Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Le Cadre des Compétences en Matière de Cybersécurité du Canada

Adapter le cadre de perfectionnement de la main-d'œuvre dans le domaine de la cybersécurité de la NICE (cadre de la NICE) au marché du travail canadien

Série gestionnaires

Canada

Avant-propos

Le Cadre des Compétences en Matière de Cybersécurité du Canada (ITSM.00.039) est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité). Pour obtenir de plus amples renseignements, prière d'envoyer un courriel ou de téléphoner au Centre de coordination des services du Centre pour la cybersécurité :

Centre de coordination des services
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

Étant donné la nature hautement dynamique de la cybersécurité, ce présent guide sera passé en revue chaque année par l'équipe des Relations et de la collaboration avec le milieu universitaire du Centre canadien pour la cybersécurité. Toutes les modifications proposées à la présente publication devraient être envoyées par courriel à :

academicoutreach-collaborationacademique@cyber.gc.ca.

Date d'entrée en vigueur

Le présent document entre en vigueur en 19 avril 2023.

Historique des révisions

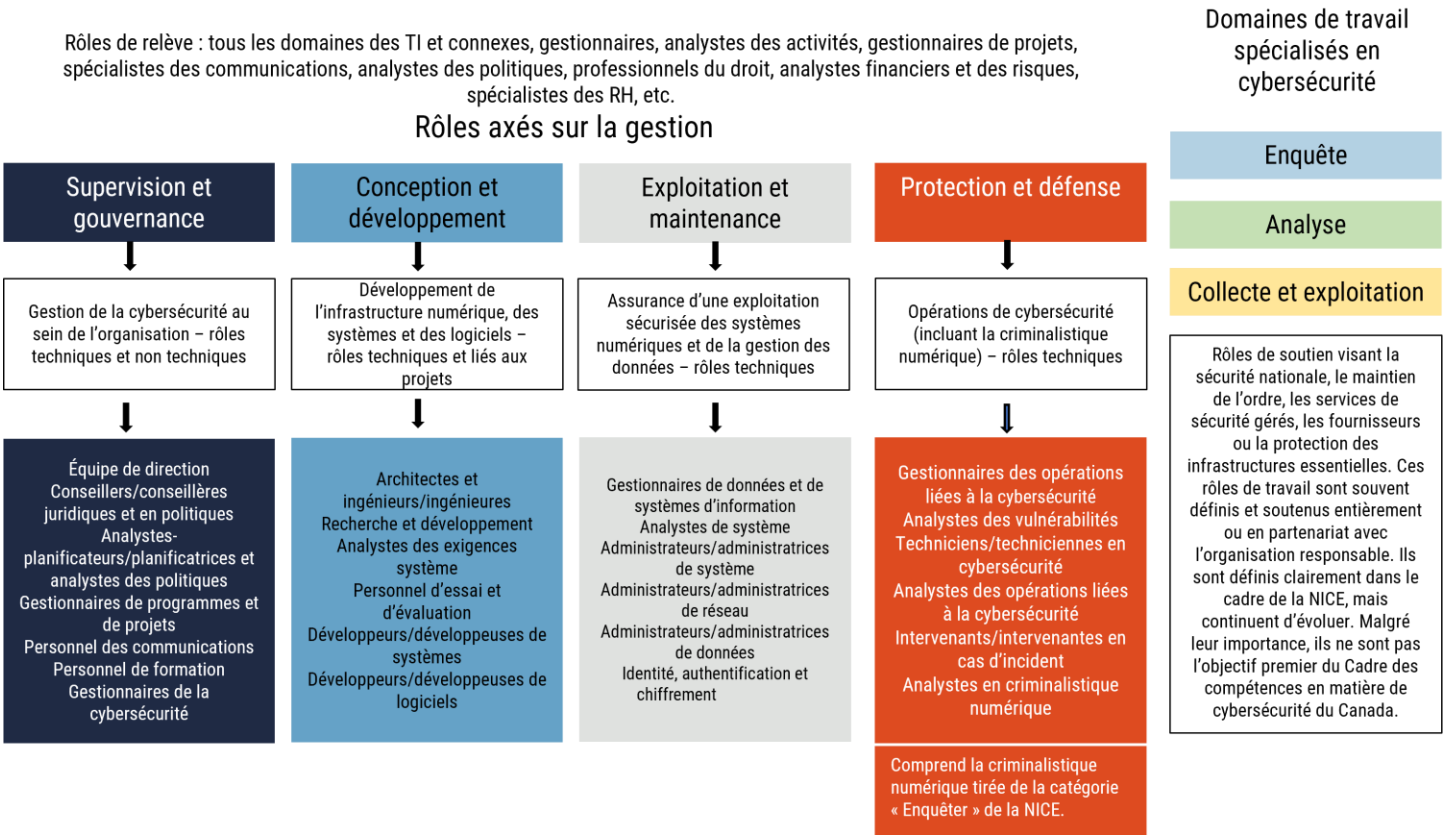
Version	Modifications	Date
1	Première version	19 avril 2023

