cybercriminalité atteindra 10 500 milliards de dollars US d'ici 2025[2].

En réaction à cette menace sans précédent, l'écosystème de la cybersécurité québécois s'est développé rapidement au cours des dernières années. Les grandes entreprises ainsi que les grandes firmes de consultation les épaulant ont recruté des experts en grand nombre. Des programmes de formation ont vu le jour dans les universités québécoises. Alors que la demande croît à grande vitesse, dans un contexte où les menaces se multiplient, et que la conscientisation du public et des entreprises augmente sur la nécessité de devenir cyber-résilient, des entreprises d'ici prennent leur place dans ce marché.

On estime que 101,5 milliards de dollars US seront dépensés auprès de fournisseurs de services en cybersécurité d'ici 2025[3]. Voilà un domaine technologique qui évolue rapidement et auquel Prompt, étant donné son rôle de regroupement sectoriel de recherche industrielle en technologies numériques, se devait de s'intéresser. C'est ce qu'il fait, depuis 2019, par ses programmes de financement de l'innovation et de certifications en cybersécurité.

Toutefois, il existe encore très peu de données sur l'industrie québécoise de la cybersécurité, sur ses enjeux et ses besoins. C'est la raison pour laquelle Prompt, avec comme collaborateurs des joueurs clé de l'écosystème, a élaboré ce portrait de l'industrie. Ce portrait vise à mieux connaître les entreprises du secteur, leurs besoins et leurs enjeux, ainsi que l'écosystème dans lequel elles évoluent. Il permet une base de compréhension commune qui facilitera la réflexion et la recherche de solutions afin d'appuyer encore plus efficacement cet écosystème d'une importance stratégique indéniable pour le Québec.

Je vous en souhaite une bonne lecture,

Liette Lamonde

Directrice générale, Prompt

[1] "Cybersecurity Workforce Study 2023", ISC2
[2] Cybersecurity Ventures 2023
[3] "Cybersecurity trends: Looking over the horizon", McKinsey & Company, mars 2022.

COLLABORATEURS

Ce portrait est le fruit de plusieurs collaborations et collaborateurs.

Prompt remercie pour leur apport à la rédaction :

- Daniel J. Caron, professeur à l'École nationale d'administration publique
- Benoît Dupont, professeur titulaire à l'École de criminologie de l'Université de Montréal et titulaire de la Chaire de recherche du Canada en Cyber-résilience et de la Chaire de recherche en Prévention de la cybercriminalité
- Nicolas Duguay, co-directeur général d'In-Sec-M
- Pascal Fortin, président et directeur général de Cybereco

Pour leur rétroaction sur la première version et leur apport en intelligence et au financement de l'étude :

- le ministère de l'Économie, de l'Innovation et de l'Énergie
- le ministère de la Cybersécurité et du Numérique.

Enfin, nous remercions tout particulièrement tous les membres de l'écosystème de la cybersécurité québécois (CISO, experts, consultants, etc.) qui nous ont gracieusement accordé de leur temps en répondant au sondage et lors de nombreuses rencontres et discussions formelles et informelles.

INTRODUCTION

Présentation de l'initiative et de ses objectifs

Dès juillet 2023, Prompt a entrepris une enquête en vue de la réalisation d'un portrait des entreprises du secteur de la cybersécurité au Québec afin de mieux connaître l'offre québécoise de produits et services en cybersécurité ainsi que l'écosystème qui soutient ce secteur.

Ce portrait se décline en cinq sections, présentées dans ce rapport. La première section est une revue de la littérature québécoise, canadienne et internationale sur le marché de la cybersécurité et ses dynamiques. La deuxième section fait ressortir quelques données sur les principaux acteurs du secteur en s'appuyant sur une cartographie des entreprises offrant des produits et des services de cybersécurité, ainsi que sur un sondage auprès d'une cinquantaine de ces entreprises. La troisième section approfondit ce panorama en examinant les grands acteurs publics, privés et communautaires qui composent l'écosystème québécois de la cybersécurité et qui permettent au marché d'acquérir de nouveaux talents, de développer des produits innovants, ou encore de bénéficier de politiques publiques et de cadres réglementaires incitatifs. La quatrième section analyse les défis et opportunités de la cybersécurité au Québec. Finalement, la cinquième section explore quelques éléments de réflexion susceptibles de renforcer l'industrie québécoise.

Mise en contexte

Chaque jour, les médias mettent en évidence les périls associés à l'omniprésence des technologies numériques dans chaque aspect de notre vie quotidienne. Les brèches de données qui affectent des millions de consommateurs, les attaques par rançongiciel qui paralysent des entreprises de toutes tailles pendant de longues semaines, ou encore les campagnes d'ingérence étrangère qui interfèrent avec le bon déroulement des processus électoraux, représentent quelques exemples d'un vaste répertoire de dommages numériques venant empêcher les citoyens, les entreprises et les organismes publics de tirer pleinement profit de la Révolution numérique et des taux élevés de connectivité disponibles au Canada et au Québec[4]. Dans le contexte post-pandémique où les entreprises ont radicalement accéléré la numérisation de leurs activités et où de nombreux employés continuent à travailler en mode hybride, la prolifération des risques numériques peut nuire à la prospérité de notre économie et au bien-être de la population.

Dans la plus grande enquête représentative des entreprises menée à ce jour, Statistique Canada a constaté qu'en 2019, 21 % des entreprises canadiennes avaient été touchées par au moins un incident de cybersécurité qui avait empêché les employés de mener leurs activités quotidiennes et généré des pertes financières et des atteintes à la réputation. Cette exposition au risque ne s'est pas améliorée ces dernières

[4] Voir à cet égard les statistiques canadiennes de 94% de la population utilisant internet en 2022, par comparaison avec une moyenne mondiale de 67,4%, de 90,5% en Europe, et de 97,1% aux États-Unis. Voir la page de l'Union internationale des télécommunications, repérée à https://datahub.itu.int/data/?e=CAN&c=701&i=11624.

années, malgré des dépenses en cybersécurité estimées à 9,7 milliards de dollars par an au Canada en 2021 (Statistique Canada, 2022). Les petites et moyennes entreprises (PME), qui constituent l'essentiel du tissu économique québécois, sont particulièrement exposées aux cyber-risques, accusant un retard dans le déploiement des mesures de protection les plus élémentaires en raison de défis organisationnels et technologiques (Berry et Berry 2018).

La cybersécurité est un terme qui a fait son apparition à la fin des années 2000 (Bouchard et Henri, 2023). Celle-ci « peut être définie au sens large comme la pratique consistant à se protéger et à protéger son organisation contre les attaques numériques » (Quan et Herron, 2022). Depuis son apparition, la cybersécurité n'a cessé de prendre de l'importance étant donné le caractère essentiel des technologies numériques dans le fonctionnement de la société actuelle.

Les professionnels de la cybersécurité ont vu évoluer la terminologie utilisée pour encadrer leurs offres de services et de produits, passant de la sécurité informatique dans les années 1960 à la sécurité de l'information dans les années 2000, le préfixe cyber s'imposant largement dans les années 2010 (Landwehr, 2010). Cette évolution ne reflète pas seulement les nouvelles tendances lancées par des entrepreneurs désireux de différencier leur solution de celle de leurs concurrents. Elle dénote également l'élargissement du champ d'action de la cybersécurité, qui a dépassé son intérêt initial restreint à la sécurité des machines pour intégrer progressivement des considérations sur les informations stockées et traitées par ces machines, et finalement les humains et les institutions qui interagissent avec celles-ci (Dupont et Whelan, 2022).

Dans un tel contexte, l'industrie de la cybersécurité joue donc aujourd'hui un rôle central dans la protection des infrastructures critiques et des technologies numériques qui constituent le moteur de notre prospérité et permettent à notre économie de rester compétitive à l'échelle mondiale. Il apparaît dès lors nécessaire, afin de mieux comprendre les facteurs qui influencent son développement et de mettre en œuvre des mécanismes de soutien efficaces, de dresser un état de la situation. Le présent rapport réunit ainsi diverses sources de données primaires et secondaires afin de dresser le portrait le plus complet possible de l'industrie de la cybersécurité au Québec, pour lequel les informations étaient jusqu'à présent parcellaires et fragmentées. En raison de la nature des données disponibles, ce document comporte certaines limites en termes de représentativité des résultats que nous soulignerons lorsque pertinent. Il offre néanmoins de précieuses informations sur l'état actuel et l'évolution de cette industrie, grâce à la pleine collaboration des principaux acteurs de cette industrie.

L'industrie de la cybersécurité

Une industrie est typiquement définie comme un groupe d'entreprises ou de commerces qui produisent ou fournissent des biens, des services ou des sources de revenu qui sont reliés à leurs activités commerciales principales. En ce sens, les diverses entreprises qui offrent des produits et des services de cybersécurité peuvent être considérées comme une industrie.

Celle-ci englobe une large gamme d'activités, de produits et de services conçus pour protéger les réseaux, les dispositifs informatiques, les programmes et les données contre les attaques, les dommages ou les

accès non autorisés. Les principaux critères qui définissent une industrie sont examinés ci-dessous dans le contexte particulier de la cybersécurité afin de déterminer son niveau de maturité :

Produits et services spécifiques	Cette industrie offre des produits et services distincts, tels que les logiciels antivirus, les pare-feu (et autres équipements de protection réseau), la surveillance de sécurité, l'analyse des menaces, la formation en sécurité informatique et les services de conseil en sécurité, qui sont spécifiquement conçus pour répondre aux besoins de sécurité informatique des organisations et des individus.	
Marché commun	Les entreprises au sein de l'industrie desservent le même marché ou la même base de clients, bien qu'elles puissent cibler différents segments de ce marché. Elles se disputent le même groupe de clients. La demande pour la cybersécurité est en augmentation constante à travers le monde, en raison de la numérisation croissante des entreprises et de la société en général. Cette croissance est alimentée par l'augmentation des menaces cybernétiques et par la prise de conscience de la nécessité de protéger les informations et les infrastructures critiques.	
Chaîne d'approvisionnement et écosystème	L'industrie cyber comprend une chaîne d'approvisionnement et un écosystème complexe, incluant des développeurs de logiciels, des fournisseurs de matériel, des entreprises de services et de conseil en sécurité, ainsi que des organismes de recherche et de normalisation. Les entreprises au sein d'une industrie peuvent s'approvisionner en technologie ou en main d'œuvre auprès des mêmes fournisseurs et vendre leurs solutions à travers des canaux similaires.	
Réglementations et normes	Le secteur est réglementé de manière irrégulière et inégale, notamment avec des lois spécifiques visant à protéger les données dans le contexte de la protection des renseignements personnels. Les entreprises et organismes publics sont généralement soumis aux mêmes lois, régulations et directives. L'industrie aide ces derniers à s'y conformer. Toutefois, les règles de l'art, la qualité, la portée des services et solutions ne sont pas encadrées par des lois et relèvent plutôt de mécanismes d'autoréglementation peu fiables. Ces cadres réglementaires peuvent définir les limites d'une industrie et affecter la manière dont les entreprises opèrent au sein de celle-ci.	
Forces économiques et du marché	Les acteurs de l'industrie sont influencés par des forces économiques et de marché similaires, telles que les dynamiques de demande et d'offre, les avancées	

	technologiques et les tendances économiques mondiales. Les entreprises au sein de cette industrie répondent de manière similaire à ces facteurs externes. Les macros-tendances (ex : XDR, Zero Trust, mouvement vers les plates-formes toute-incluses, etc.) sont extrêmement influentes sur le comportement des consommateurs et par conséquent des entreprises	
Impact économique et social	La cybersécurité a un impact significatif sur l'économie et la société, car les cyberattaques peuvent entraîner des pertes financières considérables, porter atteinte à la réputation des entreprises et compromettre la sécurité nationale.	
Innovation et recherche	L'industrie de la cybersécurité est caractérisée par une innovation rapide et continue, avec des recherches en cours pour développer de nouvelles technologies et approches pour contrer les menaces cybernétiques émergentes.	
Systèmes de classification	Divers systèmes de classification, tels que le Système de classification des industries de l'Amérique du Nord (SCIAN) au Canada, les codes de Classification des industries standard (CIS) et la Classification internationale type, par industrie, de toutes les branches d'activité économique (CITI), sont utilisés pour catégoriser et définir les industries en fonction d'une structure hiérarchique des activités économiques. La plupart des entreprises de cette industrie utilisent les codes liés au développement logiciel ou aux services conseils scientifiques. Il n'y a aucune catégorie pour la cybersécurité.	

Au regard de ces observations, la cybersécurité constitue une industrie à part entière, même si elle est fortement soudée à celle des TI en général. Comme nous l'avons déjà souligné, cette industrie joue un rôle crucial dans la protection des infrastructures critiques (de plus en plus dépendantes des technologies numériques) et dans la sécurisation de l'économie numérique mondialisée. Cela l'expose à des enjeux et des contraintes qui transcendent les limites des seuls acteurs de l'industrie et représentent un ensemble complexe de défis nécessitant une approche intégrée englobant les technologies, la gestion, l'éducation et la coopération intersectorielle pour protéger efficacement les actifs numériques dans un paysage de menaces en constante évolution.

Ces enjeux et contraintes sont les suivants:

1. **Ubiquité des menaces** : les cyberattaques ne connaissent pas de frontières sectorielles. Elles peuvent affecter n'importe quelle organisation, quel que soit son secteur d'activité. Les infrastructures critiques telles que les institutions financières, les opérateurs de télécommunication, les entreprises de transport, de distribution énergétique ou les services de santé sont souvent des cibles privilégiées en raison de leur importance pour la société et l'économie.

2. **Gestion et gouvernance** : la protection contre les cybermenaces exige une approche de gestion stratégique qui intègre la cybersécurité dans la planification et les opérations quotidiennes de

l'entreprise. Cela nécessite une gouvernance solide, une allocation de ressources adéquate et une prise de décision au plus haut niveau de l'organisation. Ces processus sont relativement complexes à mettre en œuvre pour des organisations disposant de ressources conséquentes et d'un niveau de maturité élevé en cybersécurité, mais ils peuvent décourager les petites ou moyennes entreprises qui disposent rarement des moyens et des connaissances pour les adopter (Westin et al., 2022).

3. **Capacités technologiques** : les défis de la cybersécurité et de la cyber résilience requièrent des solutions technologiques avancées et une adaptation continue aux nouvelles menaces. Cela implique non seulement d'investir dans la technologie, mais aussi de développer la capacité à intégrer et à gérer efficacement ces technologies au sein des processus d'affaires existant. Cette réactivité permanente soumise aux innovations des attaquants explique pourquoi cette industrie a de la difficulté à se stabiliser et ne se conforme pas aux modèles de développement traditionnels comme celui de l'industrie automobile ou aéronautique (Carmel et Roche, 2023).

4. **Connaissances et compétences** : la lutte contre les cybermenaces demande des connaissances spécialisées et des compétences techniques pointues. Les organisations doivent investir dans la formation et le développement des compétences de leur personnel, mais également dans la sensibilisation à la cybersécurité à tous les niveaux de l'organisation.

5. **Collaboration intersectorielle** : étant donné que les chaînes d'approvisionnement et les infrastructures sont interconnectées à travers différents secteurs, la résilience face aux cybermenaces dépend de la collaboration entre différents acteurs industriels. Le partage d'informations sur les menaces, les meilleures pratiques et les stratégies d'atténuation est crucial pour renforcer la cyber résilience de manière collective.

6. **Normes et réglementations** : bien que certaines normes de cybersécurité soient spécifiques à des industries (PCI-DSS, NERC/FERC, etc.), de nombreuses normes, directives et bonnes pratiques sont applicables à travers différents secteurs (ISO 27000, US NIST, SOC II, Cybersécuritaire Canada, etc.). La conformité avec ces normes requiert une approche globale de la cybersécurité qui dépasse les limites d'une seule industrie.

1. PORTRAIT DE LA CYBERSÉCURITÉ DANS LE MONDE ET AU QUÉBEC (REVUE DE LITTÉRATURE)

1.1 Sources des données et méthodologie

Ce rapport est basé sur des données colligées à partir de trois méthodologies complémentaires (analyse documentaire, sondage et entretiens semi-dirigés) qui permettent de dresser un tableau relativement détaillé de l'industrie de la cybersécurité au Québec et de l'écosystème au sein duquel elle opère.

Tout d'abord, une analyse documentaire a été effectuée afin de brosser un portrait de la cybersécurité dans le contexte canadien et québécois, et de comparer ces informations avec des données issues du contexte mondial lorsque cela s'est avéré pertinent. À ce titre, une trentaine de rapports, de sites web gouvernementaux et d'articles scientifiques identifiés à l'aide du moteur de recherche Google Scholar a été consultée et analysée en s'appuyant sur les thématiques suivantes : état actuel de la cybersécurité au Québec, au Canada, et dans le monde, tendances et développement du marché de la cybersécurité, et interventions gouvernementales afin de soutenir et renforcer l'industrie de la cybersécurité.

Deuxièmement, un portrait statistique des entreprises en cybersécurité au Québec a été réalisé sur la base d'informations publiques colligées au sujet de 157 entreprises œuvrant dans ce domaine. Par ailleurs, un sondage a été réalisé par Prompt auprès d'un échantillon de 47 entreprises provenant de cette industrie[5]. Ce sondage comprenait 43 questions spécifiques au module administré aux fournisseurs et prestataires de cybersécurité et avait pour but d'obtenir des données quantitatives et qualitatives sur les entreprises dans les domaines suivants : implantation géographique, historique de l'entreprise, composition de la main d'œuvre et principaux défis rencontrés à l'acquisition et la rétention des talents, types de produits et de services offerts, intensité technologique des produits et services offerts (existence d'une solution logicielle spécifique à l'entreprise), investissement en R&D, clientèle cible et domaines d'activité des clients, principaux défis dans les interactions avec les clients, facteurs influençant les ventes aux clients privés et publics, profitabilité, état de la compétition, activités à l'exportation, avenir anticipé de l'entreprise.

Troisièmement, le rapport utilise les données qualitatives recueillies dans les questions ouvertes du sondage permettant aux répondants de préciser certains enjeux et défis rencontrés par leur entreprise, ainsi que des témoignages recueillis lors de la tenue de quatre entretiens semi-dirigés auprès de personnes clés œuvrant au sein d'entreprises en cybersécurité au Québec.

Comme indiqué en introduction, ce rapport comprend un certain nombre de limites : il ne prétend pas être représentatif de la diversité des situations et des tendances dans une industrie très dynamique et en

[5] L'échantillon complet du sondage comprenait 58 répondants, mais sept d'entre eux appartenaient à la catégorie des acheteurs de produits ou de services, et quatre autres représentaient une université ou un centre de recherche. Leurs réponses ont été utilisées pour documenter le chapitre sur l'écosystème, mais n'ont pas été traitées dans le chapitre descriptif de l'industrie.

perpétuelle évolution. Le sondage n'a pu rejoindre qu'un échantillon limité de répondants, et sa longueur en a découragé certains qui n'ont pas répondu à toutes les réponses. La quantité de réponses obtenues et l'accès qu'elles nous donnent à l'expérience des dirigeants d'entreprises de toutes tailles en cybersécurité nous semblent toutefois contribuer à une nette amélioration des connaissances sur cette industrie. Par ailleurs, les données statistiques disponibles sur la taille et les activités de cette industrie restent très parcellaires, que ce soit au Québec ou au Canada, ce qui ne permet pas de suivre son évolution dans le temps de manière fiable. Enfin, les quatre entretiens qualitatifs ont été menés de manière ouverte avec des entreprises de taille modeste (de trois à quarante employés) dont les expériences pouvaient s'avérer très limitées dans certains domaines et dont les réponses pouvaient varier selon les intérêts immédiats ou les connaissances des répondants.

Ces limites viennent donc renforcer la raison même d'être de ce rapport et le besoin de poursuivre l'effort de cartographie de l'industrie de la cybersécurité au Québec, dont le rôle stratégique pour la protection des actifs numériques vitaux est indéniable.

1.2 Le marché mondial de la cybersécurité et les trois méga-grappes

Afin de mieux contextualiser les activités de l'industrie québécoise de la cybersécurité et de son écosystème d'attache, il est important de comprendre quelle place occupe la cybersécurité en tant qu'activité économique à l'échelle mondiale et où sont concentrées les principales grappes d'expertise et de capacités dans ce domaine en très forte croissance.

L'entreprise de consultants spécialisés Gartner estimait en septembre 2023 que le marché mondial de la cybersécurité représentait un chiffre d'affaires de 166 milliards de dollars US en 2022, et prédisait qu'il atteindrait 188 milliards en 2023 et 214 milliards en 2024, soit une croissance moyenne remarquable de 13% par an dans un contexte économique général par ailleurs assez morose (Gartner, 2023). Parmi les sous-secteurs porteurs de la plus forte croissance figuraient la sécurité des infrastructures infonuagiques (+24,7% en 2024), la protection de la vie privée (+24,6% en 2024), et la protection des infrastructures essentielles (+17,5% en 2024). Les services représenteraient 42% de ce marché global, constituant ainsi le premier poste de dépenses dans ce domaine (Gartner, 2023). À l'échelle continentale, le marché nord-américain était estimé à un peu plus de 67 milliards de dollars US en 2022, ce qui représentait alors 44% du marché mondial et en faisait un leader incontesté (Fortune Business Insights, 2024).

L'offre de produits et de services est concentrée autour d'environ 3 000 entreprises à l'échelle mondiale (The Economist, 2018), plus de la moitié des plus puissantes ayant leur siège social dans trois zones géographiques pouvant être qualifiées de méga-grappes : la Silicon Valley au Sud de San Francisco, la région de Washington DC, et Israël (autour des quatre centres urbains de Haïfa, Tel Aviv, Jérusalem et Beersheba). En effet, en 2018, année la plus récente pour laquelle des données comparatives sont disponibles, ces trois régions accueillaient plus de 930 entreprises qui cumulaient 37 milliards de dollars US d'investissement en capitaux de risque et généraient collectivement 33 milliards de dollars US de revenus (Carmel et Roche, 2023). D'autres centres tentent de former une masse critique et d'émerger à Londres, New York, Boston, San Antonio, Singapour ou même Paris, mais il leur est difficile de réunir les

principaux facteurs qui permettent l'éclosion et le développement d'une grappe aussi performante en cybersécurité.

