Innovation, Science and Economic Development Canada
Innovation, Sciences et Développement économique Canada
Canada

APERÇU STATISTIQUE DE L'INDUSTRIE DE LA CYBERSÉCURITÉ AU CANADA EN 2018

Octobre 2020

Contexte : développer des informations stratégiques pertinentes, de qualité et opportunes sur l'industrie de la cybersécurité afin d'informer les décideurs politiques et industriels

- **Le Canada** est le premier parmi les pays de l'Organisation de coopération et de développement économiques (OCDE) à mener une enquête approfondie **au moyen d'un organisme gouvernemental de statistiques** sur les capacités de l'industrie de la cybersécurité du point de vue des fournisseurs
    - Complémentaire à l'enquête canadienne sur la cybersécurité et le cybercrime, de Statistique Canada (point de vue de l'utilisateur)

- Soutenu par un accord de collaboration analytique pluriannuel avec des associations industrielles

- Ce rapport présente un **aperçu statistique** des activités de l'**industrie de la cybersécurité du Canada en 2018**, fondé sur les données les plus récentes disponibles

- Ainsi, ces résultats donnent un aperçu de l'état de l'industrie de la cybersécurité canadienne **avant le début de la pandémie de COVID-19**

- La **prochaine itération** de l'enquête bisannuelle **mesurera les activités industrielles de 2020**, et reflétera donc les **impacts potentielles de la pandémie** sur l'industrie en 2020
    - La publication des **données de base pour 2020 par Statistique Canada** est actuellement prévue pour le **début de 2022**

Cadre du projet

I. Définition du concept (décembre 2017 à février 2019)

- Consultation avec l'industrie, les experts en la matière, les organisations de défense et de sécurité publique, et les décideurs politiques sur le cadre de recherche et la population ciblée*

II. Élaboration des données (mars 2019 à décembre 2019)

- ISDE a parrainé l'enquête bisannuelle mesurant les statistiques de 2018 (pré-COVID), effectuée par Statistique Canada, avec obligation légale pour les entreprises d'y répondre en vertu de la Loi sur la statistique
- **Validation de la qualité des données et imputation au niveau des entreprises** fondées sur les données administratives

III. Analyse des données (janvier 2020 à septembre 2020)

- Élaboration d'un cadre de données et d'analyses
- Méthodologie de l'impact économique éclairée par des **experts** de l'OCDE et de Statistique Canada
- Préparation d'un aperçu de l'industrie de la cybersécurité au Canada (2018)

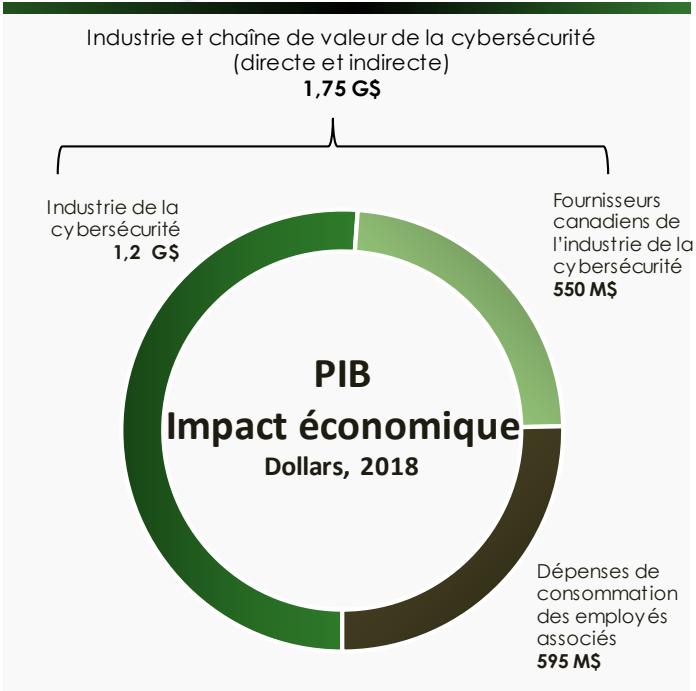
* La population ciblée comprend les entreprises de toutes tailles déterminées par tous les partenaires du projet. De plus, une approche de recensement de toutes les entreprises comptant plus de 20 employés dans toutes les industries connexes des technologies de l'information et des communications (TIC) a été utilisée pour compléter la liste d'enquête.

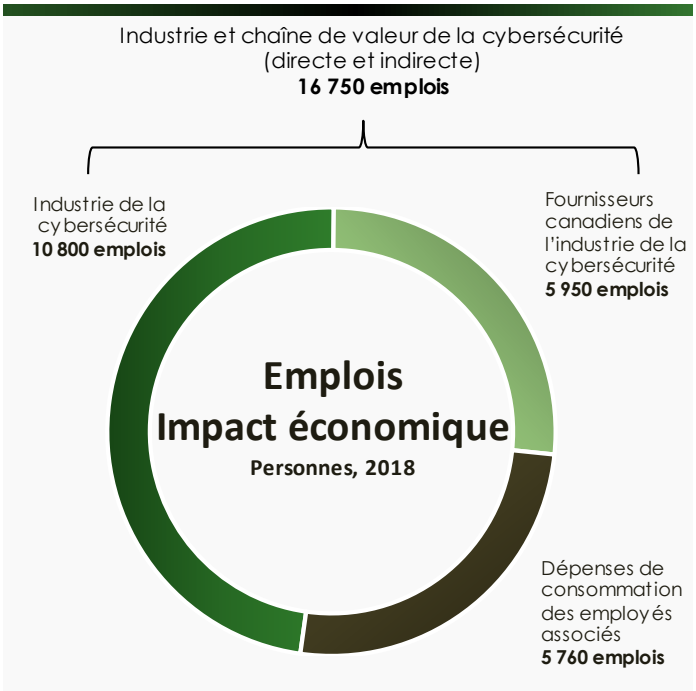
Aperçu

Domaines principaux de recherche et d'analyse

- Impact économique
- Compétences et diversité
- Empreinte par taille des entreprises
- Points forts régionaux
- Exportations
- Innovation
- Annexe

L'industrie de la cybersécurité a contribué plus de **2,3 G$ au PIB** et **22 500 emplois** à l'économie canadienne en 2018

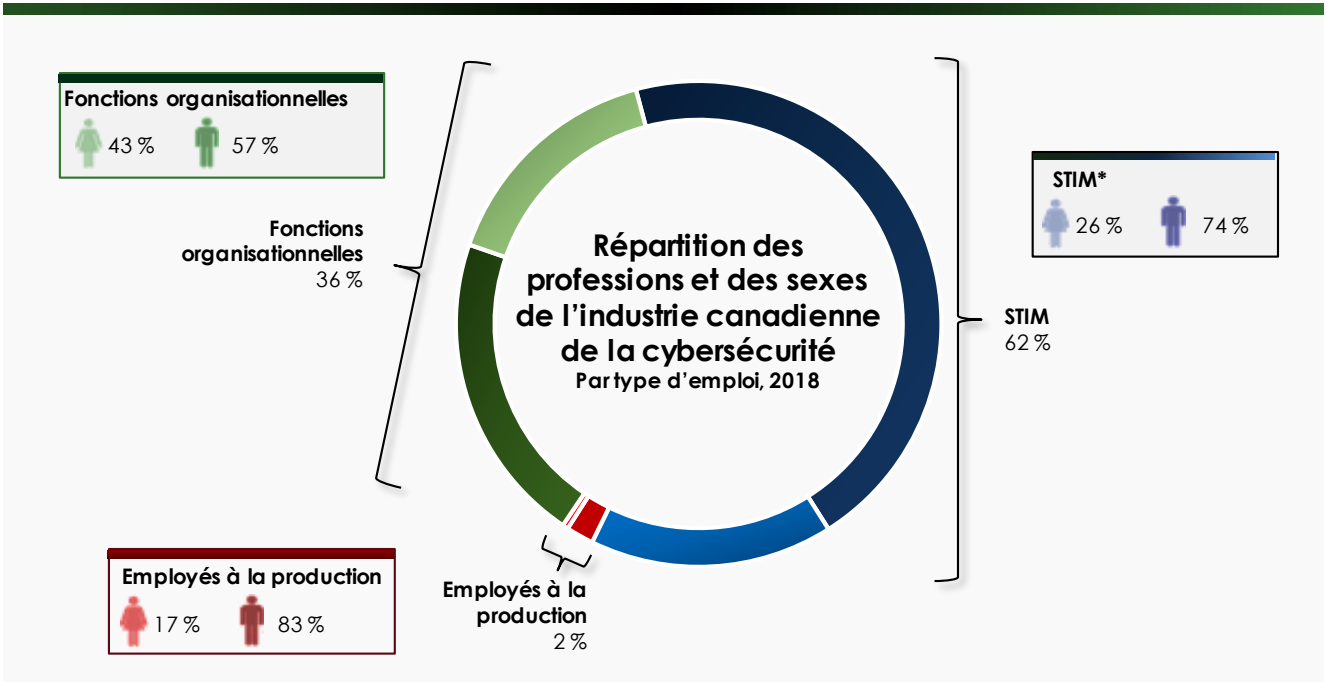




- L'industrie de la cybersécurité et sa chaîne de valeur ont contribué plus de **1,7 G$ au PIB** et **16 750 emplois** à l'économie canadienne* (directs et indirects)
- Les dépenses de consommation des employés associés ont contribué **595 M$ supplémentaires au PIB** et **5 760 emplois** (induits)

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020; modélisation économique d'ISDE fondée sur les plus récents multiplicateurs d'entrées-sorties (2016) de Statistique Canada et les multiplicateurs d'impact économique spécifiques connexes les plus proches qui ont trait à l'industrie de la cybersécurité.

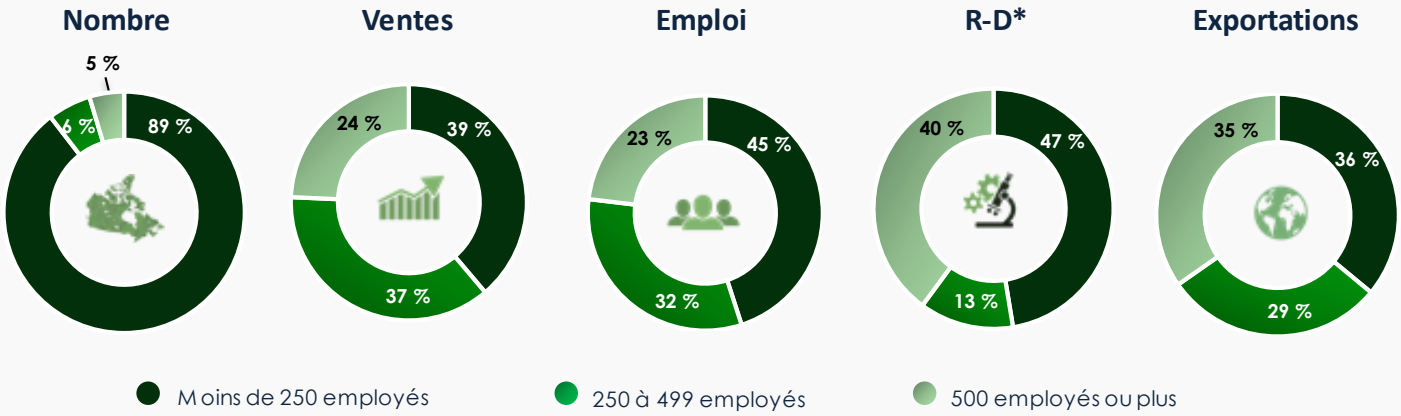
Les emplois en **STIM*** ont représenté **plus de 60 %** des emplois total de l'industrie en 2018



- La part des **professions en STIM** était **65 % supérieure à la moyenne** de **l'industrie canadienne des TIC****

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020; Enquête sur la population active de Statistique Canada (2018), 2020; Innovation, Sciences, Développement économique Canada, «Profil du secteur canadien des TIC 2018», 2020
*STIM : science, technologie, ingénierie et mathématiques
** Voir l'annexe 2 pour les définitions de l'industrie des TIC

Près de 90 % des **entreprises** canadiennes de l'industrie de la cybersécurité comptaient **moins de 250 employés en 2018**



- Contrairement à la plupart des industries, les **entreprises comptant moins de 250 employés** ont enregistré **plus de 45 % des emplois dans l'industrie** et **des activités de R-D**, tout en étant responsables de **plus de 35 % des exportations de l'industrie**

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020
* Les dépenses de R-D sont liées à la R-D effectuée à l'interne par les entreprises de cybersécurité.