Dans une étude de référence, Cohen et al. (2017) ont identifié sept facteurs déterminants. Tout d'abord, on note quatre facteurs connus et communs à d'autres types de grappes industrielles : l'existence de réseaux sociaux et commerciaux facilitant l'échange d'informations, l'établissement de relations, la collaboration et la mobilité de la main-d'œuvre ; la présence de centres de recherche et d'universités qui servent de plateformes de recherche, de sources de financement pour les entreprises en démarrage et de générateurs de personnel qualifié ; des industries complémentaires proches qui connaissent le marché (par exemple en infonuagique, en intelligence artificielle ou en informatique quantique); et des politiques gouvernementales favorables en matière de marchés publics, de financement de la R&D et de promotion commerciale à l'étranger. Trois facteurs spécifiques à la cybersécurité ont été identifiés, qui stimulent la croissance de ces grappes : la proximité d'activités gouvernementales en matière de cybersécurité, la disponibilité de personnel qualifié qui découle souvent du départ à la retraite d'employés gouvernementaux issus des organismes de sécurité et de renseignement et de la formation dispensée par les collèges et universités, et un facteur plus flou : l'existence d'un « leadership industriel fort » qui permet de catalyser les efforts de ce qui s'apparente à un écosystème diversifié et fonctionnel.

1.3 La demande de cybersécurité au Canada et au Québec

Plusieurs facteurs technologiques ont contribué à faire de la cybersécurité une préoccupation qui gagne en importance. Parmi ceux-ci se retrouvent l'adoption de l'infonuagique, l'intégration des systèmes numériques, l'utilisation de l'intelligence artificielle, la connexion 5G et la montée en popularité du télétravail (Heron et al., 2020 ; TECHNOCompétences, 2021). Aujourd'hui, toutes les entreprises ont recours à la technologie dans leurs opérations. La transition des organisations vers des pratiques numériques amène la cybersécurité à jouer un rôle de premier plan dans leur fonctionnement (Deloitte, 2023).

Au Québec, un sondage réalisé auprès de 336 conseils d'administration relève que la cybersécurité est perçue par les administrateurs comme le deuxième risque le plus important pour la prochaine année, juste derrière la rétention et le recrutement de personnel (Bouchard et Henri, 2023). Cette même étude note toutefois des différences quant à l'importance accordée à la cybersécurité selon la taille des entreprises (Bouchard et Henri, 2023). La cybersécurité arrive au deuxième rang des préoccupations pour les moyennes et grandes organisations (Bouchard et Henri, 2023). Pour les petites organisations, la cybersécurité arrive plutôt au cinquième rang (Bouchard et Henri, 2023).

Une étude réalisée par la Fédération des chambres de commerce du Québec (2021) montre également l'importance accordée par les hauts dirigeants des entreprises à la cybersécurité. À ce titre, 87% des chefs de direction au Canada se disent préoccupés par les cybermenaces (Fédération des chambres de commerce du Québec, 2021). Les organisations canadiennes se préoccupent de la cybersécurité pour de nombreuses raisons, mais l'Enquête canadienne sur la cybersécurité et la cybercriminalité de 2017 révèle que leur principale motivation est la protection des renseignements personnels (Quan et Herron, 2022).

Comme mentionné précédemment, un facteur non négligeable qui fait croître l'importance de la cybersécurité est la conformité aux nouvelles obligations législatives et règlementaires mises en place par les gouvernements canadien et québécois. Des attaques importantes et fortement médiatisées ont également attiré l'attention vers la cybersécurité au cours des dernières années. En effet, « (…) les attaques ayant visé Desjardins, Revenu Québec, Bell Canada, Equifax, Capital One, le Cégep de St-Félicien et la Société de transport de Montréal ont frappé l'imaginaire, par le nombre de données personnelles volées, par l'ampleur des rançons exigées, ou par la durée de l'arrêt des opérations des organisations infectées » (Bouchard et Henri, 2023, p.5). Conséquemment, les entreprises ont de plus en plus de pression pour protéger leurs atouts informatiques et leurs données, ce qui crée des opportunités pour l'industrie de la cybersécurité (Aiyer et al., 2022).

Dans une économie de marché, toute industrie doit apporter des réponses satisfaisantes et adaptées à la demande des acheteurs qui disposent des ressources nécessaires pour acquérir ses biens et ses services. Les données colligées par Statistique Canada dans le cadre de son enquête bisannuelle sur la cybersécurité et le cybercrime comptent probablement parmi les plus représentatives d'un marché national. Plus de 12 000 entreprises ont en effet participé à l'exercice en 2021 avec un taux de réponse de 74% (Statistique Canada, 2022)[6]. Face à une menace en évolution constante, 62% des entreprises canadiennes ont acheté des produits ou des services de cybersécurité en 2021, pour un montant total estimé à dix milliards de dollars CAD. Les grandes entreprises avaient effectué 45% de ces dépenses, les moyennes entreprises 25%, alors que les petites entreprises étaient à l'origine de 30% d'entre elles. Les dépenses associées à des opérations de rétablissement des opérations après une cyber-attaque représentaient pour leur part environ 600 millions de dollars CAD, en nette augmentation par rapport à 2019 (+50% en deux ans).

L'exposition au risque de cyber-attaque des entreprises canadiennes est assez uniformément répartie, puisqu'environ 20% des entreprises sont touchées par des incidents chaque année. Les grandes entreprises sont les plus exposées (37% d'entre elles ont été victimes), mais les moyennes et petites entreprises sont loin d'être à l'abri (respectivement 25% et 16% d'entre elles sont touchées). Si l'enquête ne permet pas de calculer le montant global des préjudices subis et des coûts indirects induits par les cyber-attaques visant les entreprises canadiennes, elle permet néanmoins de constater que les entreprises victimes déclarent avoir dépensé environ 80% de plus pour leur cybersécurité que les entreprises épargnées (+120% dans le cas des petites entreprises et +75% dans le cas des grandes entreprises). Ces chiffres combinés suggèrent que l'industrie de la cybersécurité au Canada devrait connaître une croissance robuste au cours des prochaines années, le nombre et le rythme des cyber-attaques semblant destinés à continuer de progresser.

Si les chiffres de Statistique Canada ne sont pas disponibles sur une base provinciale, un sondage mené en 2021 auprès de 157 des plus grandes entreprises par Cybereco laisse entrevoir une logique similaire. En effet, 60% des dépenses en matière de cybersécurité sont affectées à du rattrapage, 90% des entreprises ayant connu des augmentations de budget au cours des deux années précédentes. Par ailleurs, avec une proportion de 50% des entreprises consacrant moins de 6% de leur budget TI à la

[6] Les données brutes des précédentes vagues de l'enquête (2017 et 2019) peuvent être téléchargées librement sur le site du Réseau intégré sur la cybersécurité (SERENE-RISC) à https://www.serene-risc.ca/fr/statistique-canada.

cybersécurité, et le vol de données des clients constituant une préoccupation majeure pour les entreprises, la marge de progression reste relativement importante (Cybereco, 2022), même si une situation économique incertaine pourrait freiner les investissements requis.

1.4 Retombées économiques de l'industrie de la cybersécurité au Canada et au Québec

Au cours des dernières années, l'industrie de la cybersécurité a crû de façon importante, tant au Canada qu'au Québec sous la pression des facteurs présentés plus haut. Entre 2018 et 2020, l'industrie canadienne de la cybersécurité a surpassé le secteur élargi des TIC, autant sur le plan des revenus (30% de croissance contre 12%), de l'emploi (31% de croissance contre 3%), de la recherche et du développement (35% de croissance contre 19%), que sur celui des exportations (10% de croissance contre 2%) (Innovation, Sciences et Développement économique Canada, 2022). En 2020, l'industrie canadienne de la cybersécurité avait ainsi généré 3,2 milliards de dollars CAD de PIB sous la forme de revenus directs (1,6 milliards de dollars CAD), de revenus générés par les fournisseurs de cette industrie (0,8 milliards de dollars CAD), et de dépenses de consommation des employés (0,8 milliards de dollars CAD). Par ailleurs, 29 400 emplois avaient été créés, qu'il s'agisse d'emplois directs créés par cette industrie (14 100), d'emplois chez les fournisseurs (7 800 emplois), ou d'emplois induits par les dépenses de consommation des employés associés (7 500 emplois) (Innovation, Sciences et Développement économique Canada, 2022).

Cette industrie est composée dans son immense majorité de petites ou de moyennes entreprises, puisque 90% emploient moins de 250 personnes et 6% seulement emploient plus de 500 personnes. Les revenus générés et les emplois créés par les grandes entreprises s'élevaient cependant respectivement à 36% et 37% du total, pour 47% dans les deux domaines pour leurs homologues de petite et moyenne taille. Cependant, les PME contribuent de manière marquée aux exportations, étant responsables de 55% des ventes de produits et services de cybersécurité à l'étranger, contre 26% pour les grandes entreprises. Au total, ce sont ainsi plus de 1,1 milliards de dollars CAD d'exportations qui ont été générés, dont plus de 72% provenaient des États-Unis (Innovation, Sciences et Développement économique Canada, 2022). Le dynamisme de l'industrie se reflète également dans le positionnement du Canada au 6^{e} rang mondial pour les investissements en capital de risque en cybersécurité en 2019 (Investissement Québec, 2021).

Le Québec occupe le troisième rang des pôles canadiens de cybersécurité, avec 15% du total des emplois recensés, derrière l'Ontario (58% des emplois en cybersécurité) et l'Ouest autour du centre de gravité que représente Vancouver (20%) (Innovation, Sciences et Développement économique Canada, 2022). Il faut noter que cela représentait une baisse de 4% par rapport à l'état de situation réalisé en 2017, alors que l'Ontario avait augmenté ses effectifs pendant la même période de 6%. La pandémie de Covid-19 et l'explosion de l'intelligence artificielle, où Montréal bénéficie d'une position privilégiée, ont certainement provoqué des changements significatifs, mais aucune statistique n'est hélas disponible pour les cinq dernières années. Les activités de cybersécurité les plus répandues au Québec sont les suivantes : les solutions d'infrastructures de sécurité, les audits de conformité et l'élaboration de programmes, les solutions groupées, les tests de pénétration et de surveillance ainsi que la formation (Innovation, Sciences et Développement économique Canada, 2022).

1.5 La main-d'œuvre en cybersécurité

Une des conditions requises à la croissance harmonieuse du marché de la cybersécurité est l'existence d'une main d'œuvre qualifiée capable d'occuper les emplois disponibles. « Les professionnels de la cybersécurité sont responsables de protéger les organisations et les particuliers contre les cyberattaques » (Quan et Herron, 2022). Ces personnes possèdent des compétences pour créer, exploiter et maintenir des systèmes sécurisés tout en répondant aux menaces (Herron et al., 2020). La forte demande pour la cybersécurité observée ces dernières années est toutefois une source de défis pour le recrutement et la rétention de personnel.

La pénurie importante de talents en cybersécurité est un phénomène observé à l'échelle mondiale (Quan et Herron, 2022). Entre 2016 et 2021, la demande de talents en cybersécurité a augmenté de plus de 40% (Fédération des chambres du commerce du Québec, 2021). Au Canada, en 2021, bien que le nombre de personnes œuvrant en cybersécurité ait connu une augmentation fulgurante au cours des dernières années, il reste une pénurie de talents (Quan et Herron, 2022). Dans un domaine où le chômage est pratiquement nul, environ un poste sur six n'est pas pourvu (Quan et Herron, 2022, p. 4). Au Québec, en 2022, plus de la moitié des organisations qui employaient des professionnels en cybersécurité disposaient de postes qui n'étaient pas comblés (31% cherchaient à combler de 1 à 5 équivalents temps plein (ETP), 12% de 6 à 15 ETP, et 11% plus de 15 ETP) (Cybereco, 2022). Par ailleurs, un autre défi majeur de la main d'œuvre en cybersécurité est l'alignement entre les compétences effectives des employés et les compétences requises pour faire face aux besoins de sécurité actuels et prévisibles. Là encore, les organisations québécoises semblent souffrir d'un déficit préoccupant, puisque 62% d'entre elles estimaient que leur personnel spécialisé en cybersécurité manquait de compétences, voire souffrait de graves lacunes dans le domaine (Cybereco, 2022).

Une autre conséquence de la pénurie de talents est qu'elle accroît la compétition entre employeurs, et, par le fait même, les salaires des employés de cette industrie, ce qui n'aide pas les organisations en quête de personnel. Les travaux de Quan et Herron (2022) montrent que les salaires sont gonflés par la demande. De plus, le manque de diversité est aussi mentionné comme un facteur qui a des conséquences négatives sur la main d'œuvre. À titre d'exemple, la sous-représentation des femmes dans le milieu accentue le manque de main-d'œuvre (ISC)², 2021). Au Canada, en 2020, les femmes occupaient ainsi seulement 23% des postes techniques et scientifiques en cybersécurité, alors que leur présence était plus équilibrée dans les fonctions d'administration, de marketing et de gestion où elles occupaient 40% des postes (Innovation, Sciences et Développement économique Canada, 2022). Les enjeux de recrutement n'épargnent pas le secteur public. Au contraire, celui-ci est confronté à des défis qui lui sont propres, tels que « (…) des niveaux de rémunération inférieurs à ceux du secteur privé, un financement insuffisant, des obstacles bureaucratiques, des processus d'embauche fastidieux, la vérification des antécédents et l'épuisement professionnel « (Quan et Herron, 2022, p. 8).

Bien que cette pénurie de main-d'œuvre soit présente aux États-Unis également, la pénurie canadienne comporte des particularités. Tout d'abord, le Canada ne détient pas de cadre de compétences à l'échelle nationale (semblable au NICE aux États-Unis), ce qui entrave la communication entre les employeurs et les employés potentiels en cybersécurité au sujet des compétences nécessaires pour réussir (Quan et Herron, 2022). Deuxièmement, les travaux de Quan et Herron (2022) dénotent un manque de communication entre l'industrie de la cybersécurité et le milieu universitaire. Enfin, le marché de l'emploi américain fait concurrence au marché canadien en offrant une rémunération souvent plus avantageuse (Quan et Herron, 2022). Les États-Unis sont confrontés à une pénurie de main-d'œuvre 15 fois plus importante que celle vécue au Canada (Quan et Herron, 2022). La perte de talents canadiens qui se redirigent vers les États-Unis met en lumière la fragilité de l'industrie canadienne. Cette compétition et ses manifestations négatives se sont drastiquement accentuées depuis la pandémie de Covid-19, où la généralisation du télétravail permet de recruter des employés canadiens délocalisés géographiquement qui n'ont pas besoin de déménager tout en accédant à des rémunérations très avantageuses proposées par leur employeur américain.

Par ailleurs, un bon nombre de travailleurs dans le domaine de la cybersécurité sont des généralistes en TI qui se sont vu confier des responsabilités en matière de cybersécurité (Herron et al., 2020). Ce ne sont pas toutes les entreprises qui souhaitent embaucher du personnel spécialisé (Herron et al., 2020). À cet égard, un sondage pancanadien souligne deux principales raisons pour lesquelles les entreprises n'avaient pas embauché de professionnels de la cybersécurité : 1) elles avaient recours à des consultants externes plutôt qu'à leur propre personnel, ou 2) elles estimaient que la cybersécurité de leur entreprise n'était pas suffisamment menacée (Herron et al., 2020, p. 22). Ce deuxième point témoigne du besoin de faire reconnaître les risques, mais aussi l'expertise en cybersécurité et de sensibiliser les entreprises à son importance.

Plusieurs stratégies sont mises en œuvre par les entreprises pour remédier aux problèmes de recrutement et de rétention du personnel en cybersécurité. Un sondage effectué par Deloitte (2023) met en lumière les stratégies suivantes comme étant les plus utilisées par les répondants : l'offre de formation et l'accès à des certifications, un environnement de travail flexible ou hybride, des parcours de carrières spécialisées, des modèles de rémunération différenciés, des opportunités de mobilité à l'interne et à l'international et enfin du soutien pour compléter un MBA (Deloitte, 2023).

La cybersécurité est un domaine spécialisé pour lequel il existe une multitude de formations et de certifications, avec plus de 70 certifications différentes recensées par Knowles et al. (2017). Les certifications sont une partie intégrante de l'écosystème de la cybersécurité. Une enquête de 2019 auprès de plus 3 000 répondants à travers le monde révèle que 59% des professionnels de la cybersécurité prévoyaient obtenir une certification au cours de l'année ou étaient déjà en train d'en poursuivre une ((ISC)²,2019). Toutefois, les certifications peuvent être coûteuses, ce qui constitue une barrière à l'entrée pour le domaine (Quan et Herron, 2022). Par ailleurs, la capacité de ces certifications à évaluer avec de hauts niveaux de fiabilité les compétences de leurs détenteurs est mise en doute par de nombreux professionnels, qui estiment que le recours quasi-systématique aux questions à choix multiples comme méthode d'évaluation des qualifications est trop statique et inefficace (Knowles et al., 2017).

Outre les certifications, plusieurs formations universitaires et collégiales sont offertes en cybersécurité au Québec et au Canada. Le Canada arrive d'ailleurs au premier rang pour son nombre de programmes de premier cycle et de cycles supérieurs en cybersécurité (Montréal International, 2021). Uniquement à Montréal, on compte 14 programmes collégiaux et de formation continue en cybersécurité, en plus d'une dizaine de chaires de recherche en cybersécurité (Montréal International, 2021). Selon un décompte réalisé en 2018 par le Réseau intégré sur la cybersécurité, le Québec hébergeait près de 30% des programmes collégiaux et universitaires en cybersécurité disponibles pour tout le Canada, soit 37 programmes sur 125[7]. Cette multiplicité et cette diversité des formations offre un bassin conséquent d'employés potentiels, mais la fragmentation des programmes et l'absence de coordination quant à l'élaboration de leurs curriculums nuisent à leur visibilité et n'aident pas les étudiants à bien évaluer lesquels sont les mieux adaptés aux besoins et aux exigences du marché de l'emploi. Le Centre canadien pour la cybersécurité a bien publié en 2024 une liste commentée des principales certifications en cybersécurité disponibles au Canada (Centre canadien pour la cyber sécurité, 2024), mais aucune ressource similaire n'est encore disponible pour les formations universitaires et collégiales.

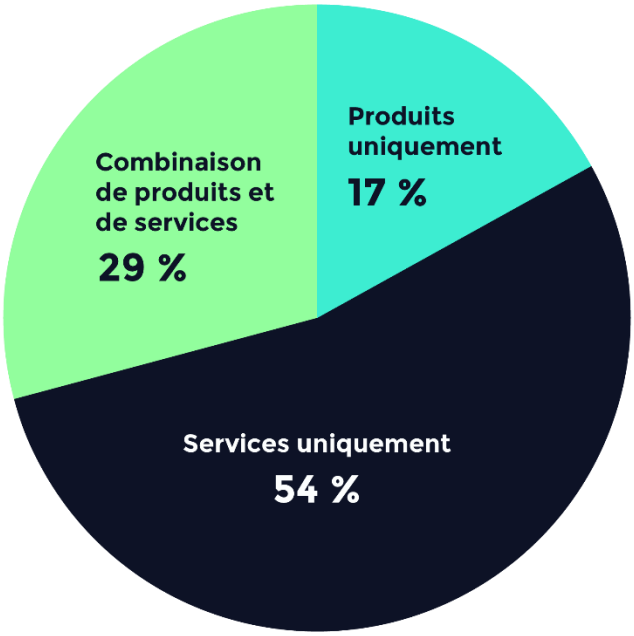
2. PORTRAIT DES ENTREPRISES QUÉBÉCOISES DE CYBERSÉCURITÉ

Afin de brosser un portrait de l'industrie de la cybersécurité au Québec, nous avons procédé à une recension des caractéristiques d'entreprises répertoriées dans ce secteur.

2.1 L'offre des entreprises et leurs domaines d'activités

Sur les 157 entreprises répertoriées par le biais de l'analyse documentaire, 26 (16,6%) d'entre elles offrent uniquement des produits[8], 46 (29,3%) offrent une combinaison de produits et de services[9] et 85 (54,1%) offrent uniquement des services[10].

[7] Pour un détail des programmes et cours disponibles à cette date, voir la page https://www.serene-risc.ca/fr/repertoire-des-programmes-en-cybersecurite.
[8] Produit : l'entreprise a pour principale activité le développement de produits/solution.
[9] Produit et service : l'entreprise développe des produits/solutions cyber qui leur sont propre tout en ayant une activité de service importante dépassant le support du produit développé.
[10] Solution : l'entreprise a pour principale activité l'offre de services dans le domaine cyber (consultation).



Le sondage auprès des 47 répondants fait apparaître une réalité similaire, avec 26 entreprises (55,3%) de l'échantillon déclarant offrir des services conseils en cybersécurité, et 21 entreprises (44,7%) des produits de cybersécurité, probablement assortis d'une offre de services complémentaires.

Que l'offre de cybersécurité soit caractérisée par des services ou des produits, la très grande majorité des entreprises s'appuyaient sur des solutions logicielles 'propriétaires': 44 entreprises (93,6%) déclaraient ainsi utiliser une ou plusieurs solutions logicielles, alors que seulement 3 entreprises (6,4%) offraient exclusivement du service à leurs clients. Dans plus de la moitié des cas (56,8% de l'échantillon), les solutions logicielles avaient été entièrement développées en interne par les entreprises, et partiellement dans 29,5% des cas, avec seulement 13,6% des entreprises dépendant de solutions développées par des tierces parties[11]. Ainsi, 86,3% des entreprises sondées avaient généré de la propriété intellectuelle et de l'innovation à l'interne, ce qui peut constituer un facteur de différentiation et de compétitivité non négligeable pour ces entreprises sur les marchés mondiaux.

Une question du sondage concernait l'origine géographique de ces développements logiciels : 65,9% des entreprises qui avaient développé des solutions logicielles s'étaient appuyées sur des ressources québécoises, 13,6% sur des ressources américaines, 9,1% sur des ressources provenant des autres provinces canadiennes, et 9,1% sur des ressources européennes[12]. On observe donc une bonne maîtrise par les entreprises de cybersécurité québécoises de leur chaîne d'approvisionnement numérique, qui

[11] Pour cette question, seulement 44 réponses sur 47 ont été obtenues.
[12] Pour cette question également, seulement 44 réponses ont été recueillies sur 47 entreprises sondées.

reste aux deux-tiers basée au Québec, et pour plus de 20% des cas concentrée dans le reste de l'Amérique du Nord.

Les principaux champs d'expertise des entreprises ont aussi été compilés. Pour ce faire, 13 catégories ont été sélectionnées avec les partenaires de cette étude pour préciser les domaines d'expertise prépondérants au Québec. Le tableau ci-dessous présente la distribution des répondants du sondage à travers ces 13 domaines d'activités, classés par ordre décroissant[16].