Répartition des activités de l'industrie canadienne de la cybersécurité en 2018

Les ventes totales ont atteint près de **2,9 G$** avec **344 entreprises**

Types de produits ou de services	Part des ventes totales de cybersécurité (%)
Solutions en matière d'infrastructure : services et solutions d'infrastructure de cybersécurité servant à la protection continue de réseaux et des données	50,7 %
Solutions regroupées : solutions de cybersécurité reposant sur un seul ensemble de services, de logiciels ou de matériel — et qui englobe des éléments de plusieurs catégories de cybersécurité susmentionnées	11,9 %
Chiffrement	9,0 %
Vérifications de conformité et conception de programmes : audits de conformité et conception de programmes, élaboration de stratégies et activités connexes liées à la gestion des risques ainsi qu'aux services d'experts-conseils	8,0 %
Systèmes de contrôle industriels (SCI) : système d'acquisition et de contrôle des données (SCADA); technologie d'exploitation liée à la cybersécurité	5,4 %
Tests d'intrusion et surveillance des menaces : tests de pénétration, et évaluation des vulnérabilités et des menaces connexes, surveillance des cybermenaces, détection, services de renseignements, et mesures actives de cyberdéfense	4,2 %
Expertise judiciaire et enquêtes : criminalistique, enquêtes sur les cyberattaques ou autres cyberincidents et intrusions, et mesures correctrices adoptées	1,7 %
Formation : formation en cybersécurité	0,3 %
Autres : tous les autres biens et services liés à la cybersécurité	8,8 %
Total de l'industrie de la cybersécurité	**100,0 %**

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête publiée en 2020

En 2018, l'industrie de la cybersécurité était présente partout au Canada avec des spécialisations régionales*

Répartition régionale de l'industrie canadienne de la cybersécurité

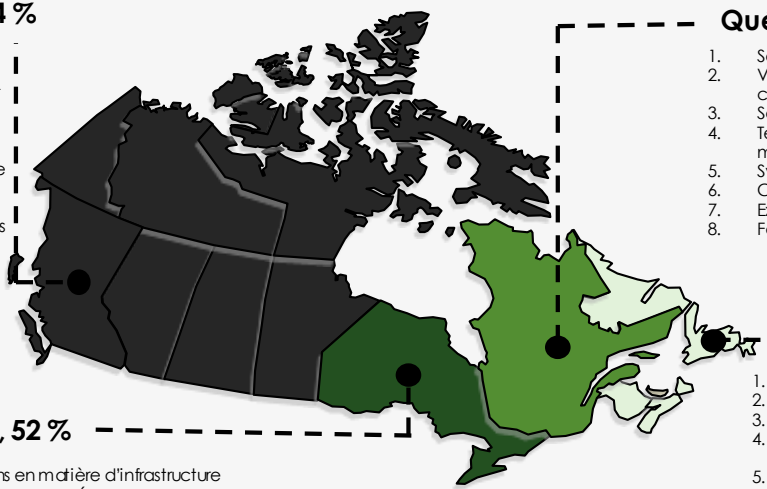
par part des emplois, 2018

Ouest du Canada, 24 %

1. Solutions en matière d'infrastructure
2. Vérifications de conformité et conception de programmes
3. SCI
4. Solutions regroupées
5. Tests d'intrusion et surveillance des menaces
6. Chiffrement
7. Expertise judiciaire et enquêtes
8. Formation

Québec, 19 %

1. Solutions en matière d'infrastructure
2. Vérifications de conformité et conception de programmes
3. Solutions regroupées
4. Tests d'intrusion et surveillance des menaces
5. Systèmes de contrôle industriels (SCI)
6. Chiffrement
7. Expertise judiciaire et enquêtes
8. Formation



Canada atlantique, 5 %

1. SCI
2. Solutions en matière d'infrastructure
3. Solutions regroupées
4. Vérifications de conformité et conception de programmes
5. Tests d'intrusion et surveillance des menaces
6. Chiffrement
7. Expertise judiciaire et enquêtes
8. Formation

Ontario, 52 %

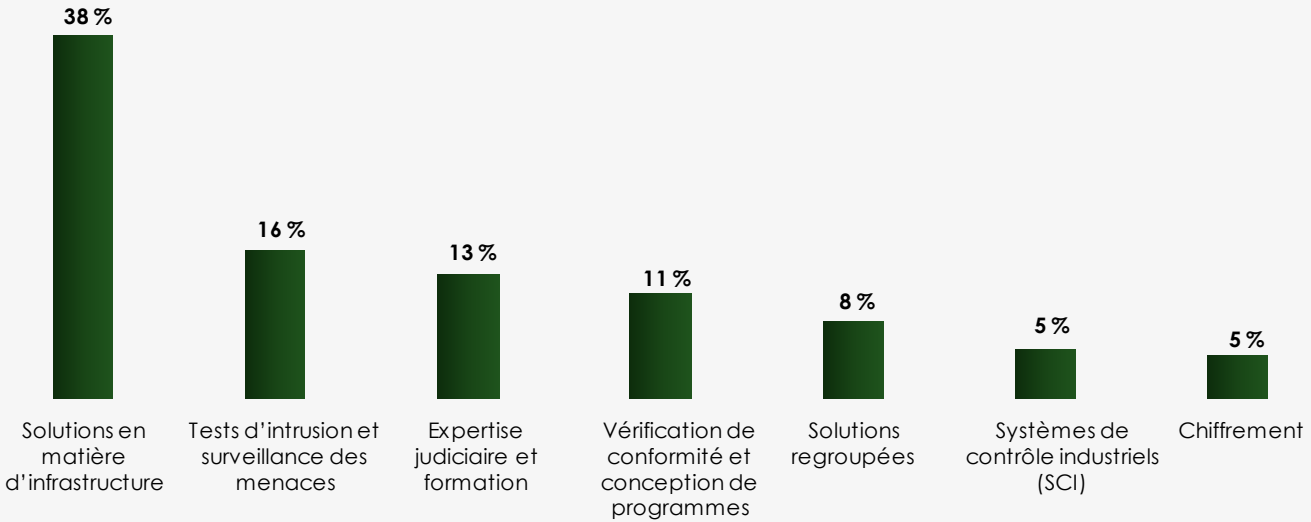
1. Solutions en matière d'infrastructure
2. Solutions regroupées
3. Chiffrement
4. Vérifications de conformité et conception de programmes
5. Tests d'intrusion et surveillance des menaces
6. Systèmes de contrôle industriels (SCI)
7. Expertise judiciaire et enquêtes
8. Formation

* Voir à l'annexe 5 les titres complets des catégories de biens et de services de la cybersécurité

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020

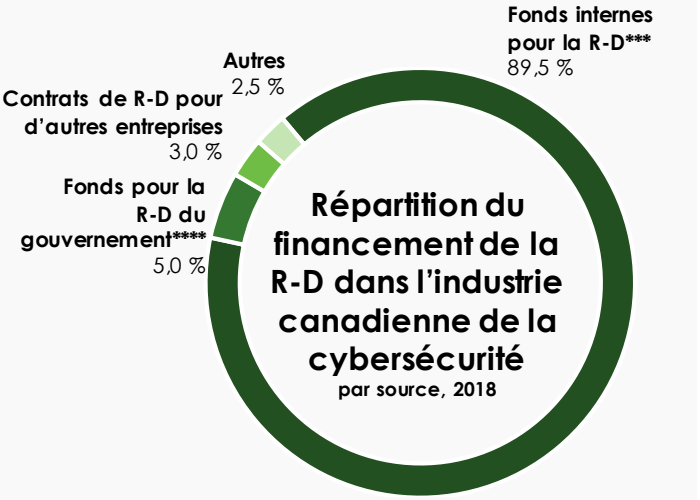
Près de 30 %* des ventes totales en cybersécurité ont été dirigées vers les forces armées, les organismes d'application de la loi, le renseignement et les organismes de sécurité nationale en 2018

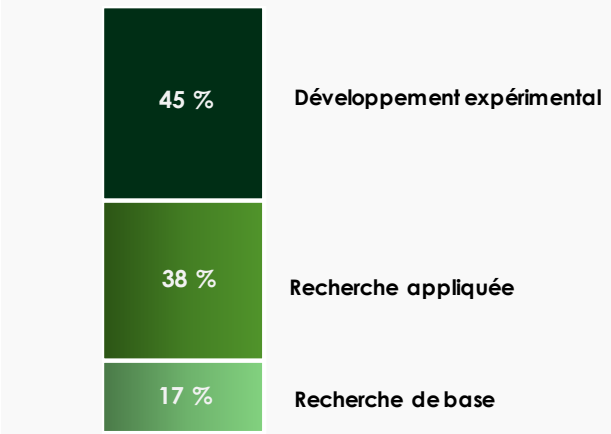
Intensité des ventes aux organismes militaires et de sécurité selon les types de produits et de services, 2018**



Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020
* Comprend d'autres biens et services liés à la cybersécurité
** La catégorie « Autres activités de cybersécurité » est exclue de ce tableau.

L'intensité de la R-D* dans l'industrie de la cybersécurité était **3 fois supérieur** à la moyenne de l'industrie canadienne des TIC** en 2018





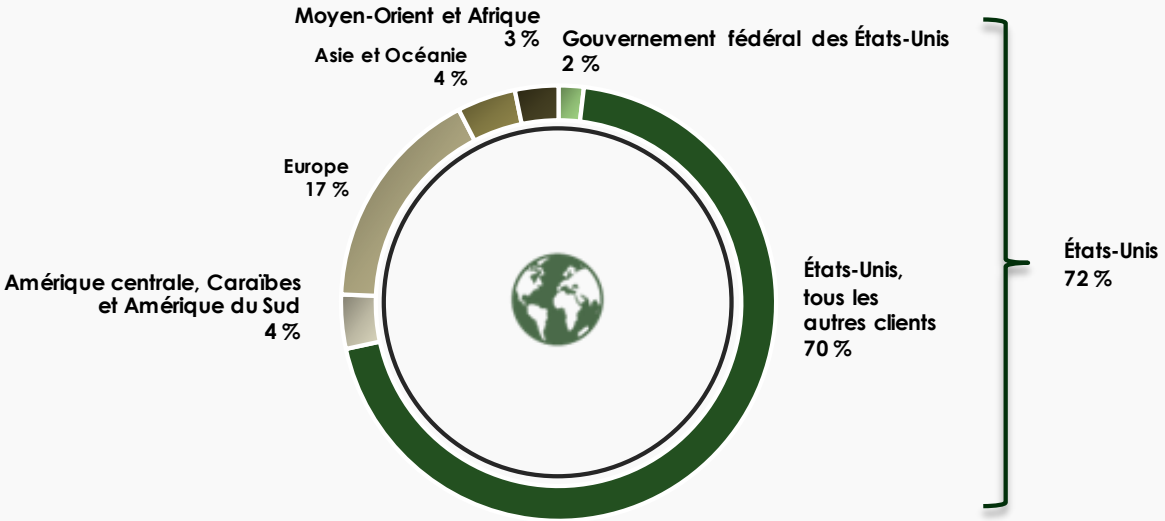
- Avec **près de 260 M$** d'investissements en R-D, **plus de 90 % de la R-D effectuée par l'industrie de la cybersécurité** a été financée par l'**industrie**
- La **composition** de l'ensemble des **activités de R-D de l'industrie de la cybersécurité par type** était **différente** de celle de l'industrie canadienne des TIC**

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020 et tableau en ligne de Statistique Canada : 27-10-0344-01 (anciennement CANSIM 358-0521)
* L'intensité de la R-D est calculée en utilisant le ratio de la R-D par rapport au PIB.
** Voir l'annexe 2 pour les définitions de l'industrie des TIC
*** Comprend les fonds des entreprises de cybersécurité qui effectuent la R-D, ainsi que certains fonds de leur société mère, de leurs sociétés affiliées et de leurs filiales.
**** La R-D financée par le gouvernement est dominée par les subventions.