Champs d'expertise	N	%
Services gérés en cybersécurité	33	77%
Gouvernance de la cybersécurité	21	49%
Tests d'intrusions	21	49%
Accompagnements en certifications de cybersécurité et audits	20	47%
Formation/sensibilisation/éducation/perfectionnement de la main-d'œuvre	19	44%
Réponses aux incidents/forensic	19	44%
Protection des renseignements personnels	19	44%
Gestion des accès/authentification (IAM)	18	42%
Détection de la menace	18	42%
Cyberprotection des technologies opérationnelles (T.O.) et IoT	14	33%
Sécurité des développements logiciels	13	30%
Protection des actifs	12	28%
Autres	9	21%

Le sondage permet de constater que les services gérés, la gouvernance de la cybersécurité, et les tests d'intrusion sont les trois principaux domaines d'expertises des entreprises québécoises, suivis de très près par une demi-douzaine d'autres types d'activités. À l'opposé, la cyber protection des technologies opérationnelles (T.O.) et de l'internet des objets (IoT), la sécurité des développements logiciels, et la protection des actifs sont les domaines dans lesquels on retrouve le moins d'activités parmi les entreprises ayant participé au sondage (avec cependant près du tiers des entreprises se déclarant compétentes). Ces résultats laissent penser qu'une majorité des entreprises québécoises en cybersécurité sont des généralistes qui opèrent à travers des champs d'expertise multiples, et que seule une minorité d'entre elles (sept entreprises, soit 15% de l'échantillon) sont des « pure players » qui se spécialisent dans un seul domaine d'activité.

Une dimension significative de l'industrie de la cybersécurité au Québec est le rôle qu'elle joue dans la protection des infrastructures essentielles. En effet, 34 entreprises (72,3%) de l'échantillon déclaraient avoir une offre liée à la protection des infrastructures essentielles, les clients les plus fréquemment cités comprenant le secteur du transport et de la logistique (82,3%), les infrastructures critiques de distribution d'électricité et d'eau (79,4%), le secteur gouvernemental et paragouvernemental relatif à la protection des données citoyennes (70,6%), suivis du secteur des télécommunications (67,6%), du secteur financier

[16] Pour cette question du sondage, 43 réponses ont été obtenues. Le total est supérieur à 100%, puisque chaque entreprise peut exercer son expertise dans plusieurs champs simultanément.

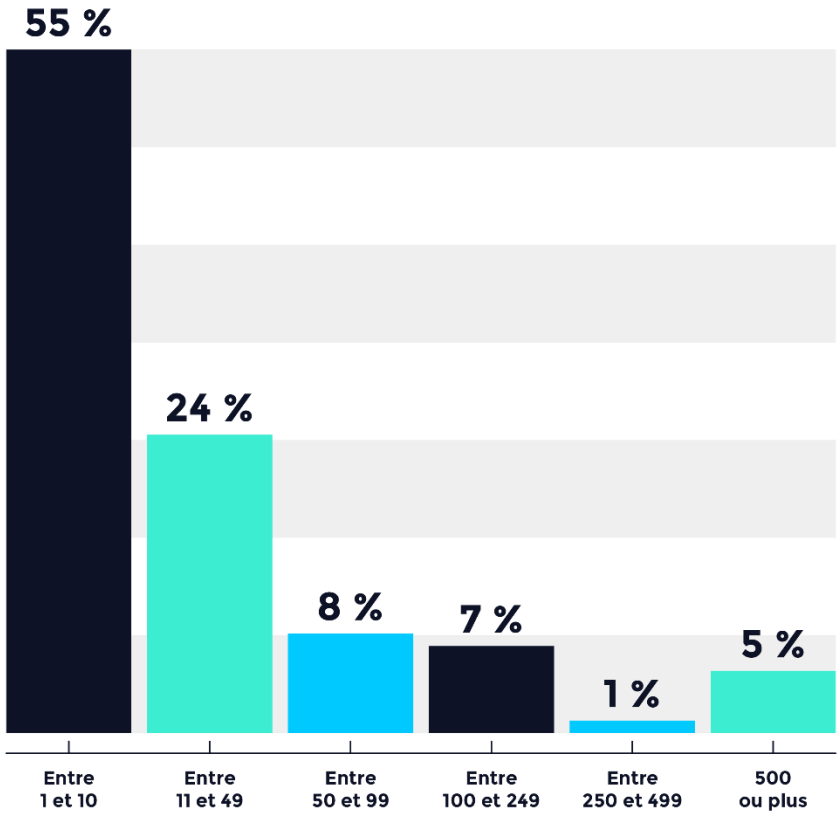
(banque et assurance) (67,6%), et du secteur de la santé (64,7%). Le secteur légal, pour sa part, semblait beaucoup moins bien couvert, puisque seulement 32,3% des entreprises répondantes déclaraient offrir des produits ou des services dans ce domaine.

Ces résultats permettent de définir une typologie des entreprises actives dans le domaine de la cybersécurité et d'en mesurer les impacts économiques et en termes de valeur ajoutée.

Type d'organisation	Création de valeur	Impact économique
Producteurs de technologies logicielles et matérielles spécialisées	Ces entreprises contribuent directement à l'innovation technologique et au développement économique en créant des produits de haute technologie. Elles génèrent des emplois qualifiés et stimulent la R&D dans la région.	Leur succès à l'exportation peut améliorer la balance commerciale de la région et renforcer sa position comme un leader technologique
Firmes de service-conseil	Ces firmes apportent une expertise cruciale pour évaluer les risques de cybersécurité, concevoir des stratégies de sécurité adaptées et former le personnel. Elles jouent un rôle vital dans la sensibilisation et la préparation des entreprises face aux cybermenaces	Leur travail aide à minimiser les pertes économiques dues aux cyberattaques et à renforcer la confiance dans l'écosystème numérique, ce qui est essentiel pour attirer les investissements dans tous les secteurs et assurer une stabilité dans la capacité d'exploitation des organisations et appareils gouvernementaux.
Revendeurs et intégrateurs de solutions	En facilitant l'accès aux technologies de pointe et en personnalisant les solutions de cybersécurité pour répondre aux besoins spécifiques des clients, ces entreprises aident à démocratiser la sécurité numérique.	Ils soutiennent la compétitivité des petites et moyennes entreprises (PME) en leur permettant d'accéder à des solutions de sécurité avancées, contribuant ainsi à la résilience économique globale. Ils peuvent aussi permettre aux producteurs de technologies logicielles et matérielles en cybersécurité du Québec à accéder aux clients, répondant à un besoin critique d'accès au marché.
Prêt de ressource - basé sur des demandes à court et long-terme (1 mois à plusieurs années).	Ces sociétés facilitent l'arbitrage entre les employeurs et une main d'œuvre qui peut paraître inaccessible, difficile à recruter et à maintenir en poste	Ils permettent de combler une demande non-structurée.

2.2 Nombre d'employés et caractéristiques de la main d'œuvre

Sur les 157 entreprises répertoriées par l'analyse documentaire, la majorité répondent au profil de PME. Ainsi, 54,7% ont moins de 10 employés et 24,2% ont moins de 50 employés, le reste des entreprises ont plus de 50 employés.



L'échantillon de 47 entreprises auquel a été administré le sondage répondait à une distribution similaire, avec 49% d'entreprises de moins de 10 employés, 34,1% d'entreprises comptant entre 11 et 49 employés, et 12,8% d'entreprises comptant de 50 à 200 employés, laissant penser que les réponses plus détaillées sur la main d'œuvre reflétaient également assez fidèlement l'état de l'industrie.

Un premier constat tiré du sondage concernant la main d'œuvre est que les entreprises en cybersécurité ont connu au cours des deux dernières années une forte croissance du nombre d'employés, comme l'illustre le tableau ci-dessous. Dans un contexte post-pandémique agité, plus du tiers des entreprises de cybersécurité (38,2%) ont ainsi enregistré une croissance de plus de 31% de leur personnel, dans un secteur où nous avons vu que la pénurie de main d'œuvre représentait un facteur de tension important. Plusieurs stratégies d'adaptation sont mises en œuvre par les entreprises afin de répondre à cette pression positive sur leur développement.

Taux de croissance du personnel des entreprises québécoises de cybersécurité : 2021-2023

Taux de croissance	Pourcentage (%) d'entreprises	Nombre d'entreprises
Plus de 100%	10,6%	5
51 à 100%	8,5%	4
31 à 50%	19,2%	9
21 à 30%	25,6%	12
11 à 20%	10,6%	5
1 à 10%	14,9%	7
Croissance nulle ou négative	10,6%	5

Une première stratégie est le recours à des employés contractuels afin de compléter les effectifs permanents. Une majorité des entreprises ayant répondu au sondage employaient ainsi des employés contractuels : 70,2% (33 entreprises) employaient entre 1 et 10 contractuels, 12,8% (6 entreprises) employaient entre 11 et 49 contractuels, 2,2% (1 entreprise) employaient plus de 200 contractuels, et seulement 14,9% (7 entreprises) n'employaient aucun contractuel. Le recours aux employés contractuels, par la flexibilité qu'il procure, permet aux entreprises en cybersécurité d'absorber la croissance qui accompagne le dynamisme de ce marché.

Une deuxième stratégie d'adaptation est le recours à des stagiaires ou des étudiants : 80,9% des entreprises sondées (38 entreprises) déclaraient avoir recours à cette main d'œuvre temporaire qui peut également faire l'objet d'offres de recrutement lorsque les compétences correspondent aux besoins de l'organisation. Pour 68,5% des entreprises (26 entreprises), ces stagiaires et étudiants représentaient 1 à 10% de la main d'œuvre, alors que pour près du quart de l'échantillon (23,7% ou 9 entreprises), ils constituaient entre 10 et 20% de la main d'œuvre, soit une part conséquente.

Une troisième stratégie déployée par les entreprises de cybersécurité est de recruter parmi les personnes issues de l'immigration, qu'il s'agisse de faciliter l'obtention de permis de travail ouverts ou fermés, ou de puiser dans le bassin des résidents permanents. Ainsi, plus du quart des entreprises interrogées (27,7% ou 13 entreprises) employaient plus de 25% de salariés issus de l'immigration, et un autre quart (27,7% ou 13 entreprises) employaient entre 10 et 24% de salariés issus de l'immigration. Les entreprises qui ne comptaient dans leur main d'œuvre aucun employé issu de l'immigration ne représentaient que 19,1% de l'échantillon. Les entreprises québécoises de cybersécurité sont donc enchâssées dans des réseaux internationaux de circulation de la main d'œuvre qui contribuent à la diversité de leur expertise.

Malgré toutes ces démarches, près des trois quarts des entreprises (78,7% ou 37 entreprises) disposaient de postes restant à pourvoir ou en cours de dotation, ce qui renforce à la fois le constat d'un marché en croissance et d'une pénurie de main d'œuvre.

Un des facteurs additionnels qui pourrait contribuer à l'atténuation de cette tension sur la main d'œuvre – mais qui reste encore largement sous-exploité – serait une participation plus marquée des femmes au sein des entreprises. Le tableau ci-dessous décrit la proportion des fonctions techniques occupée par des femmes dans les entreprises sondées[13]. Près de la moitié des entreprises (46,6%) présentaient des taux

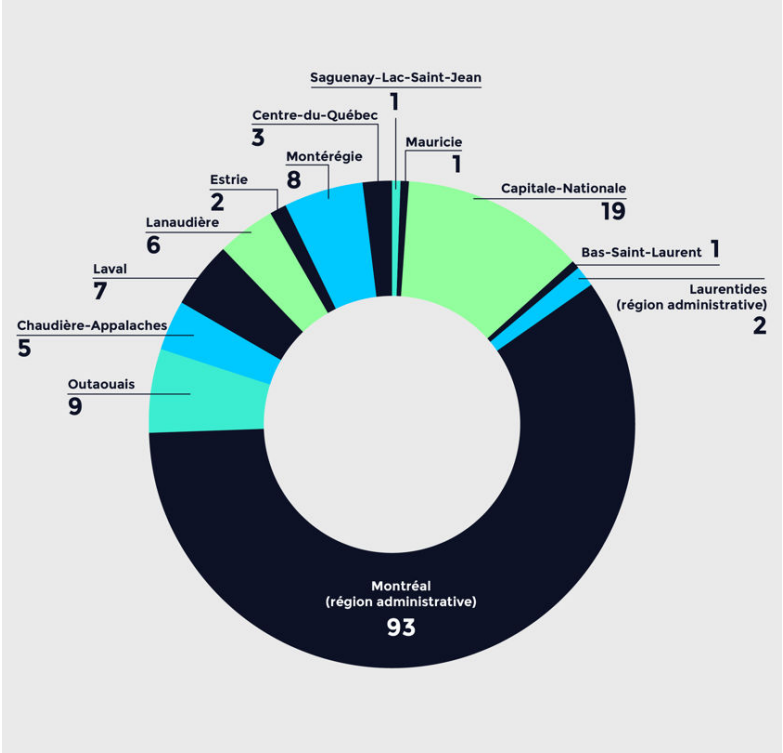
[13] Pour cette question, seulement 45 répondants sur 47 ont fourni une réponse.

de participation féminins de moins de 5%, un quart des entreprises n'ayant même aucune femme occupant un rôle technique en cybersécurité.

Taux de participation des femmes aux rôles techniques en cybersécurité

Taux de participation	Pourcentage (%) d'entreprises	Nombre d'entreprises
Plus de 25%	20,1%	9
21 à 25%	8,9%	4
16 à 20%	6,7%	3
11 à 15%	4,4%	2
6 à 10%	13,3%	6
1 à 5%	22,2%	10
0%	24,4%	11

2.3 Répartition géographique des entreprises



Au sein de l'échantillon documentaire, on constate que la forte majorité des entreprises en cybersécurité est basée à Montréal, une tendance également observée dans l'échantillon soumis au sondage, où les entreprises ayant leur siège dans la région métropolitaine de Montréal (Montréal, Laval et Longueuil) représentaient 55,2% des répondants (32 entreprises).

2.4 Historique des entreprises et profitabilité de leurs activités

Bien que la cybersécurité soit un secteur d'activité dont le dynamisme économique est relativement récent, plus de la moitié des entreprises sondées (53,2% ou 25 entreprises) sont en activité depuis plus

de 6 ans (25,5% depuis plus de 15 ans), alors que près d'un tiers (29,8% ou 14 entreprises) ont de 3 à 5 ans d'existence. Les startups en activité depuis 2 ans ou moins ne représentent par ailleurs que 17% de l'échantillon. Cette distribution reflète l'évolution historique de la cybersécurité, qui était auparavant commercialisée sous le terme de sécurité informatique, puis de sécurité de l'information, et dont le changement d'image (*rebranding*) a permis à des entreprises déjà bien établies d'améliorer leur visibilité dans un contexte où les enjeux de cybersécurité occupent le devant de la scène.

En termes de profitabilité de leurs activités, plus des trois quarts des entreprises avaient généré un résultat net positif (55,3% ou 26 entreprises), ou avaient atteint un seuil d'équilibre entre leurs revenus et leurs dépenses (19,2% ou 9 entreprises). Un quart des entreprises (25,5% ou 12 entreprises) étaient pour leur part en situation de résultat net négatif. Ces chiffres doivent être considérés dans un contexte de forte croissance des activités, qui peuvent provoquer un déséquilibre temporaire de trésorerie pour des entreprises qui investissent dans le recrutement de nouveaux employés et l'acquisition de nouveaux clients.

Comme nous l'avons déjà vu, le secteur de la cybersécurité est en pleine croissance, avec des chiffres très au-dessus des moyennes des autres industries québécoises. Ainsi, entre 2021 et 2023, près de la moitié des entreprises (48,8% ou 23 entreprises) ont déclaré avoir connu un taux de croissance nette de leur résultat de plus de 40%, alors que près d'un cinquième (19,1% ou 9 entreprises) dépassaient 100% de croissance nette. Le tableau ci-dessous présente la distribution des entreprises de l'échantillon selon les taux de croissance déclarés.

Taux de croissance net du résultat pour les années 2021-2023

Taux de croissance	Pourcentage (%) d'entreprises	Nombre d'entreprises
Plus de 100%	19,1%	9
51 à 100%	19,1%	9
41 à 50%	10,7%	5
31 à 40%	8,5%	4
21 à 30%	10,7%	5
11 à 20%	25,5%	12
1 à 10%	0,0%	0
Croissance nulle ou négative	6,4%	3

Ces chiffres sont à comparer avec l'évolution du PIB réel par industrie au Québec qui a progressé de 6,0% en 2021, 2,8% en 2022 et de 0,1% en 2023 pour l'ensemble des industries de biens et de services[14]. Ils indiquent à quel point la cybersécurité constitue pour le Québec un réservoir de prospérité économique, même au sein de son secteur de référence des services professionnels, scientifiques et techniques, où ses performances sont manifestes.

Bien que plus modeste, la croissance des exportations représente néanmoins une contribution appréciable à l'économie québécoise, d'autant plus pour des entreprises majoritairement de petite et moyenne taille. Le tableau ci-dessous décrit la croissance des exportations des entreprises sondées au

[14] Pour accéder aux statistiques officielles de l'Institut de la statistique du Québec sur le PIB, voir https://statistique.quebec.ca/fr/document/produit-interieur-brut-par-industrie-au-quebec.

cours de la période 2021-2023. On remarque que plus du quart (27,7% ou 13 entreprises) des répondants avait connu une hausse des exportations de plus de 25%, mais aussi qu'un autre quart (27,7% ou 13 entreprises) avait vu des augmentations plus modestes de 1 à 10%, et que près d'un cinquième (19,1% ou 9 entreprises) avait même subi une stagnation ou un recul de ses exportations. Ces chiffres sont à analyser au regard des statistiques du commerce extérieur québécois pendant ces trois années, durant lesquelles les exportations de biens et de services ont augmenté cumulativement de 18,6% (Gouvernement du Québec, 2024 : p. 13).

Taux de croissance des exportations (hors Québec) pour les années 2021-2023

Taux de croissance	Pourcentage (%) d'entreprises	Nombre d'entreprises
Plus de 25%	27,7%	13
20 à 25%	6,4%	3
15 à 19%	10,6%	5
10 à 14%	8,5%	4
5 à 9%	14,9%	7
1 à 4%	12,8%	6
Croissance nulle ou négative	19,1%	9

Un résultat plus préoccupant concerne la stabilité de l'actionnariat de ces entreprises, puisqu'un quart des répondants (25,5% ou 12 entreprises), prévoyait vendre l'entreprise au cours des cinq prochaines années. Il est difficile de vérifier si ces intentions se sont concrétisées, ou si des démarches ont été engagées en ce sens, mais on peut déduire de la répartition géographique des principaux compétiteurs quels pourraient être les acquéreurs potentiels de ces entreprises. Les répondants déclaraient en effet que leurs principaux compétiteurs se situaient au Québec (91,5% ou 43 entreprises), dans le reste du Canada (74,5 % ou 35 entreprises), aux États-Unis (44,7% ou 21 entreprises), et dans une moindre mesure en Europe (36,2% ou 17 entreprises). Les chances sont donc non négligeables de voir des entreprises provenant de ces trois grands marchés prendre le contrôle d'entreprises ayant développé une expertise et des compétences au Québec.

2.5 Intensité des activités de recherche et de développement (R&D)

Un dernier volet du sondage explorait les pratiques des entreprises québécoises de cybersécurité en matière de recherche et de développement, un domaine stratégique dans un secteur où les besoins en innovation sont constamment renouvelés sous la pression combinée de facteurs tels que la créativité sans borne des acteurs malveillants et le développement accéléré de nouvelles technologies à sécuriser (l'internet des objets, les technologies opérationnelles, l'informatique quantique ou l'intelligence artificielle, pour n'en citer que quelques-unes). Dans ce contexte, il est plutôt rassurant de constater que 80,9% des répondants (38 entreprises) déclaraient mener des activités de recherche-innovation.

L'intensité de ces activités mesurée en proportion des coûts d'opération annuels est par ailleurs significative, comme l'indique le tableau ci-dessous[15], puisque plus de la moitié des entreprises (52,6% ou

[15] Pour cette question, seulement les 38 entreprises ayant déclaré avoir initié des dépenses de recherche-innovation ont répondu à la question de la part des coûts de ces activités dans les montant global des coûts opérationnels.

20 entreprises) consacre plus d'un cinquième des coûts opérationnels aux activités de recherche-innovation. Ces chiffres peuvent sembler démesurés, mais ils reflètent l'intensité des investissements d'innovation requis dans l'industrie des technologies numériques pour rester compétitif. Une étude menée aux États-Unis en 2019 établissait ainsi que les entreprises éditant des logiciels investissaient en moyenne entre 17% et 26% de leurs revenus annuels en dépenses de recherche et d'innovation, selon la vélocité de leur croissance, certaines entreprises désirant conquérir de nouveaux marchés n'hésitant pas à investir jusqu'à 40% ou 50% de leurs revenus annuels en R&D (Ahlawat et al., 2019).

Proportion des coûts opérationnels consacrés aux activités de recherche-innovation au cours de la dernière année financière

Part de la recherche-innovation dans les coûts opérationnels	Pourcentage (%) d'entreprises	Nombre d'entreprises
Plus de 25%	42,1%	16
20 à 25%	10,5%	4
15 à 19%	13,2%	5
10 à 14%	18,4%	7
5 à 9%	13,2%	5
1 à 4%	2,6%	1

Les aides gouvernementales jouent un rôle important dans l'exécution de ces activités, un peu plus de la moitié des répondants (53,2% ou 25 entreprises) ayant déclaré en avoir bénéficié au cours des trois années précédentes. Parmi ces bénéficiaires, on observe une nette préférence pour les programmes provinciaux, plébiscités à 92% (23 entreprises), par contraste avec les programmes fédéraux, activés dans seulement 40% des cas (10 entreprises). Ces aides gouvernementales sont principalement affectées à des dépenses générales liées à l'innovation telles que le développement de nouveaux produits, processus et procédés (80% des cas), à des dépenses de R&D (68%), ainsi qu'à des activités de commercialisation (60%).

Dans leurs activités de recherche-innovation, les entreprises québécoises semblent en revanche beaucoup moins fréquemment associées à des universités, des centres de recherche publique ou des centres collégiaux de transfert de technologie (CCTT). Moins d'un tiers d'entre elles (31,9% ou 15 entreprises) déclaraient avoir fait appel à l'une de ces organisations, malgré le nombre important de chaires de recherche et de ressources en cybersécurité actives au Québec. Parmi les institutions académiques les plus actives dans des collaborations avec cet échantillon de 15 entreprises figuraient Polytechnique Montréal (40% des cas ou 6 entreprises), l'université Concordia (26,7% des cas ou 4 entreprises), suivies des universités Laval, de Sherbrooke et de l'ETS avec 20% des cas chacune (3 entreprises).

3. ÉCOSYSTÈME INSTITUTIONNEL DE LA CYBERSÉCURITÉ AU QUÉBEC

Quelle que soit leur taille, leur modèle d'affaire, le profil de leur main d'œuvre, leur degré de profitabilité, ou la nature de leurs activités de R&D, les entreprises québécoises de cybersécurité évoluent dans un

réseau organisationnel complexe constitué d'une diversité d'acteurs publics, privés et communautaires dont les interactions facilitent ou au contraire contraignent leurs activités et leurs capacités d'innovation. En ce sens, bien plus qu'un simple marché, la cybersécurité constitue un véritable écosystème d'affaires, un concept dont la structure et le fonctionnement sont analysés par la littérature scientifique depuis le début des années 1990 (Moore, 1993).