Près de 1,1 G$ d'**exportations** en cybersécurité en 2018

Industrie canadienne de la cybersécurité, répartition du marché mondial

Par chiffre d'affaires, 2018

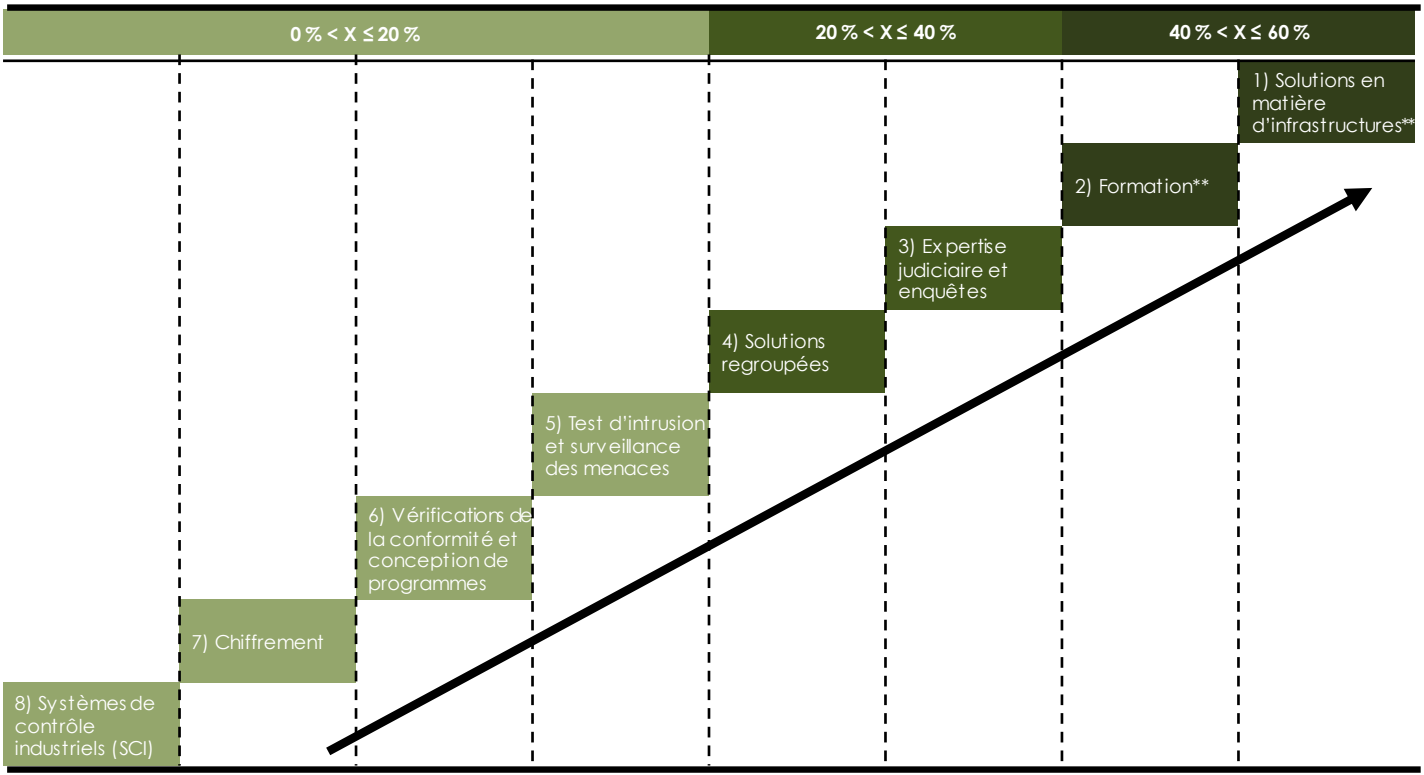


- **L'intensité des exportations** était **3 fois plus élevée** que la moyenne de l'industrie canadienne des TIC*

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020
* Voir l'annexe 2 pour les définitions de l'industrie des TIC

L'intensité des exportations a grandement varié selon le type de produits et de services en 2018

Classement de l'intensité des exportations des activités de cybersécurité*, 2018



Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité(2018), enquête de 2018 publiée en 2020
* La catégorie « Autres activités de cybersécurité » est exclue de ce tableau
** Les activités de formation et de solutions en matière d'infrastructure étaient égales en ce qui concerne leurs intensités d'exportation

Conclusions principales

En 2018, l'industrie canadienne de la cybersécurité:

- a généré de près de **2,9 G$** en ventes par **344 entreprises** dans le cadre de diverses activités
- a contribué près de **22 500 emplois** à l'économie canadienne
- a investit de près de **260 M$** dans la **R-D** et l'innovation
- Était hautement qualifiée **avec plus de 60 %** de sa main-d'œuvre liée aux STIM
- Avait un engagement mondial avec **des exportations de 1,1 G$**
- Était soutenue par **des entreprises comptant moins de 250 employés** pour ses capacités d'innovation et d'exportation

Annexe

Annexe 1 : Principes méthodologiques concernant les impacts économiques

Annexe 2 : Définition de l'industrie canadienne des TIC

Annexe 3 : Classement régional des activités

Annexe 4 : Tableaux de données

Annexe 5 : Définition de l'industrie de la cybersécurité

Annexe 1 : Principes méthodologiques concernant les impacts économiques

- Les données de base sont fondées sur la dernière (2018) enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité publiée en 2020

- Modélisation économique d'ISDE fondée sur les derniers multiplicateurs d'entrées-sorties (2016) de Statistique Canada et les multiplicateurs d'impact économique spécifiques connexes les plus proches qui ont trait aux activités de cybersécurité

- Le modèle économique est fondé sur les multiplicateurs d'entrées-sorties (E-S) de Statistique Canada