Au lieu d'étudier le fonctionnement des entreprises de manière isolée, cette approche préfère les considérer comme une communauté dont les membres coopèrent ou entrent en compétition afin de développer et de commercialiser des produits et des services innovants. Les autres acteurs organisationnels, par leurs actions et leurs capacités, influencent également fortement la performance de l'ensemble de l'écosystème, en permettant par exemple la mise sur pied d'une infrastructure de recherche propice à l'innovation, en formant une main d'œuvre hautement qualifiée qui pourra opérationnaliser et commercialiser cette innovation à grande échelle, en mobilisant des capitaux de risque en quantité suffisante pour favoriser l'éclosion et le croissance de startups numériques, ou encore en élaborant des cadres règlementaires qui accélèreront l'adoption de certains produits ou services. On est donc en présence d'une « architecture de coopération à grande échelle » (Moore, 1996), dont la cartographie est nécessaire afin de mieux comprendre les leviers qui peuvent être utilisés pour renforcer l'efficacité de tout l'écosystème et des parties qui le composent.

L'étude systématique de l'écosystème québécois dont les contours sont esquissés dans ce rapport repose sur neuf grandes catégories d'entités interdépendantes. Cette typologie est inspirée de recherches menées sur les écosystèmes d'innovation et de gouvernance en cybersécurité (Deloitte, 2016; Dupont, 2024), et permet de comprendre quelles capacités complémentaires sont mobilisées par chacune des grandes catégories afin de construire une cybersécurité collective robuste.

- Entreprises de cybersécurité
- Acheteurs privés
- Assureurs
- Acheteurs publics
- Organismes de soutien à la cybersécurité
- Organismes de formation et de recherche (monde académique)
- Investisseurs & infrastructures d'incubation et d'accélération
- Autorités régulatrices
- Associations professionnelles et groupes communautaires

Pour chaque catégorie, une rapide description de son rôle dans l'écosystème est fournie, accompagnée de quelques faits saillants spécifiques au Québec.

3.1 Entreprises de cybersécurité

La section précédente dresse un portrait récent des entreprises québécoises de cybersécurité, et il n'est donc pas nécessaire de revenir en détail dessus. Nous avons réalisé une cartographie (voir en annexe 2) des entreprises qui tente de les catégoriser selon leur principal domaine d'activité. Ces entreprises

peuvent être classées selon une taxonomie développée par Cybereco[16] et dont un aperçu est proposé ci-dessous. Cette dernière est particulièrement adaptée pour décrire les expertises de l'écosystème québécois afin de développer *'un langage commun pour bien catégoriser et avoir une appréciation commune du secteur dans les efforts de développement de solutions ciblant l'industrie de la cybersécurité, notamment les mesures d'appui à la commercialisation, l'exportation ou l'innovation*' (Pascal Fortin, Cyberéco)

3.2 Acheteurs privés

La catégorie des acheteurs privés comprend les petites et grandes entreprises qui consomment les produits et services commercialisés par les entreprises de cybersécurité. Ces entreprises sont donc à l'origine de la demande dans ce marché dynamique, et par leurs capacités d'achat, leurs besoins et leurs exigences, elles dictent les types de solutions et les technologies que les vendeurs doivent développer. À l'intérieur de cette catégorie, on doit distinguer deux sous-groupes : les grandes entreprises et les PME.

Les grandes entreprises disposent en général de budgets confortables et d'équipes étoffées pour acquérir et déployer des solutions de cybersécurité, surtout lorsqu'elles appartiennent à l'un des secteurs opérant des infrastructures critiques comme les services financiers, l'énergie, les télécommunications ou le transport. À titre d'exemple, les coûts consolidés moyens liés à l'achat de produits et de services de cybersécurité représentaient 601 000$ en 2021 pour les grandes entreprises canadiennes, contre 7 950$ pour les petites entreprises, selon Statistique Canada[17]. Les grandes entreprises jouent donc un rôle central dans l'écosystème de la cybersécurité et influencent les pratiques de cet écosystème.

[16] Ontologie des sociétés fournisseurs en Cybersécurité, v1.0 Cyberéco, Juillet 2024
[17] Repéré à https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=2210013101&pickMembers%5B0%5D=3.1&pickMembers%5B1%5D=4.2&cubeTimeFrame.startYear=2021&cubeTimeFrame.endYear=2021&referencePeriods=20210101%2C20210101.

Le statut des petites et moyennes entreprises – qui représentent près de 98% des entreprises québécoises – dans cet écosystème est beaucoup plus marginal, en dépit de l'importance de la cybersécurité pour le maintien leurs activités quotidiennes. Ces entreprises tardent en effet à adopter les solutions de cybersécurité qui pourraient les protéger contre les risques émergents, et sont donc fragilisées face aux attaques les plus fréquentes comme celles par rançongiciel, par hameçonnage, ou les fraudes au président. La cause principale de ce désintérêt est le manque de ressources financières qui freine l'acquisition de solutions et le recrutement d'employés compétents en cybersécurité. Le manque d'expertise complique par ailleurs les démarches de sous-traitance des fonctions de cybersécurité auprès de prestataires externes qui proposent par ailleurs rarement des solutions techniques adaptées à la réalité des PME. En effet, la cybersécurité est un secteur où les promesses faites par les services de marketing s'appuient rarement sur des données probantes et où les exagérations nuisent à une prise de décision éclairée. Les PME sont particulièrement mal équipées pour analyser et interpréter ces prétentions hyperboliques. Ne sachant par où commencer leur long périple vers un état de cybersécurité plus robuste, de nombreuses PME choisissent tout simplement d'ignorer le problème jusqu'à ce qu'une crise vienne perturber leurs opérations (Westin et al., 2022). Ainsi, en 2021, seulement 14,2% des petites entreprises canadiennes étaient dotées d'une politique écrite pour gérer les risques liés à la cybersécurité, alors que 62,7% des grandes entreprises avaient entrepris cette démarche[18].

3.3 Assureurs

Les compagnies d'assurance représentent une catégorie à part sur le marché de la cybersécurité, car elles offrent à la fois un service aux acheteurs privés (une couverture permettant de transférer les impacts négatifs des risques subis vers une tierce partie qui contribue à leur atténuation financière), tout en constituant un puissant intermédiaire entre ces mêmes acheteurs et les entreprises de cybersécurité.

Les assureurs jouent un rôle clé dans le fonctionnement de l'écosystème de la cybersécurité grâce à cinq mécanismes principaux :

- Tout d'abord, lors de la souscription d'une police d'assurance, les assureurs évaluent minutieusement les risques auxquels leurs clients sont exposés et leur posture de sécurité, afin d'identifier les faiblesses et vulnérabilités à corriger avant de finaliser le contrat ;
- Ensuite, ils peuvent offrir des incitations financières sous forme de réductions de primes en échange d'investissements des clients dans l'amélioration de leur cybersécurité, bien que cette approche reste difficile à mettre en place ;
- Troisièmement, les assureurs imposent des exigences minimales de sécurité à leurs souscripteurs, comme l'activation de l'authentification multi-facteurs ou la mise en place d'un plan de réponse aux incidents ;

[18] Repéré à https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=2210013001&pickMembers%5B0%5D=3.1&pickMembers%5B1%5D=4.4&cubeTimeFrame.startYear=2019&cubeTimeFrame.endYear=2021&referencePeriods=20190101%2C20210101

- Quatrièmement, ils fournissent à leurs clients des prestataires de services spécialisés en cas d'incident majeur, offrant des services juridiques, de gestion de crise, d'expertise forensique et de communication ;
- Enfin, le cinquième levier d'influence des assureurs réside dans leur accumulation de données et de connaissances sur les pratiques et technologies de cybersécurité efficaces. Ils utilisent ces informations pour présélectionner des solutions performantes et offrir des conditions contractuelles plus avantageuses, ou pour mettre en place des programmes de sensibilisation et de formation à destination de leurs clients (Dupont, 2024).

Dans l'ensemble, les assureurs exercent une influence non négligeable sur l'écosystème de la cybersécurité, à travers des mécanismes de gouvernance allant de l'évaluation des risques à la diffusion de connaissances, en passant par l'incitation financière, l'imposition d'exigences et l'accompagnement en cas de crise. Leur rôle de régulateur *ad hoc* et d'agrégateur de données contribue à façonner les pratiques et les innovations dans ce domaine.

Bien que l'industrie de l'assurance soit en général très développée au Québec, particulièrement dans la région de Québec, qui compte une dizaine de sièges sociaux d'entreprises en assurance, il ne semble pas que la cyber assurance représente un pôle de croissance particulièrement dynamique. Pourtant, le potentiel semble plein de promesses, puisque seulement 46,5% des grandes entreprises canadiennes, 24,4% des entreprises moyennes, et 13,7% des petites entreprises avaient souscrit une assurance contre les cyber-risques en 2021[19].

3.4 Acheteurs publics

Les organismes publics jouent un rôle central dans l'écosystème de la cybersécurité du fait des montants et de la durée prolongée des contrats qu'ils peuvent offrir aux entreprises de cybersécurité pour protéger les actifs informationnels gouvernementaux. La sensibilité des données qui doivent être sécurisées fait également en sorte que les besoins des acheteurs publics répondent à des exigences plus élevées que leurs homologues privés (particulièrement dans les secteurs de la sécurité et de la défense), qui se traduisent ultimement par le développement d'une expertise plus poussée parmi leurs fournisseurs.

Par leurs stratégies d'appels d'offres, les acheteurs publics peuvent aussi favoriser le développement de certaines catégories d'entreprises, en réservant par exemple une proportion de leurs contrats à des startups – ce qui permet à ces dernières de se constituer une clientèle de référence en mesure de rassurer leurs investisseurs et d'ouvrir les portes vers de nouveaux marchés, ou à des entreprises locales qui pourront ainsi renforcer leur offre et innover face à des entreprises multinationales dont la taille représente parfois un facteur de distorsion de la compétition qui nuit à l'émergence d'une industrie nationale.

[19] Repéré à https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=2210013001&pickMembers%5B0%5D=3.1&pickMembers%5B1%5D=4.3&cubeTimeFrame.startYear=2019&cubeTimeFrame.endYear=2021&referencePeriods=20190101%2C20210101

La création du ministère de la Cybersécurité et du numérique (MCN) au Québec en 2022 et la publication en juillet 2024 de la Stratégie gouvernementale de cybersécurité et du numérique 2024-2028 constituent à ce titre de puissants leviers afin de baliser et d'encadrer les pratiques d'acquisition des organismes publics dans un double objectif d'efficacité et d'efficience.

3.5 Investisseurs & infrastructures d'incubation et d'accélération

L'accompagnement des entrepreneurs qui souhaitent offrir des produits et services innovants en cybersécurité dépend dans une grande mesure de la disponibilité du capital-risque nécessaire pour assurer la croissance des startups. Au-delà des capitaux, les investisseurs orientent stratégiquement les entrepreneurs vers les segments les plus prometteurs d'un marché très compétitif, les connectent à des opportunités d'affaires ou des partenaires aux expertises complémentaires, et favorisent l'émergence d'une culture d'entreprise qui combine agilité et profitabilité.

Au Canada, le montant total des investissements de capital-risque réalisés en 2023 (tous secteurs confondus) s'élevait à près de 7 milliards de dollars, dont 48% étaient concentrés en Ontario et 20% au Québec (CVCA, 2024). L'année 2024 semble suivre une trajectoire identique avec plus de 3,8 milliards de dollars d'investissements enregistrés durant les premiers six mois (CPE Media & Data Company, 2024). Il n'est pas possible de quantifier la proportion de ces investissements qui relèvent de la cybersécurité, mais quelques annonces récentes au Québec incluent Inscora (2 millions de dollars de financement annoncés en août 2024)[20], Mondata (17 millions de dollars de financement annoncés en juillet 2024)[21], Qohash (17,4 millions de dollars annoncés en avril 2024)[22], Flare (12,5 millions de dollars levés en 2022)[23], ou encore Terranova (9 millions de financement en 2021)[24].

L'analyse de l'origine des investissements effectués indique par ailleurs que 55% du capital-risque provient d'entreprises américaines. En ce qui concerne les fonds privés canadiens, ces derniers dépendent fortement des investissements consentis par le gouvernement fédéral et ses homologues provinciaux, ce qui fait de l'industrie canadienne du capital-risque une « entité quasi-gouvernementale » selon certains observateurs (CPE Media & Data Company, 2024).

Les incubateurs et accélérateurs d'entreprises sont des structures qui offrent un soutien en termes de mentorat, de ressources, et de réseaux, en plus du financement initial parfois disponible pour les entreprises en démarrage. Ils aident les jeunes entreprises à affiner leurs modèles d'affaires, à tester leurs produits, et à se préparer à des levées de fonds plus importantes. Selon le Mouvement des accélérateurs d'innovation du Québec, il existerait plus de soixante d'incubateurs et accélérateurs dans la province[25], mais seulement trois à notre connaissance ont développé des parcours spécialisés en cybersécurité : l'organisme Cilex, basé dans la région de Gatineau, a lancé en janvier 2023 un programme de maillage en

[20] Repéré à https://www.newswire.ca/fr/news-releases/inscora-annonce-un-financement-de-2-millions-de-dollars-pour-aider-les-courtiers-a-revolutionner-leur-pratique-de-cyberassurance-863012703.html.
[21] Repéré à https://privatecapitaljournal.com/mondata-secures-17m-financing-led-by-fonds-de-solidarite/.
[22] Repéré à https://privatecapitaljournal.com/qohash-secures-17-4m-series-b/.
[23] Repéré à https://privatecapitaljournal.com/flare-systems-secures-3m-series-a-add-on-funding/.
[24] Repéré à https://privatecapitaljournal.com/terranova-security-secures-9m-financing-from-bdc-capital/.
[25] Voir la carte interactive des ressources d'accompagnement à https://mainqc.com/trouver-un-accelerateur/.

cybersécurité s'appuyant sur les ressources locales spécialisées en sécurité et identité numérique[26]. Ce programme d'un an a accueilli une première cohorte de six startups. À Montréal, le programme Propolys de Polytechnique Montréal propose un parcours entrepreneurial spécialisé en cybersécurité de dix mois permettant à dix projets d'aboutir au lancement de leur entreprise[27]. Finalement, l'organisme Cybereco a lancé en novembre 2023 son Carrefour Cyber, qui ambitionne de devenir un complexe d'innovation et de commercialisation focalisé sur la cybersécurité des infrastructures essentielles. Le Carrefour Cyber héberge une dizaine de startups et de scale-ups en cybersécurité qui peuvent y cultiver leurs réseaux d'affaires[28].

3.6 Organismes de soutien à la cybersécurité

Deux grandes catégories d'organismes contribuent également au financement de la recherche et de l'innovation, au soutien de l'entreprenariat et à la constitution et consolidation de grappes technologiques contribuant à la croissance d'un écosystème de la cybersécurité robuste. Certains de ces organismes relèvent du secteur public, alors que d'autres sont des organismes à but non lucratif (OBNL).

3.6.1 Organismes publics

Les ministères provinciaux et fédéraux de l'économie et de l'innovation disposent de programmes de soutien génériques et spécifiques permettant de soutenir l'écosystème de la cybersécurité. Le Ministère de l'Économie, de l'innovation et de l'énergie a ainsi annoncé une aide financière de 3,5 millions de dollars à la grappe In-Sec-M en avril 2023 dans le cadre de son initiative stratégique d'Offensive en transformation numérique (OTN), afin que la grappe offre des activités de sensibilisation et de formation à la cybersécurité à des entreprises québécoises de tous secteurs[29]. Le gouvernement fédéral débloquait pour sa part 80 millions de dollars en février 2022 afin de financer le Réseau d'innovation pour la cybersécurité, dont le mandat est d'intensifier la recherche et le développement, d'accroître la commercialisation et de former des personnes spécialisées en cybersécurité[30].

Les fonds et programmes de soutien à la recherche peuvent également être inclus dans cette catégorie d'acteurs, qu'il s'agisse de programmes récurrents destinés à soutenir les entreprises et universités développant des solutions innovantes, comme c'est le cas avec le programme IDEeS (Innovation pour la défense, l'excellence et la sécurité) du gouvernement fédéral[31], ou à travers des initiatives ponctuelles comme la décision du Scientifique en chef du Québec d'octroyer 2,5 millions de dollars à l'Université du

[26] Repéré à https://www.cilex.ca/maillage-cybersecurite.
[27] Repéré à https://www.polymtl.ca/propolys/parcours-entrepreneuriaux/parcours-entrepreneurial-en-cybersecurite.
[28] Repéré à https://cybereco.ca/carrefour-cyber/.
[29] Repéré à https://www.quebec.ca/nouvelles/actualites/details/offensive-de-transformation-numerique-pres-de-37-m-pour-accelerer-le-virage-numerique-des-entreprises-quebecoises-46807.
[30] Repéré à https://www.canada.ca/fr/innovation-sciences-developpement-economique/nouvelles/2022/02/le-gouvernement-du-canada-annonce-la-prochaine-phase-de-renforcement-du-reseau-dinnovation-pour-la-cybersecurite.html.
[31] Repéré à https://www.canada.ca/fr/ministere-defense-nationale/programmes/idees-defense.html.

Québec en Outaouais en octobre 2023 pour créer un centre de recherche et d'innovation en cybersécurité et société[32].

L'écosystème de la cybersécurité peut également bénéficier du soutien d'organismes gouvernementaux à travers des programmes destinés à accélérer le développement de technologies émergentes telles que l'intelligence artificielle ou l'informatique quantique, pour lesquelles les différents paliers de gouvernement ont dégagé des ressources conséquentes au cours des derniers cycles budgétaires et qui propulseront les prochaines générations de solutions de cybersécurité.

3.6.2 Organismes à but non lucratif

Par ailleurs, le soutien des organismes publics est relayé et amplifié au Québec par deux grappes industrielles co-financées par le secteur privé et différents paliers de gouvernement : Cybereco et In-Sec-M. Le mandat principal de ces deux organismes est de structurer et promouvoir l'expertise des entreprises locales. Dotés de conseils d'administration représentatifs de l'écosystème dans toute sa diversité, ils peuvent compter sur des dizaines de membres actifs qui s'impliquent dans des activités destinées à accélérer le développement d'un écosystème canadien de la cybersécurité vigoureux et innovant. Ces deux grappes offrent, par exemple, selon leurs missions respectives, des communautés de pratique à leurs membres, de grandes conférences réunissant tous les acteurs de l'écosystème, des missions de développement commercial à l'étranger, des outils et programmes de soutien aux PME, ainsi que des parcours d'innovation pour les entrepreneurs en démarrage et des initiatives visant à développer le réservoir de talents en cybersécurité[33].

Un autre OBNL contribuant au soutien de l'écosystème est Prompt, un regroupement sectoriel en recherche industrielle (RSRI) spécialisé dans le secteur des technologies numériques qui, depuis 2019, a octroyé plus de 44,5 millions de dollars afin de financer plus de 150 projets d'entreprise dans le cadre des programmes PICQ1 et PICQ2 (pour Programme d'innovation en cybersécurité au Québec) (Prompt, 2023). Le financement offert provient du ministère de l'Économie, de l'Innovation et de l'Énergie. Prompt collabore étroitement avec les autres acteurs du milieu afin d'offrir un financement adapté et évoluant selon les besoins de l'industrie.

3.7 Organismes de formation et de recherche (monde académique)

Les universités et les collèges québécois ont établi des centres et des unités de recherche de calibre mondial qui contribuent au développement de technologies, de processus et de bonnes pratiques susceptibles de renforcer la cybersécurité, même s'il est apparu dans le chapitre précédent que les liens entre le monde académique et les entreprises de cybersécurité pourraient faire l'objet de collaborations plus approfondies.

Trois universités se distinguent notamment par une masse critique de chercheurs en cybersécurité provenant de disciplines diverses et unis au sein d'entités fédératrices : l'Université Concordia et son pôle

[32] Repéré à https://uqo.ca/nouvelles/52373.
[33] Pour plus d'informations, voir https://cybereco.ca/ et https://insecm.ca/.

de recherche en cybersécurité réunit 18 professeurs, dont trois sont à la tête de chaires de recherche industrielles du CRSNG[34]. L'Université de Sherbrooke a fondé le Groupe de recherche interdisciplinaire en cybersécurité (GRIC) qui mobilise 20 professeures et professeurs provenant de cinq facultés et écoles différentes (sciences, génie, droit, gestion et science politique)[35]. Finalement, Polytechnique Montréal, l'Université de Montréal et HEC ont pour leur part créé l'Institut multidisciplinaire en cybersécurité et cyberrésilience (IMC2) qui réunit 45 professeures et professeurs des trois institutions[36].

Des pôles d'expertise plus concentrés existent aussi à l'Université Laval, qui héberge une chaire de recherche sur la gouvernance et la gestion de la cybersécurité, conjointement financée par Microsoft et le MCN[37], ainsi que le pôle d'expertise en cybersécurité et impacts sociétaux à l'OBVIA[38]; à l'UQAM, avec la Chaire de recherche du Canada en analyse respectueuse de la vie privée et éthique des données massives et le Groupe de recherche sur la cybersécurité[39]; à l'Université McGill, avec la Chaire de recherche du Canada en forage des données pour la cybersécurité[40]; à l'UQO, qui héberge un Laboratoire de recherche en sécurité informatique piloté par trois professeurs; ou encore à l'UQAC avec la Chaire de recherche institutionnelle en cyberdéfense et en protection des données personnelles[41].

Le Cégep de l'Outaouais a également fondé en juin 2018 un centre collégial de transfert de technologie (CCTT) se spécialisant dans la cybersécurité et nommé CyberQuébec, dont les champs d'intervention privilégiés incluent des services d'accompagnement en cybersécurité et transition numérique à destination des PME, la sensibilisation, et dans une moindre mesure la recherche appliquée[42].

De surcroît, les cégeps et les universités contribuent à la formation de la main d'œuvre par la création de programmes de premier, deuxièmes et troisièmes cycles destinés à répondre aux besoins des employeurs et à l'évolution des compétences requises. Un effort de cartographie initié par le Réseau intégré sur la cybersécurité (SERENE-RISC) en 2018 et mis à jour par l'IMC2 en 2024 révèle ainsi l'existence au Québec de 34 programmes de formation accessibles au niveau collégial et universitaire dispensant plus de 300 cours couvrant les aspects techniques, organisationnels, juridiques et sociaux de la cybersécurité[43].