    - Les activités de cybersécurité ont été liées aux multiplicateurs d'impact économique précis les plus récents (2016) et les plus pertinents par catégorie de produits et de services de cybersécurité
    - L'impact sur le PIB est rapportée de façon cumulative et sur une base annuelle moyenne
    - L'impact sur l'emploi est rapportée sur la base de la moyenne annuelle et mesurée en termes d'emploi équivalent temps plein (ETP)
        - Les emplois ne peuvent être cumulatifs puisqu'ils sont maintenus pendant une période prolongée après leur création
    - L'impact économique totale de l'industrie de la cybersécurité comprend les activités qui se déroulent au sein de l'industrie canadienne de la cybersécurité, les fournisseurs canadiens de l'industrie canadienne de la cybersécurité, ainsi que les dépenses de consommation des employés associés dans l'ensemble de l'économie canadienne
    - Les estimations des impacts économiques sont présentées au niveau national et ne peuvent être répartis au niveau régional
    - La somme peut ne pas égaler 100 % en raison de l'arrondissement

Annexe 2 : Industrie canadienne des TIC

Fabrication de composantes des TIC
- Matériel informatique et périphérique
- Matériel de communications
- Composants électroniques
- Équipement audio et vidéo
- Supports magnétiques et optiques

Commerce de gros des TIC

Logiciels et services informatiques
- Éditeurs de logiciels
- Conception de systèmes informatiques
- Traitement des données
- Réparation et entretien de matériel électronique et de matériel de précision

Services de communications
- Entreprises de télécommunications sans fil
- Télécommunications par fil
- Câblodistribution et autres activités de distribution d'émissions de télévision

Source : Innovation, Sciences, Développement économique Canada, « Profil du secteur canadien des TIC 2018 » (2019), 2020

Annexe 3 : Classement régional des activités

Classement	Classement des activités dans l'Ouest et le Nord du Canada
1	Solutions en matière d'infrastructures
2	Vérifications de la conformité et conception de programmes
3	Systèmes de contrôle industriels (SCI)
4	Solutions regroupées
5	Tests d'intrusion et surveillance des menaces
6	Chiffrement
7	Expertise judiciaire et enquêtes
8	Formation

Classement	Classement des activités en Ontario
1	Solutions en matière d'infrastructures
2	Solutions regroupées
3	Chiffrement
4	Vérifications de la conformité et conception de programmes
5	Tests d'intrusion et surveillance des menaces
6	Systèmes de contrôle industriels (SCI)
7	Expertise judiciaire et enquêtes
8	Formation

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020

Annexe 3 : Classement régional des activités (suite)

Classement	Classement des activités du Québec
1	Solutions en matière d'infrastructures
2	Vérifications de la conformité et conception de programmes
3	Solutions regroupées
4	Tests d'intrusion et surveillance des menaces
5	Systèmes de contrôle industriels (SCI)
6	Chiffrement
7	Expertise judiciaire et enquêtes
8	Formation

Classement	Classement des activités du Canada atlantique
1	Systèmes de contrôle industriels (SCI)
2	Solutions en matière d'infrastructures
3	Solutions regroupées
4	Vérifications de la conformité et conception de programmes
5	Tests d'intrusion et surveillance des menaces
6	Chiffrement
7	Expertise judiciaire et enquêtes
8	Formation

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020

Annexe 4 : Tableaux de données

Tableau I : Impact économique

Impacts économiques sur le PIB (M$)				
Industrie de la cybersécurité (M$)	**Fournisseurs de l'industrie de la cybersécurité (M$)**	**Industrie et chaîne de valeur de la cybersécurité (M$)**	**Dépenses de consommation par employés associés (M$)**	**PIB total cumulatif (M$)**
1 200 M$	550 M$	**1 750 M$**	595 M$	**2 345 M$**

Impact économique sur l'emploi				
Industrie de la cybersécurité	**Fournisseurs de l'industrie de la cybersécurité**	**Industrie et chaîne de valeur de la cybersécurité**	**Dépenses de consommation par employés associés**	**Nombre annuel moyen d'emplois**
10 800 emplois	5 950 emplois	**16 750 emplois**	5 760 emplois	**22 500 emplois**

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020; modélisation économique d'ISDE fondée sur les plus récents multiplicateurs d'entrées-sorties (2016) de Statistique Canada et les multiplicateurs d'impact économique spécifiques connexes les plus proches qui ont trait à l'industrie de la cybersécurité.

Annexe 4 : Tableaux de données (suite)

Tableau II : Répartition régionale

Répartition régionale	Ouest et Nord du Canada	Ontario	Québec	Canada atlantique
Répartition de l'emploi dans l'industrie de la cybersécurité	24 %	52 %	19 %	5 %

Tableau III : Intensité des ventes aux organismes militaires et de sécurité selon les types de produits et de services, 2018

Catégories	Intensité des ventes aux organismes militaires et de sécurité selon les types de produits et de services, 2018
Solutions en matière d'infrastructures	38 %
Tests d'intrusion et surveillance des menaces	16 %
Expertise judiciaire et formation	13 %
Vérifications de la conformité et conception de programmes	11 %
Solutions regroupées	8 %
Systèmes de contrôle industriels (SCI)	5 %
Chiffrement	5 %

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020

Annexe 4 : Tableaux de données (suite)

Tableau IV : répartition par taille d'entreprise

Répartition par taille	Part du recensement total de l'industrie de la cybersécurité	Part des ventes totales de l'industrie de la cybersécurité	Part de l'emploi total dans le secteur de la cybersécurité	Part de la R-D totale de l'industrie de la cybersécurité	Part des exportations totales de l'industrie de la cybersécurité
Entreprises comptant moins de 250 employés	89 %	39 %	45 %	47 %	36 %
Entreprises comptant entre 250 et 499 employés	6 %	37 %	32 %	13 %	29 %
Entreprises ayant un effectif de 500 employés ou plus	5 %	24 %	23 %	40 %	35 %
Total des entreprises	**100 %**	**100 %**	**100 %**	**100 %**	**100 %**

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020

Annexe 4 : Tableaux de données (suite)

Tableau V : répartition selon la profession et le sexe

Répartition selon la profession	Part de l'emploi par profession	Répartition selon la profession et le sexe	Proportion de l'emploi dans les professions selon le sexe
STIM	61 %	STIM homme	74 %
		STIM femme	26 %
Employés à la production	2 %	Travailleur à la production	83 %
		Travailleuse à la production	17 %
Fonctions organisationnelles	36 %	Fonctions organisationnelles, homme	57 %
		Fonctions organisationnelles, femme	43 %