3.8 Autorités régulatrices

Face à l'insécurité croissante, les gouvernements ont un rôle à jouer afin de limiter et d'atténuer les risques associés au cyberespace et aux nouvelles technologies (Institut d'études internationales de

[34] Repéré à https://www.concordia.ca/fr/nouvelle-generation/cybersecurite.html.
[35] Repéré à https://gric.recherche.usherbrooke.ca/.
[36] Repéré à https://i-mc2.ca/linstitut/notre-equipe/.
[37] Repéré à https://www.fsa.ulaval.ca/nouvelles/nouvelle-chaire-de-recherche-sur-la-gouvernance-et-la-gestion-de-la-cybersecurite/.
[38] Repéré à https://www.obvia.ca/poles-expertise/pole-dexpertise-en-cybersecurite-et-impacts-societaux.
[39] Repéré à https://sec.uqam.ca/.
[40] Repéré à https://www.mcgill.ca/sis/people/faculty/fung.
[41] Repéré à https://cybpro.ca/.
[42] Repéré à https://cyberquebec.org/wp-content/uploads/2024/02/Planification-quinquennale-2024-2029-de-CyberQuebec.pdf.
[43] Repéré à https://www.serene-risc.ca/fr/repertoire-des-programmes-en-cybersecurite.

Montréal, 2020, p. 1). Au cours des dernières années, les États se sont dotés de nouvelles mesures législatives et règlementaires pour encadrer le cyberespace et renforcer la protection des citoyens. Ces nouveaux cadres ont des implications significatives pour l'industrie de la cybersécurité. En effet, ceux-ci incitent les organisations à se doter de mesures de sécurité supplémentaires et à adopter des approches plus proactives pour protéger les données personnelles qu'elles détiennent.

3.8.1 Contexte québécois

Du côté provincial, en 2019, le gouvernement du Québec a mis sur pied le *Centre gouvernemental de cyberdéfense* faisant partie du Secrétariat du Conseil du trésor et, depuis 2022, du Ministère de la Cybersécurité et du numérique. « Le Centre gouvernemental de cyberdéfense joue le rôle d'entité de confiance au sein du réseau gouvernemental de cyberdéfense. Il a notamment comme responsabilités de coordonner les efforts en cybersécurité des organismes publics et des centres opérationnels de cyberdéfense, d'assurer la prise en charge des incidents de sécurité à portée gouvernementale et de jouer un rôle collaboratif dans l'écosystème de cybersécurité québécois, national et international » (Fortin et al., 2021). L'année suivante, en 2020, le gouvernement du Québec a publié sa politique gouvernementale de cybersécurité dans laquelle est mis à l'avant-plan l'ouverture ainsi que le partage des connaissances, de l'expertise et des pratiques exemplaires en matière de cybersécurité (Fortin et al., 2021). Le 1er janvier 2022, le gouvernement du Québec a créé le ministère de la Cybersécurité et du Numérique qui est chargé d'animer et de coordonner les actions de l'État dans les domaines de la cybersécurité et du numérique.

Plus tard, en septembre 2022, l'adoption de la Loi 25 est venue contraindre toute organisation privée à faire preuve de plus de transparence en matière de collecte et d'utilisation des renseignements personnels, a augmenté les obligations légales et la responsabilité des entreprises dans ce domaine, les oblige à divulguer les cyberattaques et les incidents menaçant les données personnelles, et prévoit des sanctions plus sévères en cas de non-conformité (Groupe Novipro et Léger, 2023). Ce cadre règlementaire renforcé pousse les organisations à consolider les mesures de cybersécurité, à améliorer les processus de gestion des incidents, à intensifier la sensibilisation et la formation des employés, et à faire appel à des experts en cybersécurité. Les différentes mesures de la Loi 25 sont progressivement entrées en vigueur sur une période de trois ans, ce qui rend encore difficile l'analyse de ses impacts directs et indirects sur le marché de la cybersécurité. La Commission d'accès à l'information (CAI) est l'autorité détenant les pouvoirs d'évaluation et de sanction prévus par la Loi, qui publie également les informations concernant les incidents de confidentialité qui lui sont déclarés.

Des autorités régulatrices sectorielles, comme l'Autorité des marchés financiers (AMF) par exemple, incorporent également la cybersécurité dans leurs activités de surveillance et de contrôle, venant ainsi définir les mesures à prendre afin de réduire l'exposition aux risques de cyberattaque[44].

[44] Repéré à https://lautorite.qc.ca/professionnels/obligations-et-formalites-administratives/protection-des-donnees-et-des-renseignements-personnels.

3.8.2 Contexte fédéral

Du côté fédéral, en 2018, le gouvernement canadien s'est doté d'une Stratégie nationale de cybersécurité (Sécurité publique Canada, 2018). Découlant de cette stratégie, la même année, le Centre canadien pour la cybersécurité (CCCS) a vu le jour (Centre canadien pour la cybersécurité, 2022). « En tant qu'autorité technique du Canada en matière de cybersécurité, l'équipe du CCCS met à profit son expertise afin de protéger l'information et les systèmes sur lesquels se fient les Canadiens tous les jours » (Centre canadien pour la cybersécurité, 2022). Outre les conseils qu'il dispense aux entreprises de toutes tailles et au grand public, le CCCS collabore également avec les opérateurs d'infrastructures essentielles afin de les aider à sécuriser leurs systèmes. Des partenariats stratégiques sont noués avec des entreprises de cybersécurité afin d'évaluer les technologies émergentes qui apparaissent sur le marché. Notamment, le CCCS collabore avec le programme d'innovation Construire au Canada en jouant le rôle d'autorité technique afin de soutenir les entreprises de cybersécurité désirant commercialiser des produits innovants[45].

De manière plus contraignante, certaines autorités régulatrices fédérales sectorielles énoncent des exigences de plus en plus précises en matière de cybersécurité, auxquelles doivent se conformer les entités réglementées. Le Bureau du surintendant des institutions financières (BSIF) a ainsi publié en juillet 2022 ses lignes directrices sur la gestion du risque lié aux technologies et au cyberrisque, qui viennent détailler les mesures organisationnelles et techniques que les banques et les sociétés d'assurance doivent implanter pour être jugées conformes[46]. Dans le secteur des télécommunications, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) est notamment responsable de l'encadrement des fournisseurs de services de télécommunication[47]. Ses activités règlementaires liées à la cybersécurité se sont focalisées au cours des dernières années sur la lutte contre la large diffusion des pourriels en ligne et la propagation des logiciels malveillants via le blocage des réseaux de zombies (des systèmes informatiques infectés à l'insu de leurs propriétaires légitimes), d'une part, et sur la résilience accrue des systèmes de communication, d'autre part (CRTC, 2023). Par leurs exigences de plus en plus détaillées en matière de cybersécurité, ces autorités régulatrices poussent les entités réglementées à réviser leurs politiques internes, à rehausser leurs capacités techniques et à se procurer des solutions plus performantes sur le marché des produits et des services.

Finalement, le Parlement fédéral est en train d'examiner le projet de loi C-26, qui est en deuxième lecture au Sénat et qui renforcerait le cadre réglementaire de la cybersécurité auquel seraient soumis quatre secteurs d'activité jugés essentiels pour l'économie : les télécommunications, la finance, les transports, et l'énergie. Les opérateurs issus de ces quatre secteurs se verraient imposer de nouvelles obligations dans quatre domaines : l'élaboration et l'implantation de programmes de cybersécurité ; l'atténuation

[45] Repéré à https://www.cyber.gc.ca/fr/propos-centre-cybersecurite/collaboration-avec-secteur-prive.
[46] Repéré à https://www.osfi-bsif.gc.ca/fr/consignes/repertoire-consignes/gestion-du-risque-lie-technologies-du-cyberrisque.
[47] Repéré à https://crtc.gc.ca/fra/comm/telecom/.

des risques liés à la chaîne d'approvisionnement numérique ; la déclaration des incidents de sécurité subis ; et la conformité à toute directive ministérielle relative à la cybersécurité[48].

3.9 Associations professionnelles et initiatives bénévoles

La dernière catégorie d'acteurs de l'écosystème comprend les associations professionnelles, OSBL et groupes communautaires qui organisent des activités contribuant au partage et à la mobilisation des connaissances.

Les associations professionnelles telles qu'ISACA[49], l'ISC2[50], l'ASIMM[51] ou l'ASIQ[52] offrent à leurs membres des activités de réseautage, des événements tels que des séminaires et des conférences favorisant l'échange de connaissances, ou encore des programmes de certification permettant aux professionnels de la cybersecurité de faire valoir leur expertise selon des normes internationalement reconnues. Leur existence favorise ainsi la circulation informelle d'informations entre les entreprises de cybersécurité et leurs clients, ainsi qu'entre les acheteurs qui souhaitent échanger sur leur expérience avec des fournisseurs spécifiques.

Des organisations comme CyberCap[53], l'École Cybersécurité[54], ou Co-savoir[55] diffusent des contenus de formation et de sensibilisation reliés aux grands enjeux de la cybersécurité auprès de segments de la population qui ne sont pas directement en contact avec les entreprises du secteur. Ces groupes ont néanmoins besoin d'améliorer leurs connaissances afin de maintenir une protection adéquate contre les risques numériques ou de profiter des opportunités professionnelles du secteur : CyberCap a ainsi développé en collaboration avec Cybereco une formation destinée aux élèves du secondaire qui favorise l'adoption de comportements sécuritaires en ligne tout en éveillant leur intérêt pour les métiers de la cybersécurité et du numérique. Cette formation a été suivie par plus de 6 200 élèves de 12 à 17 ans[56]. Pour sa part, l'École Cybersécurité dispense des formations plus techniques accessibles en ligne, a créé un répertoire des expertes en cybersécurité afin de contribuer à une meilleure visibilité des femmes dans le domaine, et décerne chaque année le trophée Cybertalent afin de susciter les vocations et reconnaître les parcours inspirants parmi les jeunes de moins de 30 ans[57]. Dans un registre différent, Co-savoir (anciennement le Centre de documentation sur l'éducation des adultes et la condition féminine) a développé une trousse adaptée aux besoins et aux capacités des organismes communautaires souhaitant renforcer leur sécurité numérique et la confidentialité des données qu'ils traitent[58]. Ces trois exemples ne

[48] Repéré à https://www.parl.ca/legisinfo/fr/projet-de-loi/44-1/c-26.
[49] Repéré à https://engage.isaca.org/montrealchapter/homepage.
[50] Repéré à https://isc2mtl.ca/.
[51] Repéré à https://www.asimm.org/.
[52] Repéré à https://asiq.org/.
[53] Repéré à https://cybercap.qc.ca/.
[54] Repéré à https://www.ecolecyber.ca/.
[55] Repéré à https://cdeacf.ca/boite-outils-cybersecurite.
[56] Repéré à https://cybercap.qc.ca/cybereco-et-cybercap-preparent-les-eleves-des-ecoles-secondaires-du-quebec-a-relever-les-defis-lies-a-lutilisation-des-outils-numeriques/.
[57] Repéré à https://www.ecolecyber.ca/.
[58] Repéré à https://cdeacf.ca/boite-outils-cybersecurite.

sont pas exhaustifs et de nombreuses autres initiatives existent au Québec. Ces dernières ne sont toutefois pas recensées de manière centralisée, ce qui limite leur visibilité.

Une dernière contribution de taille est réalisée par les compétitions de piratage éthique et les conférences sur les vulnérabilités les plus récentes, l'évolution des attaquants ou les meilleures pratiques de sécurité. Ces événements que l'on peut qualifier de communautaires par les valeurs éducatives et d'inclusivité qu'ils prônent sont organisés par des équipes de bénévoles qui consacrent de nombreuses heures à la conception d'épreuves stimulantes et de programmes diversifiés qui réunissent plusieurs centaines de participants. Bien que ces évènements n'aient pas de visées commerciales, ils contribuent à consolider les liens transversaux entre les diverses entités de l'écosystème et à renforcer les compétences de la main d'œuvre. Parmi les événements plus réputés figurent NorthSec[59], MontreHack[60] et BSides[61] à Montréal, et le HackFest[62] et SéQCure[63] à Québec. Ces initiatives sont complémentaires aux conférences professionnelles organisées par les grappes industrielles ou des entreprises privées, comme le sommet ITSec, le Forum InCyber, GoSec, ou la Cyber Conférence.

3.10 Quelques éléments de comparaison avec des écosystèmes de calibre mondial

Dans le cadre de ses missions internationales de développement, la grappe technologique In-Sec-M a eu l'occasion d'approfondir ses connaissances sur le fonctionnement d'autres écosystèmes de cybersécurité, aux États-Unis, en Israël, en France, ou encore en Allemagne (voir les analyses sommaires en annexe 1). Les paragraphes qui suivent identifient les atouts que mobilisent les écosystèmes jugés comme les plus performants à l'échelle mondiale, sur la base de ces connaissances de terrain. Ces caractéristiques sont examinées de manière sélective à la lumière des propriétés de l'écosystème québécois afin d'en tirer des enseignements utiles à ce dernier.

Cinq grands facteurs semblent expliquer la vigueur des écosystèmes de cybersécurité jugés les plus performants. Le premier est celui d'une volonté gouvernementale affirmée de coordination par le biais de stratégies nationales qui permettent à l'ensemble des acteurs de comprendre leur rôle et d'accéder à des interlocuteurs disposant des ressources pour faciliter la coopération et les initiatives synergiques. Le Canada dispose bien d'une stratégie nationale de cybersécurité, mais celle-ci date déjà de 2018 et la nouvelle mouture de cette stratégie n'a toujours pas été rendue publique au moment d'écrire ces lignes. Le Québec a aussi adopté à l'été 2024 une Stratégie gouvernementale de cybersécurité et du numérique pour la période 2024-2028, mais ses objectifs et ses moyens restent focalisés sur les services publics.

Un deuxième facteur de réussite concerne la mise en place de structures favorisant l'entreprenariat en cybersécurité. Israël se définit par exemple comme la « Startup Nation » et valorise cette culture

[59] Repéré à https://nsec.io/.
[60] Repéré à https://montrehack.ca/.
[61] Repéré à https://bsidesmtl.ca/.
[62] Repéré à https://hackfest.ca/.
[63] Repéré à https://seqcure.org/.

d'entreprenariat aussi bien auprès de ses innovateurs que des investisseurs étrangers. Les États-Unis se sont dotés d'incubateurs et d'accélérateurs renommés qui attirent des entrepreneurs du monde entier dans la Silicon Valley ou dans la banlieue de Washington. La France a, quant à elle, conçu le label « France Cybersecurity » afin de promouvoir les solutions de cybersécurité françaises à l'international et de différencier l'offre de ses entrepreneurs sur ce marché extrêmement compétitif. Tous ces exemples impliquent des efforts considérables de pilotage de la part des pouvoirs publics ou d'investisseurs privés.

Un troisième facteur relève d'investissements massifs en recherche et développement (R&D) de la part de gouvernements qui utilisent des canaux variés : agences du secteur de la défense aux États-Unis (DARPA) et en Israël (Unité 8200), instituts de recherche dédiés à la recherche fondamentale et appliquée en France (INRIA et CEA) ou en Allemagne (Fraunhofer Institute). Dans tous les cas, des stratégies visant à créer des masses critiques d'excellence en recherche sont mises en œuvre, là où le Canada et le Québec privilégient plutôt une distribution fragmentée des ressources.

Un quatrième facteur est l'existence de systèmes de formation et d'universités de calibre mondial qui offrent des programmes réputés en cybersécurité, qu'il s'agisse de conduire des projets de recherche appliqués ou de former des experts hautement qualifiés. Des mécanismes parallèles de formation comme des programmes de certification professionnelle ou la formation continue dispensée dans certaines unités militaires ou de renseignement jouent également un rôle important. Au Québec, des pôles de formation émergent au niveau collégial et universitaire, mais il est encore difficile d'évaluer la qualité des programmes offerts et leur alignement réel avec les besoins de l'écosystème.

Un cinquième et dernier facteur commun aux écosystèmes de cybersécurité de haute performance est l'encouragement des collaborations formelles entre acteurs publics et privés. La France a ainsi créé au début de l'année 2022 à Paris un Campus Cyber, qui a aussi joué un rôle de catalyseur en faisant cohabiter entreprises, services publics et établissements d'enseignement et de recherche dans un immeuble où près de 280 000 pieds carrés sont consacrés à la cybersécurité. Israël a pour sa part inauguré son campus CyberSpark dans le désert du Néguev au milieu des années 2010, où se côtoient entrepreneurs, chercheurs et militaires. Les États-Unis ont pour leur part développé autour de la Cybersecurity & Infrastructure Security Agency (CISA) tout un ensemble de programmes de partage de renseignements sur les risques cyber, qui sont venus consolider les échanges qui existaient déjà depuis la fin des années 1990 entre les opérateurs de 27 industries jugées essentielles via le système des Information Sharing and Analysis Centers (ISACs)[64]. Ces initiatives favorisent l'agilité des partenariats qui peuvent rapidement réagir aux conditions changeantes de l'écosystème et saisir de nouvelles opportunités quand elles se présentent.

Ces cinq facteurs illustrent le rôle central que jouent les acteurs publics et parapublics dans la création et le maintien d'un écosystème de la cybersécurité robuste, capable de répondre aux besoins nationaux et de se démarquer sur les marchés internationaux. Ce rôle implique la recherche d'un délicat équilibre entre des efforts de coordination s'appuyant sur une vision partagée et l'injection de ressources significatives, d'une part, ainsi que la valorisation des compétences et des capacités des autres acteurs de l'écosystème,

[64] Repéré à https://www.nationalisacs.org/about-isacs.

qui doivent pouvoir maintenir des marges d'initiative importantes afin de développer des approches innovantes.

4. DÉFIS ET OPPORTUNITÉS POUR L'INDUSTRIE DE LA CYBERSÉCURITÉ AU QUÉBEC

Pour certaines questions du sondage, les entreprises de cybersécurité avaient la possibilité de compléter leurs choix de réponses par des précisions qualitatives sur les principaux défis auxquels elles font face. Quatre entrevues plus approfondies ont également été menées avec les dirigeants d'entreprises ayant participé au sondage. Cette section du rapport présente les principaux enseignements tirés de ces réponses[65].

4.1 Talents et main-d'œuvre qualifiée[66]

Les résultats de l'enquête reflètent ce que nous avons observé dans la revue documentaire. D'après les résultats du sondage et les entretiens, la main-d'œuvre semble occasionner cinq principaux défis aux répondants qui sont présentés par ordre décroissant de fréquence d'apparition dans les réponses.

Tout d'abord, le défi le plus fréquemment mentionné est celui de la rétention du personnel, qui apparaît dans 38,9% des réponses (14 entreprises)[67]. Les répondants éprouvent de la difficulté à retenir les employés formés, particulièrement dans un contexte où ils se trouvent en concurrence avec de grandes entreprises qui peuvent offrir des niveaux de rémunération plus élevés, ainsi que des conditions de travail et des opportunités de promotion très attractives. Cette forte compétition pour des ressources humaines en nombre restreint fait en sorte qu'il devient difficile de garder certaines expertises et que plusieurs postes subissent des niveaux de rotation élevés.

Dans le même ordre d'idées, face à cette réalité du marché, 36,1% des répondants (13 entreprises) expriment que la compensation est également un défi. Le coût élevé de la main-d'œuvre spécialisée et les exigences salariales agressives des employés potentiels représentent des défis particulièrement épineux pour des entreprises en démarrage. Il leur est difficile de rivaliser avec les offres salariales des

[65] Afin de faciliter l'analyse des données non structurées et de limiter les biais de sélection et d'interprétation, les données qualitatives ont été codées et catégorisées selon les principes de l'analyse thématique à l'aide de deux applications d'intelligence artificielle générative : ChatGPT 4o et Claude 3.5. Les données ont été d'abord anonymisées, puis elles ont été ingérées par les deux modèles, accompagnées de directives demandant à ces derniers d'identifier les principales thématiques présentes dans les réponses et de classer celles-ci en fonction de leur fréquence d'apparition dans les thèmes identifiés. Le recours à deux modèles au lieu d'un seul permet de comparer les résultats et de ne conserver que ceux qui font consensus, c'est-à-dire les plus robustes. Les résultats ont ensuite été contre-vérifiés afin de s'assurer de leur intégrité et de détecter toute possibilité d'erreur introduite par les modèles.

[66] Défis et opportunités relatives à la main d'œuvre au sein des entreprises de cybersécurité au Québec (Nombre de répondants au sondage : 36).

[67] Le total des réponses dépasse 100% puisque les répondants pouvaient mentionner plusieurs enjeux ou défis dans leurs réponses qualitatives.

grandes entreprises de l'industrie, d'autant plus que ces dernières sont prêtes à recruter des employés en télétravail dans des zones où elles n'ont pas de place d'affaires.

Le recrutement de talents qualifiés dans un contexte de pénurie constitue un troisième enjeu à surmonter pour 27,8% des répondants (10 entreprises). Le marché de l'emploi ne semble pas disposer d'une quantité suffisante de ressources qualifiées et les entreprises québécoises de cybersécurité éprouvent de la difficulté à trouver les candidats qui répondent à leurs besoins. Certains domaines d'expertise semblent être particulièrement affectés par cette pénurie. Les petites et moyennes entreprises, dont la visibilité sur le marché est moins grande que celle de leurs rivaux internationaux, peinent également à attirer l'attention de recrues compétentes.

La formation et le développement des compétences représente un quatrième défi à signaler pour 16,7% des répondants (6 entreprises). Puisque certains répondants éprouvent de la difficulté à trouver des employés pleinement qualifiés, ceux-ci doivent leur offrir de la formation à l'interne. Mais les coûts induits et le temps nécessaire pour former les employés se répercutent sur les autres activités de l'entreprise et peuvent temporairement freiner l'innovation et le développement commercial lorsque les ressources sont limitées.

Finalement, l'immigration et la mobilité internationale représentent un enjeu pour 5,6% des répondants (2 entreprises). Les entreprises qui y ont recours cherchent ainsi à pallier la pénurie locale de main d'oeuvre, mais un des répondants qui s'est tourné vers cette solution a toutefois mentionné la lourdeur du processus. Une autre entreprise a également indiqué planifier de mettre en place des bureaux à l'étranger pour offrir un programme de mobilité internationale et de travail à distance pour certaines tâches. Mais là encore, des enjeux de ressources limitées sont à anticiper pour des entreprises de petite et moyenne taille.

Malgré ces défis, certains répondants trouvent des solutions et des opportunités pour leurs entreprises en matière de recrutement et de rétention. À titre d'exemple, un répondant mentionne maintenant recruter partout à travers le Canada puisque son entreprise est dématérialisée, même si cela peut générer des défis connexes comme un sentiment d'appartenance moindre. Un autre, mise quant à lui, sur la culture d'entreprise pour attirer et retenir les employés. Bien que cette pratique soit vorace en ressources, certains répondants procèdent à l'embauche d'étudiants et de stagiaires dans le but de les garder à l'emploi de leur entreprise. Cette pratique a aussi été répertoriée auprès de deux participants aux entretiens. Un autre a d'ailleurs proposé la piste de solution suivante : « obtenir des subventions pour financer la formation, ce qui créerait de la loyauté. Cela nous permettrait de dégager entre 200 et 300 heures, soit 10 % du temps d'un salarié par exemple, cela serait très utile, en particulier pour la main-d'œuvre junior ».

4.2 La recherche et l'innovation en cybersécurité au Québec[68]

En ce qui concerne la recherche en partenariat, les principales contraintes relatées par les répondants au sondage sont liées aux longs délais bureaucratiques découlant des interactions avec les universités ou les organismes de soutien, à l'alignement des priorités et des objectifs entre les divers partenaires, aux questions portant sur la gestion de la propriété intellectuelle et à celles portant sur le manque de ressources. Les délais jugés exagérés pour mettre en place des partenariats et finaliser un projet ne sont pas en adéquation avec la rapidité à laquelle évolue le secteur et constituent un irritant pour 27% des répondants (10 entreprises), que ces retards soient vécus à l'étape de la mise en place des partenariats, lors de leur gestion quotidienne, ou lorsque vient le temps de générer des résultats rapides. Ce décalage entre un besoin de réactivité de la part des entreprises et un temps académique beaucoup plus lent constitue manifestement un facteur dissuasif pour les entreprises.

Le manque d'alignement des besoins entre le monde universitaire et celui des entreprises cause aussi des frictions qui rebutent 22% des répondants (8 entreprises). Les entreprises entendent par-là l'écart entre leurs besoins en recherche appliquée et les intérêts en recherche fondamentale de leurs interlocuteurs académiques, l'identification de partenaires académiques fiables, ou encore les différences radicales de culture entre les deux communautés.

La gestion de la propriété intellectuelle donne également du fil à retordre aux entreprises qui collaborent avec le monde académique, 19% des répondants (7 entreprises) y voyant un enjeu. Ce sont en particulier les fortes contraintes imposées par les universités sur l'utilisation de la propriété intellectuelle élaborée en partenariat qui sont perçues comme une barrière à son partage. Cela semble par effet de cascade étirer les délais de livraison pour les entreprises de cybersécurité et créer pour ces dernières une incertitude commerciale.

Face à ces trois grandes catégories de complications et à la lourdeur des processus bureaucratiques qui en découlent, les répondants se trouvent confrontés à des coûts qu'il leur semble difficile de justifier et d'assumer. L'insuffisance des ressources financières est mentionnée par 16% des répondants (6 entreprises), et cela semble inclure les financements obtenus de sources gouvernementales pour soutenir ce genre de projets, qui sont jugés insuffisants face aux coûts réels induits par leur réalisation.

4.3 Le financement de l'innovation

Quant à l'innovation, le principal enjeu soulevé par les répondants au sondage est le financement. La transformation de l'innovation en capital peut exiger du temps. Le retour sur l'investissement n'est pas

[68]Principales contraintes à l'établissement d'activité de recherche en innovation auprès d'un partenaire académique ou privé (Nombre de répondants au sondage : 37) et Enjeux relatifs aux investissements en recherche-innovation au sein des entreprises (Nombre de répondants au sondage : 36).

garanti. 34% des répondants (16 entreprises) relatent les défis auxquels ils sont confrontés en matière de financement et d'accès au capital, ce qui freine leurs élans innovateurs.

Le soutien gouvernemental constitue aussi une préoccupation pour les répondants, qui notent que les programmes d'aides sont complexes et peu adaptés à la réalité des startups. La reconduction imprévisible et les critères changeants des programmes peuvent aussi constituer un élément d'instabilité pour les entreprises. Les incitatifs gouvernementaux demandent des investissements importants en temps, dû à leur lourdeur administrative lors de la préparation des dossiers, ce qui s'avère prohibitif selon plusieurs répondants. Il devient enfin difficile pour certains répondants de se repérer à travers une offre de programmes diversifiée. Ces commentaires sembleraient indiquer que l'enjeu central concerne le ciblage adéquat de ces programmes et leur cohérence globale, plutôt que le volume du soutien disponible.

L'ensemble des politiques gouvernementales peut influer sur le comportement des entreprises de deux manières opposées :

Avantages	Inconvénients
▪ Stimuler l'innovation : les investissements, mesures fiscales et subventions peuvent encourager la recherche et le développement dans le domaine de la cybersécurité, favorisant l'innovation et le maintien d'une main-d'œuvre hautement qualifiée. ▪ Sécurité accrue : en rendant les solutions de cybersécurité plus accessibles et abordables pour les organisations publiques et privées, le gouvernement contribue à la protection des infrastructures critiques et à la sécurité des données. ▪ Développement économique : ces mesures peuvent attirer des entreprises de cybersécurité et des talents dans une région, stimulant ainsi l'économie locale et la positionnant comme un centre d'excellence en cybersécurité.	• Dépendance aux subventions : une trop grande dépendance aux aides gouvernementales peut rendre les entreprises de cybersécurité vulnérables aux changements de politiques et moins enclines à innover et à être compétitives sur le marché libre. • Allocation des ressources : il existe un risque que les subventions ne soient pas toujours allouées aux projets les plus méritants ou efficaces, ce qui pourrait entraîner une mauvaise utilisation des fonds publics. • Distorsion du marché : les interventions gouvernementales peuvent parfois fausser le marché, favorisant certaines entreprises ou technologies au détriment d'autres et inhibant la concurrence saine.

Pour maximiser les bénéfices et minimiser les inconvénients, il est crucial que les mesures gouvernementales soient bien conçues, ciblées et mises en œuvre de manière transparente et équitable. Une collaboration étroite avec l'industrie, les institutions académiques et les autres parties prenantes est essentielle pour s'assurer que les politiques soutiennent efficacement l'écosystème existant et qu'elles tiennent compte de l'évolution constante des menaces et des technologies requises pour y répondre.

4.4 Commercialisation : enjeux et défis[69]

Lorsqu'interrogés au sujet des plus grands enjeux en ce qui a trait à l'offre de services ou de produits de cybersécurité, les répondants ont mis de l'avant trois grands défis particulièrement associés aux interactions commerciales avec les acheteurs gouvernementaux et les grands donneurs d'ordre. Tout d'abord, la complexité et les délais prolongés des processus d'appel d'offre sont signalés par 44% des répondants, qui déplorent la lourdeur administrative associée à ces processus et les délais très longs pour la prise de décision, ce qui étire les cycles de vente de manière prohibitive pour les PME.

Un deuxième défi concerne les critères de sélection appliqués par les grands donneurs d'ordre pour sélectionner leurs fournisseurs en cybersécurité, qui ne semblent pas alignés avec la réalité des PME: 35% des répondants estiment ainsi que la rigidité des critères employés ne correspond pas à un paysage des risques très dynamique et en constante évolution, que l'accent mis sur le prix plutôt que sur la qualité des prestations nuit au déploiement de solutions performantes, et que les exigences de qualification pour participer aux appels d'offre sont excessives et dissuasives pour les PME. Cela se traduit selon les répondants par une réticence des grands donneurs d'ordre à faire confiance aux startups et une préférence pour les solutions proposées par les grandes entreprises établies.
Ces caractéristiques des appels d'offre induisent le sentiment chez 18% des répondants que les PME locales sont défavorisées au profit des grandes entreprises américaines et que les segments les plus profitables du marché de la cybersécurité ne leurs sont pas accessibles. Lors des entretiens, une entreprise répondante traite également de ce problème : « La cause probable est l'image des produits du Québec, les acheteurs supposent que nous ne sommes pas à la hauteur. C'est un problème de perception très grave ». Dans le même ordre d'idée, un participant aux entretiens précise comment cette dynamique du marché canadien impacte son entreprise : « En ce qui concerne la dynamique du marché, le Canada peut être un endroit difficile pour lancer une entreprise en cybersécurité. La tendance est d'acheter des produits aux États-Unis auprès de grandes entreprises, ce qui signifie que nous devons déjà vendre aux États-Unis avant de nous développer au Canada. Les enjeux de commercialisation sont liés au capital, ce qui limite le développement de notre entreprise ».

Si l'accès au marché des grands donneurs d'ordre est ardu, celui des PME soulève également un certain nombre de défis qui constituent autant d'obstacles vers la croissance et la profitabilité pour les entreprises

[69] Barrières à l'offre de services ou de produits en cybersécurité au Québec (Nombre de répondants au sondage : 44); Enjeux particuliers dans le processus de vente aux acheteurs gouvernementaux ou grands donneurs d'ordre (Nombre de répondants au sondage : 34); et, Barrières à la profitabilité des entreprises en cybersécurité au Québec (Nombre de répondants au sondage : 12).

en cybersécurité. Le premier de ces défis est celui de la sensibilisation et de l'éducation des clients, selon 19% des répondants. Les risques de cybersécurité restent perçus comme lointains pour la majorité des PME, et il est difficile pour les entreprises de cybersécurité de convaincre leurs clients potentiels de l'importance d'investir dans des technologies qui ne procurent pas de revenus immédiats, à moins que des exigences règlementaires s'imposent. Il est donc nécessaire pour les entreprises de cybersécurité d'éduquer le marché des PME sur les solutions disponibles, ce qui génère des coûts additionnels dont les retombées sont difficiles à prévoir.

Le respect des normes industrielles est crucial dans le domaine de la cybersécurité. Toutefois, le besoin d'obtenir de multiples certifications occasionne des défis pour l'offre de services ou de produits en cybersécurité selon 10,6% des répondants. Les répondants et les participants aux entretiens relatent que ce ne sont pas toujours les mêmes certifications qui sont demandées. Les frais exigés pour obtenir ces certifications sont non négligeables. À ceux-ci s'ajoutent également le temps et les ressources nécessaires pour mettre en place et maintenir les procédures et les contrôles exigés par ces certifications.

L'adaptation aux besoins des PME, dont les budgets sont limités et dont la faible maturité technologique exige des solutions simplifiées, représente un autre défi pour 8,5% des entreprises de cybersécurité. Ce défi est accentué par la structure d'un marché où il est difficile de se démarquer, en raison de la saturation de l'offre et de la visibilité dominante des grandes entreprises, même si les solutions de ces dernières ne sont pas adaptées aux besoins et aux capacités des PME. Comme l'a mentionné un participant aux entretiens : « Il est essentiel pour des petits fournisseurs de déployer des efforts marketing pour expliquer les avantages d'une solution innovante au-delà des tendances actuelles ». Cependant, plusieurs répondants au sondage rencontrent des difficultés à se faire connaître. Ceux-ci ne bénéficient pas de la visibilité espérée. Il semble difficile de se démarquer sur le marché, et ce, particulièrement pour les entreprises émergentes bénéficiant d'un budget publicitaire limité.

Toutefois, bien que le marché soit saturé, cela ne veut pas dire qu'il est statique et ne peut pas être porteur d'opportunités. La nature et les méthodes des cybermenaces évoluent constamment, créant ainsi un besoin continu d'innovation et de solutions de cybersécurité adaptées. De plus, avec l'augmentation de la connectivité numérique et la dépendance accrue aux technologies de l'information dans tous les secteurs d'activité, la demande pour des solutions de sécurité robustes et adaptatives ne cesse de croître. Il existe aussi des moteurs de croissance régionaux, voir nationaux, lorsqu'une expertise humaine doit accompagner la solution ou quand des cadres normatifs ou légaux (ex : Loi 25) font leur apparition.

4.5 Portrait FFOM synthèse

Une analyse FFOM (Forces, Faiblesses, Opportunités, Menaces) pour l'industrie des produits et services en cybersécurité et cyber résilience dans la province du Québec est fournie ici pour servir de sommaire de l'état de la situation.

Forces	Faiblesses
▪ Expertise technologique et innovation : le Québec possède une base solide en matière de recherche et d'innovation, notamment grâce à des institutions de recherche réputées et à des programmes universitaires spécialisés en cybersécurité. ▪ Soutien gouvernemental : les initiatives provinciales, telles que les investissements dans les pôles technologiques et les incitations fiscales pour la R&D en cybersécurité (RSDE, Prompt, CDAE, PARI, etc) renforcent l'industrie. ▪ Écosystème dynamique : présence d'un écosystème dynamique incluant startups, PME et grandes entreprises spécialisées dans la cybersécurité. Des entreprises comme QoHash, SecureExchanges, Cyberwall.ai, BoostSecurity.io, et OkiOk sont des exemples notables basés au Québec et détenus par des intérêts canadiens.	▪ Entreprises de petite taille, peu capitalisées et avec un déficit réputationnel (peu de champions technologiques avec création de brevets) ▪ Peu de grands donneurs d'ordre locaux ▪ Innovation ouverte académique/entreprises faible ▪ Concurrence internationale : face à des géants mondiaux, les entreprises québécoises peuvent rencontrer des difficultés à se tailler une place sur le marché international. ▪ Manque de main-d'œuvre qualifiée : Bien que l'écosystème éducatif soit robuste, la demande croissante pour les spécialistes en cybersécurité dépasse souvent l'offre, créant des défis en matière de recrutement. ▪ Dépendance aux financements publics : certaines startups et PME peuvent être fortement dépendantes des subventions et des incitatifs gouvernementaux, ce qui peut affecter leur viabilité à long terme en cas de changement de politique. ▪ Externalisation croissante vers des pays tiers de la main d'œuvre en cybersécurité
Opportunités	**Menaces**
▪ Croissance de la demande globale : l'augmentation constante des menaces cybernétiques accroît la demande mondiale pour des solutions innovantes en cybersécurité, offrant des débouchés internationaux pour les entreprises québécoises. ▪ Collaborations stratégiques : les possibilités de partenariats avec des institutions académiques, des consortiums de recherche et des entreprises internationales peuvent favoriser l'innovation et l'expansion. ▪ Secteurs verticaux spécifiques : le développement de solutions ciblées pour des industries spécifiques (par exemple, l'aéronautique, où le Québec excelle) représente	▪ Cybermenaces évolutives : l'évolution rapide et la sophistication croissante des cyberattaques représentent un défi constant pour l'industrie, nécessitant des investissements continus en R&D. ▪ Concurrence des marchés émergents : les pays avec des coûts de développement plus bas peuvent offrir des solutions compétitives à moindre coût, exerçant une pression sur les prix et les marges des entreprises québécoises. ▪ Réglementations internationales : les changements dans les cadres réglementaires internationaux peuvent affecter l'accès aux marchés étrangers pour les solutions développées au Québec.

une opportunité de différenciation et de croissance.	

5. SIX PISTES DE RÉFLEXION

L'analyse de la documentation et des données du sondage et des entretiens permet de tirer certaines conclusions et d'identifier quelques pistes de réflexion pour mieux soutenir le développement de l'industrie de la cybersécurité au Québec, ainsi que de l'écosystème dont la vitalité est indispensable à ce développement.

5.1 Fragmentation de l'écosystème

Premièrement, les données ont permis de rappeler que l'écosystème entourant l'industrie de la cybersécurité est complexe. L'analyse de la documentation et les résultats du sondage pointent vers une même constatation: l'industrie est naissante, diversifiée, et recèle un énorme potentiel commercial. Toutefois, l'écosystème dans lequel évolue cette industrie reste fragmenté et composé de nombreux acteurs aux capacités et aux objectifs très variés. Certains de ces acteurs sont des joueurs majeurs de l'industrie, disposant d'avantages comparatifs indéniables comme leur taille, leurs liens avec l'industrie des producteurs de logiciels ou de plateformes dominant le marché des infrastructures technologiques utilisées dans le monde. Cela leur confère des avantages significatifs, comme leur capacité à attirer les meilleurs talents. Les petits acteurs et les startups disposent par contraste de moins de relais dans l'écosystème et font ainsi face à des obstacles importants s'ils souhaitent se tailler une place pérenne dans ce marché. Il pourrait ainsi être utile d'initier une réflexion collective des divers acteurs de l'écosystème et sur les stratégies pouvant être élaborées afin de réduire cette fragmentation et consolider les liens entre les diverses catégories d'acteurs qui le composent.

5.2 Données incomplètes sur l'industrie et l'écosystème

Deuxièmement, pour pouvoir soutenir ce secteur et cet écosystème, des données de meilleure qualité et régulièrement mises à jour seront nécessaires. Il s'agit d'un secteur qui évolue rapidement où les enjeux sont multiples, et ce, particulièrement pour les petits joueurs. Nous notons un manque de données solides et récentes pour disposer d'une compréhension approfondie de l'industrie de la cybersécurité au Québec et de son écosystème de référence. Si des mesures sont adoptées afin d'améliorer le pilotage et les capacités de cette industrie, il est nécessaire de recueillir de manière régulière des statistiques pertinentes pour mieux comprendre l'état actuel de l'industrie, les tendances de l'écosystème et les besoins des acheteurs. Cette question se pose tout aussi bien du côté de l'offre que du côté de la demande, car même

si on peut facilement faire l'hypothèse que la demande est là pour toutes les entreprises, il est indispensable de mieux comprendre comment celles-ci s'approvisionnent en cybersécurité et sur quelles bases elles prennent leurs décisions. Par exemple, où achètent-elles leurs services et pourquoi ? De plus, il apparaît y avoir un besoin d'établir des canaux de communication plus réguliers entre les acteurs de l'industrie de la cybersécurité et les gouvernements afin de mieux partager les aspirations, les besoins et les enjeux auxquels ils font respectivement face.

5.3 Accès des PME de l'industrie aux marchés publics

L'analyse des réponses quantitatives et qualitatives au sondage ont mis en lumière les difficultés éprouvées par les PME dans leur accès aux marchés par appels d'offres des acheteurs publics et des gros acteurs institutionnels, ainsi que dans une moindre mesure aux programmes de soutien public par le biais des subventions et autres formes de contributions.

Les PME ont souvent une capacité administrative très limitée et ne peuvent donc s'outiller convenablement pour répondre aux exigences contractuelles des appels d'offres. Aider les PME à naviguer de manière plus fluide ces processus pourrait donc leur permettre de gagner en maturité par l'accès à des contrats leur permettant de se développer, de se faire connaître et de gagner sur le plan réputationnel. Certaines juridictions comme le Canada, les États-Unis ou le Royaume Uni ont développé des approches innovantes dans ce domaine. Ces programmes utilisent différents leviers afin de soutenir les PME nationales : en premier lieu, ils réservent un pourcentage des marchés publics aux PME éligibles, leur permettant d'entrer en compétition avec des entreprises aux capacités comparables. C'est par exemple le cas aux États-Unis où l'objectif est que les PME se voient octroyées 23% des marchés publics fédéraux par le biais de programmes variés supervisés par la Small Business Administration[70]. Dans d'autres cas, les processus d'appel d'offre sont simplifiés pour les contrats publics ne dépassant pas certains montants, afin d'inciter les PME à candidater. C'est le cas par exemple pour Services Publics et Approvisionnement Canada qui a lancé une initiative en ce sens dans les domaines de l'achat de services en intelligence artificielle et en logiciels-services[71]. Finalement, certains gouvernements développent des outils et des pratiques qui facilitent la participation des PME : le Royaume Uni a ainsi développé une initiative de recherche et d'innovation destinée aux PME qui leur offre des contrats dans le cadre d'un processus compétitif mais pré-commercial afin de développer des prototypes d'innovations répondant aux besoins des services publics[72]. Des formations spécifiques sont également dispensées, des opportunités de mentorat sont offertes, et les paiements sont aussi réalisés de manière accélérée, afin de limiter les impacts négatifs sur la trésorerie des PME. Dans ce dernier cas, le gouvernement britannique s'engage à payer 90% des factures provenant de PME dans un délais de 5 jours ouvrables[73].

[70] https://www.sba.gov/federal-contracting/contracting-assistance-programs.
[71] Repéré à https://www.canada.ca/fr/services-publics-approvisionnement/services/achats/mieux-acheter/simplifier-processus-approvisionnement/contrats.html.
[72] Repéré à https://www.ukri.org/what-we-do/browse-our-areas-of-investment-and-support/innovate-uk-contracts-for-innovation/.
[73] Repéré à https://www.gov.uk/guidance/Prompt-payment-policy.

Des pratiques semblables pourraient être expérimentées au Québec dans le domaine de la cybersécurité afin d'en évaluer l'impact sur les PME de l'industrie.

5.4 Le soutien et la valorisation internationale des entreprises locales

Un quatrième constat ressorti des données analysées est celui d'un enjeu de réputation. Les répondants perçoivent parfois un manque de confiance des organismes publics et des grands donneurs d'ordres à travailler avec des fournisseurs plus petits et moins implantés que les grands joueurs de l'industrie. Cet enjeu est certainement habituel pour de nouveaux joueurs dans un marché émergent. Toutefois et dans l'univers de la cybersécurité, cet enjeu peut avoir des incidences plus grandes étant donné les répercussions qu'auront des failles de sécurité pour les acheteurs potentiels. Le produit offert doit être fiable et robuste. Les petites organisations qui se lancent dans ce secteur ne sont donc souvent pas en mesure de se faire reconnaître suffisamment pour percer le marché durablement.

Ce déficit de réputation a également un impact sur la valorisation des entreprises locales qui ont tendance à se faire acquérir sans avoir pu atteindre leur pleine maturité et par conséquent leur pleine valorisation. Principalement, la tendance récente est que ces sorties se font au bénéfice d'intérêts étrangers, le plus souvent américains et européens. L'impact des acquisitions est complexe, influençant non seulement les entrepreneurs eux-mêmes mais aussi l'écosystème de la cybersécurité dans son intégralité, le paysage des investissements et l'innovation technologique.

Cependant, certaines entreprises québécoises spécialisées dans la cybersécurité ont déjà acquis une reconnaissance internationale, et la région est bien placée pour continuer à produire des innovations dans ce domaine. Afin de pallier ce manque perçu de visibilité nationale et internationale, le développement d'un label de qualité fédérateur permettrait de faciliter les activités de promotion des entreprises locales de cybersécurité. Ce label, soutenu par des campagnes publicitaires et des aides à la participation aux grandes foires internationales de cybersécurité, pourrait contribuer à améliorer la reconnaissance des entreprises québécoises auprès des acheteurs locaux et à les rendre plus visibles à l'international face à leurs concurrents américains, français, anglais ou israéliens, dans un contexte politique où les solutions québécoises peuvent être perçues comme plus « neutres » et respectueuses de la souveraineté numérique des acheteurs. C'est par exemple le choix effectué par la France avec son label « France Cybersecurity »[74].

5.5 Un ciblage de l'aide gouvernementale

Cinquièmement, il serait opportun d'explorer le soutien à la création de niches. Le marché est vaste et les joueurs sont multiples, tant au Canada qu'aux États-Unis. De plus, il est ressorti du sondage et des entrevues qu'il est très difficile de percer le marché canadien à moins d'être connu et reconnu aux États-

[74] https://www.francecybersecurity.fr/.