Tableau VI : Sources de fonds pour la R-D

Sources de la R-D	Part de la répartition de la R-D
Fonds internes des entreprises pour la R-D	89,5 %
Fonds de R-D du gouvernement	5,0 %
Contrats de R-D pour d'autres entreprises	3,0 %
Autres	2,5 %

Types de R-D	Part de la répartition de la R-D
Recherche de base	17 %
Recherche appliquée	38 %
Développement expérimental	45 %

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020

Annexe 4 : Tableaux de données (suite)

Tableau VII : Répartition des marchés intérieurs et étrangers

Ventes intérieures de cybersécurité	63 %	Ventes à l'exportation de cybersécurité	37 %
Ventes intérieures par type de client*		***Ventes à l'exportation par destination***	
• Gouvernement fédéral canadien	13 %	• États-Unis	72 %
• Autres clients canadiens	87 %	• Europe	17 %
		• Asie et Océanie	4 %
		• Amérique centrale, Caraïbes et Amérique du Sud	4 %
		• Moyen-Orient et Afrique	3 %
Total des ventes intérieures en cybersécurité	**100 %**	**Total des ventes à l'exportation en cybersécurité**	**100 %**

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), 2020
* La répartition des ventes intérieures totales entre les clients nationaux exclut la répartition des clients qui n'est pas précisée.

Annexe 5 : Définition de l'industrie de la cybersécurité

Définition des catégories de cybersécurité

Cybersécurité

Sont exclues de cette enquête les catégories suivantes :
Ventes de biens et de services (**p. ex**. matériel, logiciels, services-conseils, R-D, services de cybersécurité hébergés) essentiellement produits ou fournis par des installations et des employés situés hors du Canada et livrés tels quels à des clients au Canada ou à l'étranger.
Sont donc **exclues** les ventes relatives à toute opération avec des entités, intermédiaires ou représentants au Canada d'entités commerciales, ou toute opération organisée ou conclue par leur intermédiaire, relative à des biens et/ou services provenant essentiellement d'entreprises hors du Canada. Ventes relatives aux activités de distribution, de commerce de détail et de commerce de gros.

Services et solutions d'infrastructure de cybersécurité pour la protection continue des réseaux et des données

Cette catégorie **comprend** les ventes associées à la production de biens et/ou à la prestation de services (notamment la recherche, le développement, la conception, l'ingénierie, la mise à l'essai et l'évaluation), dans les domaines suivants :
services et solutions permettant d'établir une protection continue de réseaux et de données. Cela **inclut** la conception, l'intégration et la fourniture d'une infrastructure de sécurité.

Ces solutions peuvent **inclure** ou être associées à ce qui suit, sans nécessairement s'y limiter :
pare-feu et nouvelle génération de pare-feu;
systèmes de détection et de prévention d'intrusion (SPI/SDI);
fournisseurs de services de sécurité gérés;
pare-feu d'applications Web;
passerelles de messagerie électronique sécurisées;
sécurité, détection et intervention relatives aux terminaux;
détection de menaces internes;
gestion/contrôle de l'identité et de l'accès. Il peut également **s'agir** de systèmes et de logiciels associés à l'authentification ou à la reconnaissance d'utilisateurs fondée sur l'image, la voix et d'autres techniques analytiques biométriques (ou diverses combinaisons de méthodes d'authentification à plusieurs facteurs) afin d'assurer uniquement un accès et une utilisation autorisés des cybersystèmes;
outils de sécurité d'applications, comme l'autoprotection d'applications d'exécution (RASP);
services associés à la conception, à l'intégration et à l'installation de systèmes de sécurité;
orchestration et automatisation de la cybersécurité;
des solutions de cybersécurité en nuage;
autres technologies visant à fournir une protection contre des attaques utilisant des techniques cryptanalytiques, comme une analyse latérale d'émanations ou de signaux physiques (**p. ex.** champs et impulsions électromagnétiques, consommation d'électricité, dissipation thermique) d'appareils au cours de leur processus de fonctionnement. Des exemples de types d'attaques **comprennent**, sans s'y limiter, celles faisant intervenir des attaques temporelles, des analyses électriques ou électromagnétiques et des attaques microarchitecturales.

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020

Annexe 5 : Définition de l'industrie de la cybersécurité (suite)

Définition des catégories de cybersécurité

Solutions de cybersécurité fondées sur un ensemble unique de services, de logiciels et/ou de matériel et comportant des éléments de plusieurs des autres catégories de cybersécurité précisées dans le cadre de cette enquête

Cette catégorie **comprend** les ventes de biens et/ou de services (y compris les services de recherche, de développement, de conception, d'ingénierie, de mise à l'essai et d'évaluation) liés aux éléments suivants :
Les solutions qui permettent d'aborder les exigences de cybersécurité des clients en leur fournissant une offre unique de services, de logiciels et/ou de matériel comprenant des éléments liés à plusieurs des autres catégories de biens et de services de cybersécurité, ainsi qu'aux fonctions ou tâches qui y sont associées.
Les ventes de biens et de services de cybersécurité qui peuvent être répartis en fonction des autres catégories de biens et de services de cybersécurité devraient être déclarées dans le cadre de ces catégories respectives et NE devraient PAS être déclarées dans le cadre de la présente catégorie de ventes.

Chiffrement

Cette catégorie **comprend** les ventes associées à la production de biens et/ou à la prestation de services (notamment la recherche, le développement, la conception, l'ingénierie, la mise à l'essai et l'évaluation), dans les domaines suivants :
Chiffrement matériel ou logiciel ou services permettant de développer ou d'appliquer un chiffrement. (Cela peut également **comprendre**, sans s'y limiter, des activités liées à des algorithmes et à un chiffrement de résistance à l'informatique quantique).
Exclusion :
Il ne faut **inclure** ici l'intégration ou la revente d'un produit de chiffrement commercial;
chiffrement principalement **inclus** dans une autre catégorie de biens et de services.

Vérifications de conformité et conception de programmes, élaboration de stratégies, et services de gestion des risques et de consultation connexes

Cette catégorie **comprend** les ventes liées à la production de biens et/ou à la prestation de services (y compris les services de recherche, de développement, de conception, d'ingénierie, de mise à l'essai et d'évaluation) comme ceux qui sont liés aux éléments suivants :
vérifications de cybersécurité et vérifications de conformité;
élaboration de stratégies sur la cybersécurité;
conception de programmes sur la conformité à la cybersécurité;
autres services de gestion des risques connexes et de consultation.