Unis, les géants de l'informatique y étant situés. Ceci explique peut-être pourquoi les entreprises québécoises évoluent principalement sur le marché des services en cybersécurité et dans une moindre mesure dans le développement de produits.

Il pourrait être intéressant de se questionner sur la possibilité d'un plus grand ciblage de l'aide gouvernementale là où elle serait la plus porteuse et se distinguerait de la concurrence. Les opportunités de financement pourraient donc viser un créneau en particulier ou un nombre limité de domaines pour lesquels le Québec dispose d'avantages compétitifs avérés. La protection des renseignements personnels apparaît comme porteuse pour l'avenir étant donné les obligations législatives et le fait que celle-ci soit mentionnée comme une des préoccupations les plus importantes des organisations canadiennes. L'intelligence artificielle comme outil de cybersécurité ou technologie à protéger, et l'informatique quantique sont également des candidats naturels à ce type d'approche ciblée, étant donné les synergies possibles avec des écosystèmes d'innovation très dynamiques en train de se développer au Québec avec le soutien du gouvernement.

5.6 Collaborations entre industriels et universitaires

Sixièmement, il serait souhaitable que les liens des entreprises de cybersécurité avec les universités soient resserrés, pour deux raisons. D'une part, le développement d'une industrie innovante et robuste de la cybersécurité nécessite une démarche stratégique centrée sur des entrepreneurs soutenus par des centres de recherche. À ce titre, il semble y avoir un déficit de communication entre l'industrie de la cybersécurité, et tout particulièrement les PME qui la composent, et le milieu universitaire. Un dialogue et des partenariats plus soutenus entre les établissements d'enseignement et les acteurs de l'industrie de la cybersécurité, qu'ils soient entrepreneurs ou acheteurs, seraient donc bénéfiques afin d'accélérer les transferts de connaissances des projets de recherche fondamentale vers des applications industrielles concrètes répondant aux besoins de l'industrie. Par ailleurs, il y a une pénurie de talents et un maillage plus serré avec les institutions d'enseignement supérieur serait crucial pour y remédier. Des activités de maillage stratégique entre chercheurs et entreprises pourraient être envisagées, avec un accent particulier sur les PME.

La même approche de ciblage du soutien gouvernemental proposée dans la section précédente pourrait aussi être étendue aux centres de recherche afin de les inciter à privilégier certains thèmes jugés prioritaires pour l'écosystème à court, moyen et long terme.

Finalement, une aide gouvernementale au recrutement par l'entremise de partenariats avec les collèges et les universités (ex. : programme de jumelage) pourrait aider à atténuer la pénurie de talents dont souffre le secteur, tout en assurant une meilleure visibilité aux métiers de la cybersécurité parmi les étudiants de niveau collégial et universitaire.

CONCLUSION

En plus d'être stratégiquement cruciale, l'industrie de la cybersécurité représente pour le Québec un secteur économique porteur de prospérité et de croissance, dans un monde incertain où les risques numériques continueront de se complexifier. Cette industrie est innovante et commercialise des produits et des services en forte demande, aussi bien sur le territoire national qu'à l'exportation. Le Québec semble bien positionné en raison du niveau élevé de qualification de sa main d'œuvre et de la présence sur son territoire d'établissements d'enseignement et de recherche de calibre mondial.

L'écosystème québécois reste toutefois fragmenté et fragile. Il est constitué principalement de petites et moyennes entreprises qui sont en compétition frontale avec de grandes multinationales et qui disposent souvent de ressources insuffisantes pour répondre aux appels d'offre des grands donneurs d'ordre ou nouer des partenariats productifs avec les équipes de recherche académiques. Un modèle qui permettrait d'exploiter les forces de cet écosystème tout en réduisant les freins à son développement reste encore à définir. Celui-ci devra émerger d'une vision commune élaborée par l'ensemble des composantes de cet écosystème dans un esprit de collaboration.

Un autre enjeu de taille pour l'écosystème de la cybersécurité est son interconnexion avec les autres écosystèmes d'innovation en développement au Québec, qu'il s'agisse de l'intelligence artificielle et de l'informatique quantique dans le secteur numérique, ou des filières de l'énergie, du transport ou de l'agroalimentaire pour les autres secteurs industriels.

La profonde transformation technologique initiée par la révolution numérique expose dorénavant toutes les entreprises et les infrastructures à des cyber-risques susceptibles de menacer leur survie en perturbant les flux logistiques, énergétiques, financiers et informationnels dont elles dépendent. La course mondiale à l'innovation incite également certains pays à recourir à des pratiques agressives de vol de la propriété intellectuelle développée au Québec par des moyens technologiques avancés. Il pourrait donc être pertinent de faire de la cybersécurité une dimension charnière des politiques et stratégies d'innovation, en créant des incitatifs pour que tout l'écosystème d'innovation puisse bénéficier de l'expertise de partenaires spécialisés en cybersécurité, afin de renforcer la résilience de l'économie québécoise. Cette notion de cyber-résilience deviendra centrale dans le paysage en constante évolution des cyber-risques. Les entreprises, les gouvernements et les particuliers sont tous concernés par la nécessité de protéger leurs données et leurs systèmes contre les cyberattaques. Cette situation crée un terrain fertile pour la croissance de l'industrie de la cybersécurité.

L'industrie de la cybersécurité offre un potentiel de croissance énorme et des opportunités passionnantes. En travaillant ensemble, nous pouvons créer un avenir numérique plus sûr et plus résilient.

RÉFÉRENCES

Ahlawat, P., Krause, T., Pagano, E., Banerjee, S., Jarvis, F., Justin, J., et Emerson, G. (2019). *How software companies can get more bang for their R&D buck*. Boston Consulting Group. Repéré à https://www.bcg.com/publications/2019/software-companies-using-research-and-development-more.

Aiyer, B., Caso, J., Russell, P. et Sorel, M. (2022). *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers*. McKinsey & Company.

Berry, C. et R. Berry (2018). An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management* 8 (1): 1-10.

Bouchard, L. et Henri, J.-F. (2023). *Gouvernance de la cybersécurité - Portrait et tendance au Québec*. Repéré à https://www.cas.ulaval.ca/wp-content/uploads/2023/04/Article_Gouvernance_Cybersecurite_vue2pages.pdf.

Carmel, E. et Roche, E. (2023). The dominant cybersecurity industry clusters: evolution and sustainment. *Industry and Innovation* 30 (3): 361-391.

Centre canadien pour la cybersécurité (2022). *À propos du Centre pour la cybersécurité*. Repéré à À propos du Centre pour la cybersécurité - Centre canadien pour la cybersécurité

Centre canadien pour la cybersécurité (2024). *Certifications dans le domaine de la cybersécurité*. Repéré à https://www.cyber.gc.ca/sites/default/files/certifications-domaine-cybersecurite-2024-f.pdf

Cohen, N., Hulvey, R., Mongkolnchaiarunya, J., Novak, A., Morgus, R. et Segal, A. (2017). *Cybersecurity as an engine for growth*. Repéré à http://www.jstor.com/stable/resrep10491.1

CPE Media & Data Company (2024). *Strong Q2 2024 VC drives Canadian VC reaching $3.87B*. Repéré à https://www.newswire.ca/news-releases/strong-q2-2024-vc-drives-canadian-vc-reaching-3-87b-817250967.html.

CRTC (2023). *Plan ministériel 2023-2024*. Repéré à https://crtc.gc.ca/fra/publications/reports/dp2023/dp2023.htm.

CVCA (2024). *Year-end 2023 VC & PE Canadian market overview.* Repéré à https://www.cvca.ca/insights/market-reports/year-end-2023/.

Cybereco (2022). *Sondage sur la cybersécurité*. Résultats présentés à la Cyber Conférence 2022.

Deloitte (2016). *Harnessing the cybersecurity opportunity for growth: Cybersecurity innovation & the financial services industry in Ontario*. Repéré à https://www.oc-innovation.ca/wp-content/uploads/2021/03/Harnessing-the-cybersecurity-opportunity-for-growth.pdf

Deloitte (2023). *2023 Global Future of Cyber Survey - Building long-term value by putting cyber at the heart of the business*. Repéré à https://www.deloitte.com/global/en/services/risk-advisory/content/future-of-cyber.html

Dupont, B. (2024). *La cybercriminalité : Approche écosystémique de l'espace numérique*. Paris : Armand Colin.

Dupont, B. et C. Whelan (2022). Enhancing relationships between criminology and cybersecurity. *Journal of Criminology* 54 (1): 76-92.

Fédération des chambres du commerce du Québec (2021). *Étude sur la cybersécurité et les opportunités offertes par l'accès aux données au Québec*. Repéré à https://www1.fccq.ca/wp-content/uploads/2021/11/RapportAviseo_cybervalorisation_FCCQ_final.pdf

Fortin, A., Watler, P., Ladouceur, R., Montès, F. C. et Roberge, L. (2021). *Chapitre 7 Cybersécurité*. Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2021-2022.

Fortune Business Insight (2024). *Cyber security market*. Repéré à https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165

Gartner (2023). *Gartner forecasts global security and risk management spending to grow 14% in 2024*. Repéré à https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024

Gouvernement du Québec (2024). *Le commerce extérieur du Québec*. Repéré à https://www.economie.gouv.qc.ca/fileadmin/contenu/publications/etudes_statistiques/echanges_exterieurs/calepin_exterieur.pdf.

Groupe Novipro et Léger (2023). *Portrait des TI dans les petites, moyennes et grandes entreprises canadiennes*. Étude Portrait TI.

Herron, C., Rice, F. et Snider, N. (2020). *À la recherche des talents cachés : L'expérience et l'expertise de la communauté de cybersécurité du Nouveau-Brunswick*, Ottawa: Conseil des technologies de l'information et des communications.

Innovation, Sciences et Développement économique Canada (2022). *L'état de l'industrie canadienne de la cybersécurité – Automne 2022*. Repéré à https://ised-isde.canada.ca/site/aerospatiale-defense/fr/rapport-letat-lindustrie-canadienne-cybersecurite

Institut d'études internationales de Montréal (2020). *La stratégie internationale du Canada en matière de cybersécurité : enjeux et recommandations*. Recommandations politiques. Repéré à https://www.ieim.uqam.ca/IMG/pdf/ieim-recommandations_politiques-cyberse_curite_-fe_v2020.pdf

Investissement Québec (2021). *Le Québec, pôle florissant de la cybersécurité*. Présentation PowerPoint.

(ISC)² (2021). *A Resilient Cybersecurity Profession Charts the Path Forward - Cybersecurity Workforce Study.* Repéré à https://www.mvrop.org/cms/lib/CA01922720/Centricity/Domain/59/ISC2%20Cybersecurity%20Workforce%20Study%202021.pdf

(ISC)² (2019). *Strategies for Building and Growing Strong Cybersecurity Teams*. Repéré à https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2 Cybersecurity-Workforce-Study 2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

Knowles, W., Such, J., Gouglidis, A., Misra, G. et Rashid, A. (2017). All that glitters is not gold: On the effectiveness of cybersecurity qualifications. *Computer* 50: 60-71.

Landwehr, C. (2010). History of US government investments in cybersecurity research. *2010 IEEE Symposium on Security and Privacy*. Repéré à https://ieeexplore.ieee.org/abstract/document/5504783.

Ministère de l'Économie, de l'Innovation et de l'Énergie (2021). *Aperçu de l'industrie des technologies de l'information*. Repéré à https://www.economie.gouv.qc.ca/bibliotheques/le-secteur/technologies-de-linformation-et-des-communications/apercu-de-lindustrie-des-technologies-de linformation#:~:text=Au%20Qu%C3%A9bec%2C%20l'industrie%20des,pr%C3%A9pond%C3%A9rante%20dans%20l'%C3%A9conomie%20qu%C3%A9b%C3%A9coise.

Montréal International (2021). *Grand Montréal : un hub de cybersécurité en pleine effervescence*. Repéré à https://www.montrealinternational.com/app/uploads/2019/04/cybersecurite_profil_sectoriel_2021-1.pdf

Moore, J. (1993). Predator and prey: A new ecology of competition. *Harvard Business Review* 71 (3): 75-86.

Moore, J. (1996). *The death of competition: Leadership and strategy in the age of business ecosystems*. New York: Harper Business.

Prompt (2023). *S'unir pour renforcer la cybersécurité au Québec.* Montréal : Prompt. Repéré à https://Promptinnov.com/wp-content/uploads/2023/12/Memoire-cyberVF.pdf.

Quan, T. et Herron, C. (2022). *Développement des talents en cybersécurité : protéger l'économie* numérique du Canada, Ottawa : Conseil des technologies de l'information et des communications.

Sécurité publique Canada (2018). *Stratégie nationale de cybersécurité*. Repéré à ntnl-cbr-scrt-strtg-fr.pdf (securitepublique.gc.ca)

Statistique Canada (2022). *L'incidence du cybercrime sur les entreprises canadiennes, 2021*. Repéré à https://www150.statcan.gc.ca/n1/daily-quotidien/221018/dq221018b-fra.htm.

TECHNOCompétences (2021). *Diagnostic sectoriel 2021-2024*. Portrait de la main-d'œuvre dans le secteur des technologies de l'information et des communications (TIC) au Québec.

The Economist (2018). *Defence companies target the cyber-security market*. 26 juillet. Repéré à https://www.economist.com/business/2018/07/26/defence-companies-target-the-cyber-security-market.

Westin, F., Ream, F. et Dupont, B. (2022). *Adapting cybersecurity to the needs and capacities of SMEs: A Canadian perspective*. Montréal: SERENE-RISC. Repéré à https://www.serene-risc.ca/public/media/files/prod/page_files/31/Serene_Cybersecurity_Ecosystem_Canada.pdf.

Cyberéco (2024). *Ontologie des sociétés fournisseurs en cybersécurité v.1.0*. Disponible sur demande.

ANNEXE 1 : écosystèmes de la cybersécurité à l'international

Analyse sommaire des principaux écosystèmes de cybersécurité internationaux préparée par In-Sec-M

Écosystème israélien

Forces

Service militaire et renseigenement

- Unité 8200 :
  - Cette unité d'élite de renseignement de l'armée israélienne est souvent comparée à la NSA américaine. Elle se concentre sur la cyberdéfense, la collecte de renseignements et les cyberattaques. Beaucoup de ses anciens membres fondent des startups en cybersécurité ou rejoignent des entreprises technologiques, apportant avec eux des compétences avancées en matière de cybertechnologies.

- Culture de l'innovation militaire :
  - L'armée israélienne encourage la prise de risque et l'innovation, formant des jeunes à penser de manière créative et à résoudre des problèmes complexes, des compétences cruciales en cybersécurité.

Écosystème de startups

- "Startup Nation" :
  - Israël est reconnu pour son écosystème de startups dynamique. Le pays dispose du plus grand nombre de startups par habitant au monde, avec un focus significatif sur la technologie et la cybersécurité.

- Investissements en capital-risque :
  - Le pays attire des investissements massifs en capital-risque, tant locaux qu'internationaux. Les investisseurs sont particulièrement attirés par les innovations en cybersécurité issues d'Israël.

Soutien gouvernemental

- Programmes de soutien et subventions :
  - Le gouvernement israélien offre des subventions et des incitations fiscales aux startups technologiques, y compris celles spécialisées en cybersécurité. Tel Aviv, depuis au moins 2011, coordonne et centralise les efforts de cybersécurité à travers le pays.

- Partenariats public-privé :

- Israël promeut activement les collaborations entre le gouvernement, les entreprises et les institutions académiques pour développer des solutions de cybersécurité robustes.

Éducation et recherche

- Institutions académiques :
  - Les universités israéliennes, telles que l'Université de Tel Aviv, l'Université Ben Gurion (Neguev), l'Université Hébraïque de Jérusalem et le Technion, sont reconnues pour leurs programmes de recherche avancés en cybersécurité.

- Programmes de formation :
  - Il existe une multitude de programmes de formation en cybersécurité à différents niveaux, destinés à former la prochaine génération de professionnels de la cybersécurité.

Innovation technologique

- Forte culture de R&D :
  - Israël consacre une part importante de son PIB à la recherche et développement (R&D), se concentrant sur l'innovation technologique, y compris dans la cybersécurité.

- Technologies avancées :
  - Le pays est à l'avant-garde des technologies émergentes telles que l'intelligence artificielle, la blockchain et l'apprentissage automatique appliqués à la cybersécurité.

Marché global

- Exportation de technologies :
  - Israël exporte une grande partie de ses technologies de cybersécurité vers le reste du monde. Les entreprises israéliennes signent des contrats avec des gouvernements et des entreprises internationales pour protéger leurs infrastructures critiques.

- Attraction des multinationales :
  - De nombreuses multinationales de la technologie, comme Microsoft, Google et IBM, ont établi des centres de recherche et développement en Israël, attirées par l'expertise locale en cybersécurité.

Mentalité entrepreneuriale

- Culture de la résilience et de l'innovation :
  - La culture israélienne valorise la résilience, l'innovation et la capacité à relever des défis complexes, des traits essentiels pour réussir dans le domaine de la cybersécurité.

- Succès des expatriés :
  - De nombreux entrepreneurs israéliens réussissent à l'international, apportant une visibilité et une crédibilité accrues à l'écosystème technologique israélien.

Faiblesses

Dépendance aux marchés étrangers :

- Une grande partie des entreprises israéliennes de cybersécurité dépend de clients et de marchés étrangers, notamment aux États-Unis et en Europe. Cette dépendance peut rendre les entreprises vulnérables aux fluctuations économiques et aux changements de politiques dans ces régions.

Pénurie de talents :

- Bien qu'Israël dispose d'un vivier de talents en cybersécurité, la demande dépasse souvent l'offre. Cette pénurie peut limiter la croissance des entreprises et rendre difficile la rétention des meilleurs talents, qui peuvent être attirés par des opportunités à l'étranger.

Concurrence intense :

- Le nombre élevé de startups dans le domaine de la cybersécurité crée une concurrence intense pour le financement, les clients et les talents. Cette situation peut mener à une fragmentation du marché et à des difficultés pour les entreprises émergentes à se différencier et à se stabiliser.

Risque de sécurité :

- En tant que nation en conflit, Israël est souvent la cible de cyberattaques. Cette situation peut représenter un risque pour les entreprises locales, même si cela génère également une expérience pratique précieuse en défense contre les cybermenaces. La guerre que mène actuellement Israël contre les terroristes du Hamas vient ajouter une couche de complexité pour le développement de l'écosystème local de la cybersécurité.

Coût élevé de l'innovation :

- Le coût de la recherche et du développement en cybersécurité est élevé. Les entreprises doivent investir constamment dans l'innovation pour rester compétitives, ce qui peut être un défi financier, surtout pour les startups.

Bureaucratie et réglementation :

- Bien que le gouvernement israélien soutienne fortement le secteur de la cybersécurité, certaines entreprises peuvent rencontrer des difficultés avec les régulations et la bureaucratie, notamment en matière de protection des données et de conformité.

Conclusion

Israël est devenu un acteur incontournable de la cybersécurité mondiale grâce à une combinaison unique de formation militaire avancée, d'un écosystème dynamique de startups, de soutien gouvernemental, de recherche et développement de pointe, et d'une culture de l'innovation. Ces facteurs ont permis à Israël de développer des solutions de cybersécurité de classe mondiale et d'attirer des investissements et des collaborations internationales, consolidant ainsi sa position de leader dans ce domaine stratégique.

Écosystème français

Forces

Politiques et soutien gouvernemental

- ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) :
  - Créée en 2009, l'ANSSI est l'organisme principal en matière de cybersécurité en France. Elle joue un rôle crucial dans la protection des infrastructures critiques, la réglementation et la sensibilisation.

- Stratégie nationale pour la cybersécurité :
  - Le gouvernement français a mis en place plusieurs stratégies nationales pour renforcer la cybersécurité, incluant des investissements dans la recherche, le développement et la formation.

Recherche et Développement

- Instituts de recherche :
  - Des institutions comme l'INRIA (Institut National de Recherche en Informatique et en Automatique) et le CEA (Commissariat à l'Énergie Atomique et aux Énergies Alternatives) jouent un rôle clé dans la recherche en cybersécurité.

- Collaborations public-privé :
  - La France favorise les partenariats entre les institutions académiques, les entreprises privées et les organismes gouvernementaux pour encourager l'innovation en cybersécurité.

Écosystème de Startups

- Label "France Cybersecurity" :
  - Ce label, lancé en 2015, vise à promouvoir les solutions de cybersécurité développées en France et à renforcer leur visibilité internationale.

- Incubateurs et accélérateurs :
  - Des initiatives comme le Cyber Campus à Paris et des programmes comme "La French Tech" soutiennent les startups innovantes en cybersécurité, leur fournissant des ressources et des réseaux pour se développer.

Formation et Éducation

- Programmes académiques :
  - Les universités et grandes écoles françaises offrent des programmes spécialisés en cybersécurité. Des institutions comme Télécom Paris et l'Université de Rennes 1 sont reconnues pour leurs cursus de pointe.

- Cyber Range :
  - La mise en place de plateformes de simulation et d'entraînement cyber (Cyber Range) permet aux professionnels de la cybersécurité de s'entraîner dans des environnements réalistes.

Normes et régulations

- RGPD (Règlement Général sur la Protection des Données) :
  - Bien que d'origine européenne, la France a joué un rôle actif dans l'adoption et la mise en œuvre du RGPD, renforçant ainsi la protection des données et la cybersécurité.

- LPM (Loi de programmation militaire) :
  - La LPM inclut des dispositions spécifiques pour la cybersécurité, notamment la protection des infrastructures critiques et la défense des systèmes d'information.

Entreprises leaders

- Grandes entreprises :
  - Des entreprises comme Thales, Airbus CyberSecurity, Orange Cyberdefense sont des leaders mondiaux en cybersécurité, offrant des solutions avancées et opérant à l'international.

- PME innovantes :
  - La France compte également de nombreuses PME et startups innovantes en cybersécurité, comme Stormshield, Wallix, et Thetris, qui développent des technologies de pointe.

Sensibilisation et Communication

- FIC (Forum InCyber) :
  - Le FIC, organisé annuellement à Lille, est l'un des plus grands événements européens en cybersécurité, attirant des professionnels du monde entier pour échanger sur les meilleures pratiques et les innovations.

- Campagnes de sensibilisation :
  - L'ANSSI et d'autres organismes mènent régulièrement des campagnes pour sensibiliser le public et les entreprises aux enjeux de la cybersécurité.

Faiblesses

Pénurie de talents :

- Comme dans de nombreux pays, la France fait face à une pénurie de professionnels qualifiés en cybersécurité. Cette pénurie limite la capacité des entreprises à recruter des experts nécessaires pour faire face aux menaces croissantes.

Fragmentation du marché :

- L'écosystème français est caractérisé par une fragmentation avec de nombreuses petites et moyennes entreprises (PME) et startups. Cette situation peut entraîner une dispersion

des ressources et des difficultés pour certaines entreprises à atteindre une taille critique suffisante pour rivaliser à l'échelle internationale.

Accès limité au financement :

- Les startups françaises en cybersécurité peuvent rencontrer des difficultés à accéder à des financements suffisants pour soutenir leur croissance et leur innovation, en particulier par rapport à leurs homologues américains ou israéliens qui bénéficient souvent d'un soutien financier plus important.

Régulation stricte :

- La régulation française, bien que nécessaire pour protéger les données et la vie privée, peut parfois être perçue comme un obstacle par les entreprises, notamment les petites structures qui peuvent avoir des difficultés à se conformer à toutes les exigences légales.

Visibilité internationale :

- Comparativement aux États-Unis et à Israël, l'écosystème français peut manquer de visibilité et de reconnaissance internationale, ce qui peut limiter les opportunités de partenariat et de croissance à l'étranger.

Adoption lente des nouvelles technologies :

- Certaines entreprises françaises peuvent être plus lentes à adopter de nouvelles technologies et approches en cybersécurité, ce qui peut les rendre vulnérables face aux menaces évolutives.

Coopération publique-privée :

- Bien que des efforts existent pour améliorer la coopération entre les secteurs public et privé, cette collaboration peut encore être renforcée pour une meilleure réponse coordonnée aux cybermenaces.

Conclusion

La France a su devenir un acteur important en cybersécurité grâce à une stratégie cohérente et bien articulée qui inclut le soutien gouvernemental, un écosystème dynamique de startups, des programmes de formation avancés, et une collaboration étroite entre les secteurs public et privé. Les initiatives telles que l'ANSSI, le label "France Cybersecurity", et des événements comme le FIC ont permis à la France de se positionner comme un leader dans ce domaine crucial.

Écosystème américain

Forces

Écosystème technologique et industriel avancé

- Silicon Valley :

        - En tant que centre mondial de l'innovation technologique, Silicon Valley abrite de nombreuses entreprises de cybersécurité de premier plan, telles que Palo Alto Networks, Symantec, FireEye, et bien d'autres.

    - Grandes entreprises technologiques :
        - Des géants technologiques comme Google, Microsoft, IBM, et Amazon ont des divisions de cybersécurité robustes, investissant massivement en R&D pour développer des solutions avancées.

Investissements Massifs en R&D

- Capital-Risque :
    - Les États-Unis bénéficient d'un accès considérable au capital-risque, permettant aux startups de cybersécurité de se développer rapidement. En 2020, le secteur de la cybersécurité a attiré plus de 7,8 milliards de dollars en capital-risque.

- Innovations :
    - Les investissements en R&D mènent à des innovations continues dans des domaines tels que l'intelligence artificielle, le machine learning, la cryptographie avancée, et la sécurité des infrastructures critiques.

Soutien gouvernemental et stratégies nationales

- NSA et Cyber Command :
    - La National Security Agency (NSA) et le United States Cyber Command jouent un rôle crucial dans la protection des intérêts nationaux et le développement de technologies de cybersécurité avancées.

- Politiques et régulations :
    - Des initiatives telles que la Cybersecurity Information Sharing Act (CISA) encouragent le partage d'informations sur les menaces entre le secteur privé et le gouvernement.

- Financements fédéraux :
    - Des agences comme la DARPA (Defense Advanced Research Projects Agency) financent des projets de recherche avancés en cybersécurité.

Éducation et Formation

- Universités de premier plan :
    - Les États-Unis abritent certaines des meilleures universités au monde, telles que MIT, Stanford, et Carnegie Mellon, qui offrent des programmes de formation et de recherche de pointe en cybersécurité.

- Certifications professionnelles :
    - Le pays dispose d'un grand nombre de certifications professionnelles reconnues mondialement, telles que CISSP, CEH, et CISM, qui renforcent la compétence des professionnels de la cybersécurité.

Écosystème de Startups Dynamique

- Incubateurs et accélérateurs :

        - Des programmes comme Y Combinator et Techstars soutiennent des startups innovantes en cybersécurité, leur fournissant des ressources et des réseaux pour se développer.

    - Acquisitions stratégiques :
        - Les grandes entreprises technologiques acquièrent fréquemment des startups de cybersécurité pour intégrer leurs technologies et talents, favorisant ainsi l'innovation continue.

Secteur privé proactif

- Industries sensibles :
    - Des secteurs comme la finance, la santé, et l'énergie investissent massivement en cybersécurité pour protéger leurs infrastructures critiques.

- Cyber Threat Intelligence :
    - De nombreuses entreprises américaines disposent de capacités avancées en matière de renseignement sur les menaces, leur permettant de réagir rapidement aux cyberattaques.

Sensibilisation et partage d'information

- ISACs (Information Sharing and Analysis Centers) :
    - Ces centres facilitent le partage d'informations sur les cybermenaces entre les entreprises d'un même secteur, améliorant la résilience collective.

- Conférences et événements :
    - Des événements comme RSA Conference et Black Hat attirent des professionnels du monde entier, favorisant l'échange de connaissances et l'innovation.

Faiblesses

Pénurie de talents :

- Les États-Unis font face à une pénurie critique de professionnels qualifiés en cybersécurité. La demande croissante pour des experts dépasse largement l'offre, ce qui complique le recrutement et la rétention de personnel compétent.

Complexité réglementaire :

- Le paysage réglementaire américain est fragmenté avec des lois et des régulations variées au niveau fédéral, étatique et local. Cette complexité peut entraîner des difficultés de conformité pour les entreprises, en particulier celles opérant dans plusieurs juridictions.

Fragmentation du marché :

- Bien que le marché américain soit vaste, il est également très fragmenté avec de nombreuses entreprises, allant des startups aux géants de la technologie. Cette fragmentation peut diluer les efforts de coordination et de collaboration nécessaires pour une défense efficace contre les cybermenaces.

Défis de la protection des infrastructures critiques :

- Les infrastructures critiques américaines, telles que l'énergie, les transports et la finance, sont souvent des cibles pour les cyberattaques. La protection de ces infrastructures est un défi constant en raison de leur complexité et de leur interdépendance.

Menaces internes :

- Outre les menaces externes, les États-Unis doivent également faire face à des menaces internes, notamment les employés mécontents ou négligents qui peuvent compromettre la sécurité des systèmes.

Innovation et mise à jour lente :

- Certaines grandes organisations peuvent être lentes à adopter de nouvelles technologies de cybersécurité ou à mettre à jour leurs systèmes, ce qui les rend vulnérables aux nouvelles menaces.

Coûts élevés de la cybersécurité :

- Le coût de la mise en œuvre et de la maintenance des mesures de cybersécurité est élevé, ce qui peut être un obstacle pour les petites et moyennes entreprises. Ces coûts incluent la technologie, la formation et les audits de sécurité réguliers.

Dépendance aux fournisseurs étrangers :

- Une partie des technologies et des composants utilisés dans les systèmes de cybersécurité provient de fournisseurs étrangers, ce qui peut poser des risques en matière de sécurité nationale et de chaîne d'approvisionnement.

Conclusion

Les États-Unis dominent le secteur mondial de la cybersécurité grâce à un écosystème technologique et industriel avancé, des investissements massifs en R&D, un soutien gouvernemental solide, des institutions académiques de premier plan, et un secteur privé proactif. Cette combinaison de facteurs permet aux États-Unis de rester à la pointe de l'innovation en cybersécurité et de répondre efficacement aux menaces cybernétiques croissantes.

Écosystème allemand

Forces

Expertise en sécurité industrielle

- Industrie 4.0 :
  - L'Allemagne est un pionnier de l'Industrie 4.0, intégrant des systèmes cyber-physiques et des technologies de l'Internet des Objets (IoT) dans les processus industriels. Cela a conduit à un développement avancé des solutions de cybersécurité pour protéger les infrastructures critiques.

- Siemens, Bosch :

- Des géants industriels comme Siemens et Bosch investissent massivement en cybersécurité, développant des solutions pour sécuriser les environnements industriels et les infrastructures critiques.

Centres de recherche et universités

- Fraunhofer Institute :
  - Fraunhofer est l'une des principales institutions de recherche appliquée en Europe, avec des centres spécialisés en cybersécurité, comme l'Institut Fraunhofer pour la sécurité de l'information (SIT).

- Universités de renom :
  - Des universités comme l'Université technique de Munich (TUM) et l'Université de Darmstadt offrent des programmes avancés en cybersécurité, produisant des chercheurs et des professionnels hautement qualifiés.

Soutien gouvernemental

- BSI (Bundesamt für Sicherheit in der Informationstechnik) :
  - Le BSI est l'agence fédérale de cybersécurité, jouant un rôle central dans la protection des infrastructures critiques, la réglementation et la sensibilisation.

- Initiatives et stratégies nationales :
  - Le gouvernement allemand a mis en place plusieurs stratégies nationales pour renforcer la cybersécurité, incluant des investissements dans la recherche et le développement ainsi que des politiques de cybersécurité robustes.

Écosystème de startups

- Berlin et Munich :
  - Berlin et Munich sont des centres technologiques majeurs en Europe, abritant de nombreuses startups innovantes en cybersécurité, soutenues par un solide écosystème de capital-risque et des incubateurs.

Faiblesses

Pénurie de talents

- Manque de professionnels qualifiés :
  - Comme de nombreux pays, l'Allemagne fait face à une pénurie de professionnels qualifiés en cybersécurité, ce qui peut ralentir la croissance et la capacité à répondre aux menaces croissantes.

Fragmentation régionale

- Disparités régionales :
  - Le développement de la cybersécurité en Allemagne peut varier considérablement entre les différentes régions, certaines régions étant plus avancées que d'autres en termes d'infrastructures et de soutien à l'innovation.

Réglementations complexes

- Conformité réglementaire :

- Les entreprises doivent naviguer dans un cadre réglementaire complexe, ce qui peut représenter un défi, notamment pour les PME et les startups qui n'ont pas les ressources pour se conformer facilement à toutes les exigences.

Principaux Acteurs

Entreprises

- Siemens :
  - Leader dans les solutions de cybersécurité industrielle, Siemens développe des technologies pour protéger les infrastructures critiques et les systèmes industriels.
- Bosch :
  - Bosch investit également dans des solutions de cybersécurité pour l'industrie, l'automobile et les appareils connectés.
- SAP :
  - En tant que géant des logiciels d'entreprise, SAP développe des solutions pour la sécurité des données et des applications en entreprise.

Startups et PME

- Cure53 :
  - Spécialisée dans les tests de pénétration et les audits de sécurité, Cure53 est reconnue pour ses évaluations approfondies de la sécurité des applications Web et des systèmes.
- Rohde & Schwarz Cybersecurity :
  - Fournit des solutions de cybersécurité pour la protection des réseaux, des applications et des données.
- Cysmo :
  - Développe des solutions pour la détection des fraudes en ligne et la protection contre les cyberattaques.

Instituts de recherche

- Fraunhofer SIT :
  - Mène des recherches appliquées en cybersécurité, développant des technologies pour sécuriser les systèmes informatiques et les réseaux.
- Helmholtz Center for Information Security (CISPA) :
  - Un des principaux centres de recherche en sécurité informatique, CISPA travaille sur des projets avancés en cryptographie, sécurité des réseaux et protection des données.

Conclusion

L'Allemagne possède un écosystème de cybersécurité solide, soutenu par une forte expertise en sécurité industrielle, des centres de recherche de classe mondiale et un soutien gouvernemental robuste. Toutefois, des défis tels que la pénurie de talents et la fragmentation régionale doivent être surmontés pour maintenir et renforcer sa position de leader en cybersécurité. L'accent mis sur la sécurité des infrastructures critiques et industrielles reflète les priorités économiques et technologiques du pays, faisant de l'Allemagne un acteur clé dans le domaine de la cybersécurité mondiale.

ANNEXE 2
ORGANISATIONS DU SECTEUR DE LA CYBERSÉCURITÉ AU QUÉBEC

Écosystèmes

CENTRES DE RECHERCHE + CCTT
Gric · Laboratoire de confiance numérique · Cyber Québec · UdeS Université de Sherbrooke · ÉTS · LRSI · IMC Institut multidisciplinaire en cybersécurité et cyberrésilience

ORGANISMES DE SOUTIEN
IN SEC M · ASIQ · CQTNC · cyber eco · ASIMM · risq · REED

INCUBATEURS
propolys · CARREFOUR CYBER · Cilex

FINANCEMENT
prompt Finance l'innovation technologique · mitacs · NATIONAL CYBERSECURITY CONSORTIUM · CONSORTIUM NATIONAL POUR LA CYBERSÉCURITÉ · Canada NRC CNRC · CRSNG NSERC

Formations

COLLÉGIALES
Cégep de l'Outaouais · Collège de Maisonneuve · Collège de Bois-de-Boulogne · Cégep de Saint-Hyacinthe · Édouard-Montpetit · Cégep Garneau · CollègeAhuntsic · Collège Lionel-Groulx · Collège Montmorency · Champlain Collège Saint-Lambert · Cégep Limoilou · Cégep de Saint-Jean-sur-Richelieu · Collège LaSalle Montréal · Collège Rosemont

UNIVERSITAIRES
Polytechnique Montréal · ÉTS · McGill · Université de Montréal · UdeS Université de Sherbrooke · Concordia · Université Laval · UQAC · Université du Québec à Trois-Rivières · UQO Université du Québec en Outaouais

Fournisseurs

SERVICES CONSEIL
ARMUR · catallaxy · Securis · PDN Cyber Security Consultant · CAP2SEC · Cercle numérique · Umbrella · ubitrak · CERTI TRUST · CGI · Cogentas · CONATIX · OneSpan · CSMF · CYCLIC · Deloitte. · ZONETI · EthiSécure · DOXIA · DPOsolutions · MICROFIX · CYDEF · DEVICOM · EY · YottaSec · MSP CORP · CVA TECHNOLOGIES · EVIDEN · KPMG · formind · FORTICA · Alithya · YACK · Irosoft · RHEA · Hemley · HEXTECH · MicroMedica · onepoint. · maltem · nameshield · ISAIX · KEREON · KYBER SECURITY · PCI · levio · MAXIMIZ · VARS · NEOTRUST · noraa · OKIOK · one lab · PIVASCADA · INFOSECSW · B2B CYBER SECURE · S3 TECHNOLOGIES · vendel · S2CI · secure · opticca · sherweb · NEVERHACK · TEKAP · pwc · V2OPS · VICTRIX · VONA · vumetric · TRILOGIAM

DÉVELOPPEMENT DE SOLUTIONS LOGICIELLES OU MATÉRIELLES (SAAS OU PRODUITS)
8B · awee · BlueBear · CAIDO · Secure Pyramide · Carillon · Bradley Rollins · CGTechs Technologies · CONVERGE · Becker-Carroll · Caristix · CRYPTO4A · DiliTrust · eQualitie · eset · flare · HDCE · CYBERDEFENSE.AI · Devolutions · ARMADAIT · ESI TECHNOLOGIES · EZ-TFA · HORNETSECURITY · HITACHI Inspire the Next · 80th · MANTLE · IBM · id-m · mondata* · Northern Block · ID torney · IPTOKI · SAFE ENTRY · Radio IP · notarius · verifai · INTELLISEC SOLUTIONS · PORTAGE cybertech · optable · QOHASH · STREAMSCAN · Terranova Security · TRUSTCORE · XST · SECURE LOGIKA · SII CANADA · it-ed · Sentryfy · SENTIOM · in a blink · THALES · Xpertics Solutions

REVENTE ET INTÉGRATION DE SOLUTIONS COMMERCIALES
pcd solutions · NOVIPRO · INDIGO CONSULTING · MS SOLUTIONS

SERVICES GÉRÉS ET/OU IMPARTITION (MSSP)
ARCODIA · CISCO · AtoS · FPE · adaptiv networks · KOASEC · cyvault · SUBGRAPH · SUNPHINX CYBERSECURITE · VIGITECK · GoSECURE · Indominus Services-conseils

ORGANISATIONS DU SECTEUR DE LA CYBERSÉCURITÉ AU QUÉBEC

Écosystèmes

CENTRES DE RECHERCHE + CCTT

Cyber Québec
GRIC - Groupe de Recherche Interdisciplinaire en Cybersécurité
IMC2 - Institut Multidisciplinaire en Cybersécurité et Cyberrésilience
Laboratoire de confiance numérique
LCSec - Laboratoire de CyberSécurité - ÉTS
LRSI - Laboratoire de Recherche en Sécurité Informatique - UQO
Pôle d'expertises en cybersécurité - UdeS

FINANCEMENT

CNC - Consortium National pour la Cybersécurité
CNRC - Conseil National de Recherches du Canada (PARI)
CRSNG - Conseil de Recherches en Sciences Naturelles et en Génie du Canada
MITACS
PROMPT

INCUBATEURS

Carrefour Cyber
CILEX
Propolys

ORGANISMES DE SOUTIEN

ASIMM - Association de Sécurité de l'Information du Montréal Métropolitain
ASIQ - Association de la Sécurité de l'Information du Québec
CQTNC - Centre Québécois en Transformation Numérique et Cybersécurité
CyberÉco
In-Sec-M - Innovation Sécurité Marché
REED - Réseau d'Expertise en Éthique de Données
RISQ - Réseau d'Informations Scientifiques du Québec

Formations

COLLÉGIALES

CÉGEP de l'Outaouais
CÉGEP de Saint-Hyacinthe
CÉGEP Édouard Monpetit
CÉGEP Garneau
CÉGEP Limoilou
CÉGEP Saint-Jean-sur-Richelieu
Collège Ahuntsic
Collège Champlain Saint-Lambert
Collège de Bois-de-Boulogne
Collège de Maisonneuve
Collège LaSalle
Collège Lionel Groulx
Collège Montmorency
Collège Rosemont

UNIVERSITAIRES

ÉTS - École de Technologie Supérieure
Polytechnique Montréal
UdeM - Université de Montréal
UdeS - Université de Sherbrooke
UL - Université Laval
Université Concordia / Concordia University
Université McGill / McGill University
UQAC - Université du Québec à Chicoutimi
UQO - Université du Québec en Outaouais
UQTR - Université du Québec à Trois-Rivières

Fournisseurs

DÉVELOPPEMENT DE SOLUTIONS LOGICIELLES OU MATÉRIELLES (SAAS OU PRODUITS)

8Brains
Awee Inc.
Becker-Carroll (Converge)
Bluebear LES
Bradley & Rollins
Caido
Carillon Information Security
Caristix
CGtechs
Converge Technology Solutions
Crypto4A
CYBERDEFENSE.AI
Devolutions Inc.
DiliTrust Canada Inc.
EasyPatternZ Incorporated (IKAR-Holding/ArmadAI)
eQualitie Inc.
ESET Canada Research
ESI Technologies Inc.
EZ-TFA
F8th
Flare Systems Inc.
HDCE Inc.
Hitachi Systems Security Inc.
Hornet Securité
IBM Canada
id-m.me (IDM Gestion Identité INC)
IDtorney LAW - TECH Inc. - CAPITAL LP.
Intellisec Solutions
IPtoki
KrowdX
Logiciels Radio IP Inc.
Mantle Blockchain
Mondata / Groupe Elucidia
Northern Block
Notarius Solutions
Portage CyberTech
QoHash
Secure Exchanges Inc.
Secure Logika
Sentiom
SII (Société Informatique Industrielle) Canada
Solutions ITED
StreamScan Security
Technologies In A Blink
Technologies Optable
Technology Sentryfy
Terranova Security (Fortra)
Thales Digital Solutions
Trustcore
Verif AI (Solutions I Agree Inc.)
Xpert Solutions Technologiques
Xpertics

REVENTE ET INTÉGRATION DE SOLUTIONS COMMERCIALES

Groupe NOVIPRO
Indigo Consulting
MS Solutions conseil
PCD Solutions (Converge)

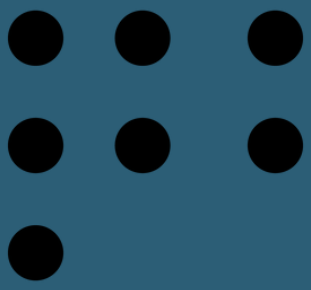
SERVICES CONSEIL

Agence PDN
Alithya
Armur360 - Expérience S3I
B2B Cyber Secure
Brainstorm CyberRisque
Cap2sec
Catallaxy (RCGT)
Cercle numérique
Certi-Trust
CGI
Cogentas Inc
Commissionnaires du Québec
Conatix
Conseils CeptBiro Inc.
CS Group Canada
CSMF - Cyber Securité Mathieu Fluet
Cybenergie
CyberEspoir Inc.
CyberShell
CY-CLIC
CYDEF
Deloitte
Devicom
Doxia
DPO Solution Inc.
Dredsec
Équipe MICROFIX
Ernst & Young (EY)
EthiSecure Services
EVA Technologies (Logicnet)
Eviden
Formind Canada
Fortica (KPMG)
Groupe Access (Groupe MSP)
Groupe CyberSwat
Groupe RHEA
Hemley
Hextech (Technologies Hexadécimales)
ILIR
Infosecsw
INSSATAD
Irosoft
IsaIX
Kéréon
KPMG
Kyber Sécurité
Levio
Maltem Canada
Maximiz
Micromedica
Nameshield Cybersécurité
Neotrust Cybersécurité
Noraa
Octosafes
OKIOK Data
One Lab Technologies
OnePoint
OneSpan
PCI 360
PM SCADA
PWC
Resolock
RMDS Innovation
S2CI - Société de Conseils en Cybersécurité et Informatique
S3 TECHNOLOGIES
Secure Digitale
SecureOps
Securis Canada
Sécurité Opticca
Sherweb Inc.
Sia Partners
Solutions NeverHack (Silicom Inc / Seela)
Sonder Sécurité
Systèmes Securitech
Tekap
Triloglam
Ubitrak (Kerson Wallaw)
Umbrella Technologies
V2OPS Solutions d'Entreprise Inc.
VARS
VersagiliT Inc.
Victrix Conseil
Vona
Vumetric
Yack Sécurité Inc.
YottaSec
ZoneTI Securité

SERVICES GÉRÉS ET/OU IMPARTITION (MSSP)

Adaptiv Networks
Arc4dia
ATOS
Cisco Systems Canada
CYVAULT
Exploriо
FPE Consultant Inc.
GoSecure (CounterTack)
Indominus Inc.
Koasec

Février 2025. Cette cartographie a été établie selon notre connaissance du secteur. Pour toute demande de changement de catégorie ou de logo, veuillez communiquer avec Prompt en remplissant ce formulaire.



Prompt
1200 McGill College Ave suite 1650, Montreal,
Quebec H3B 4G7

promptinnov.com

Avec la participation financière de

prompt

Québec