Systèmes de contrôle industriels (SCI); systèmes de contrôle et d'acquisition des données (SCADA) et technologie d'exploitation (TE) associés à la cybersécurité

Cette catégorie **comprend** les ventes associées à la production de biens et/ou à la prestation de services (notamment la recherche, le développement, la conception, l'ingénierie, la mise à l'essai et l'évaluation), dans les domaines suivants :
Toute solution et tout service associés à la cybersécurité visant à protéger des systèmes de contrôle industriels, des SCADA ou une technologie d'exploitation (TE). Cela peut, par exemple, **comprendre**, sans s'y limiter, des modules de sécurité matériels ou des modules cryptographiques matériels.
Incluant la protection de réseaux de TI d'entreprises.

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020

Annexe 5 : Définition de l'industrie de la cybersécurité (suite)

Définition des catégories de cybersécurité
Tests d'intrusion et évaluations de vulnérabilité et de menace associées. Surveillance des menaces du cyberespace, détection, services de renseignements et mesures de cyberdéfense actives Cette catégorie **comprend** les ventes liées à la production de biens et/ou à la prestation de services (qui peuvent **comprendre** les services de recherche, de développement, de conception, d'ingénierie, de mise à l'essai et d'évaluation) liés aux éléments suivants : tests d'intrusion; évaluations de la vulnérabilité. Les activités dans le cyberdomaine ou le cyberespace liées aux efforts de détection, de surveillance, d'analyse, de compréhension et/ou de prévision des cybermenaces pour, par exemple, améliorer la sensibilisation situationnelle des parties et leur capacité à adapter ou renforcer leurs mesures de cyberdéfense en conséquence afin de prévenir ou d'atténuer d'éventuels échecs en matière de cybersécurité. La mise en œuvre de mesures de cyberdéfense plus dynamiques, comme celles qui visent à préserver la capacité d'une partie défenderesse de mener ses activités en toute liberté dans le cyberespace et de protéger les données, les réseaux, les capacités axées sur les réseaux, l'infrastructure et les autres systèmes, biens et propriétés en recherchant, détectant, éliminant et/ou atténuant les cybercapacités et cyberactions offensives ou abusives de la menace.
Produits et/ou services associés à l'expertise judiciaire, aux enquêtes et aux interventions relatives aux cyberattaques ou autres cyberincidents et cyberintrusions Cette catégorie **comprend** les ventes associées à la production de biens et/ou à la prestation de services (notamment la recherche, le développement, la conception, l'ingénierie, la mise à l'essai et l'évaluation), dans les domaines suivants : Services et outils logiciels intervenant dans la détermination, l'évaluation et l'intervention en matière de cyberattaques et de cyberincidents. Exemples non exhaustifs : expertise judiciaire relative aux réseaux; services et outils de recherche associés; analyses de fraudes; identification d'auteurs internes; autres services d'intervention en cas d'incidents.
Formation en cybersécurité Cette catégorie **comprend** les ventes associées à la production de biens et/ou à la prestation de services (notamment la recherche, le développement, la conception, l'ingénierie, la mise à l'essai et l'évaluation), dans les domaines suivants : formation; perfectionnement de la main-d'œuvre; services ou solutions d'enseignement. Cela **comprend** tous les niveaux, des utilisateurs de base aux praticiens plus avancés, et couvre des services, des didacticiels, des logiciels ou d'autres mécanismes de prestation.

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020

Annexe 5 : Définition de l'industrie de la cybersécurité (suite)

Définition des catégories de cybersécurité

Autres biens et services associés à la cybersécurité

Cette catégorie **comprend** les ventes associées à la production de biens et/ou à la prestation de services (notamment la recherche, le développement, la conception, l'ingénierie, la mise à l'essai et l'évaluation), dans les domaines suivants :

Autres activités pouvant être jugées comme étant associées à la cybersécurité (notamment celles dépassant les simples activités défensives ou passives associées à la cybersécurité).

Par exemple, les outils de protection de la vie privée et de dépersonnalisation ou d'anonymisation, les biens et services associés au soutien des opérations militaires dans l'ensemble du spectre non inclus dans les catégories de ventes précédentes.

Exclusions : ventes de biens et de services essentiellement produits ou rendus/fournis par des installations et des employés situés hors du Canada et livrés tels quels à des clients au Canada ou à l'étranger.

P. ex. les ventes relatives à toute opération avec des entités, des intermédiaires ou des représentants au Canada d'entités commerciales, ou toute opération organisée ou conclue par leur intermédiaire, pour des biens et/ou services provenant essentiellement d'entreprises hors du Canada; activités de distribution, de commerce de détail et de commerce de gros.

Autres définitions associées à la cybersécurité :

Services gérés (ou cybersécurité hébergée)

Prestations aux clients de services tels que la gestion et l'assurance tierce continue de la cybersécurité et de la résilience des systèmes, réseaux et renseignements des clients (notamment la surveillance continue, la détection des menaces et des attaques et l'intervention en cas d'incident) pour des clients qui choisissent d'externaliser de telles fonctions.

De tels services peuvent également **inclure** la responsabilité de l'installation du matériel, des appareils et des logiciels associés, ainsi que la configuration, l'intégration, l'exploitation et l'entretien de solutions de cybersécurité complètes à jour pour les clients choisissant d'externaliser leur infrastructure de TI et les fonctions de cybersécurité.

Des exemples de services associés de soutien à des mesures de sécurité externalisées peuvent **inclure**, sans s'y limiter :

Gestion des renseignements et événements de sécurité, prévention de la perte de données, systèmes de détection des intrusions (SDI)/systèmes de prévention des intrusions (SPI), analyses des menaces, gestion de la vulnérabilité, recherches, intervention en cas d'incident et services d'Officier principal de la sécurité de l'information (OPSI).

Source : Enquête sur les industries canadiennes de la défense, de l'aérospatiale, de la marine et de la cybersécurité (2018), enquête de 2018 publiée en 2020


Canada