ISBN 978-0-660-46232-5
No de cat. D97-4/00-039-2022F-PDF

Vue d'ensemble

Le Cadre des compétences en matière de cybersécurité du Canada (figure 1) s'appuie sur les éléments cadre de perfectionnement de la main-d'œuvre dans le domaine de la cybersécurité (en anglais seulement) de la NICE des États-Unis (cadre de la NICE) tout en s'adaptant au marché du travail canadien. Ce modèle, qui repose sur le cadre de la NICE et vise à le simplifier, est axé sur les activités, reconnaît les talents du point de vue de la sécurité organisationnelle et constitue un modèle plus accessible aux intervenantes et aux intervenants qui n'œuvrent pas dans le domaine de la cybersécurité.

Figure 1 : Cadre des compétences en matière de cybersécurité du Canada



Tirant avantage des principaux éléments et des principales caractéristiques du cadre de la NICE, le Cadre des compétences en matière de cybersécurité du Canada vise à faire ce qui suit :

- aider à préciser les lacunes dans la main-d'œuvre du domaine de la cybersécurité qui existent sur le marché du travail canadien en approchant la question du point de vue des entreprises et en établissant une distinction entre les rôles de base en cybersécurité et les rôles organisationnels qui assument certaines responsabilités en matière de cybersécurité ou des rôles connexes dans le domaine;
- simplifier la représentation du travail lié à la cybersécurité qui est commun à la plupart des organisations;
- adapter le cadre de manière à soutenir les responsabilités plus vastes ou généralistes qui sont communes aux petites et moyennes organisations (PMO), alors qu'elles s'efforcent de répondre aux exigences fondamentales en matière de technologies de l'information (TI) et de cybersécurité;

- continuer de mettre l'accent sur les responsabilités en cybersécurité des rôles de travail dans les secteurs de la supervision et de la gouvernance, de la conception et du développement, et de l'exploitation et de la maintenance.

Le Cadre des compétences en matière de cybersécurité au Canada présente avec simplicité le travail lié à la cybersécurité au sein de nombreuses organisations du secteur privé et de petits organismes du secteur public. L'objectif de ce cadre est d'aider à mieux guider les intervenantes et les intervenants en développement de la main-d'œuvre pour combler le déficit de compétences en cybersécurité. Il peut s'appliquer tant aux secteurs public et privé qu'au milieu universitaire aux fins de sensibilisation et de développement de carrières, de formation et d'éducation, de recrutement ou de planification de l'effectif.

Table des matières

Liste des figures

Liste des tableaux

1 Canadianisation du cadre de la NICE

1.1 Contexte

La norme professionnelle nationale (NPN) définit les principaux éléments du travail en cybersécurité comme étant distincts des autres professions liées aux TI, à la sécurité, à la gestion des activités ou à l'administration publique. Cela dit, la cybersécurité ne se limite pas aux systèmes techniques. Elle englobe les gens, leurs comportements et la façon dont ils se connectent à ces systèmes et les utilisent.

On ne saurait trop insister sur l'importance que revêt l'efficacité de la cybersécurité, ainsi que des produits et services soutenus par les professionnels de la cybersécurité. Les emplois en cybersécurité sont désormais reconnus à travers le monde comme des carrières essentielles et durables dans l'économie numérique.

Au Canada, la dépendance aux systèmes d'information et de données a connu une augmentation exponentielle au cours de la dernière décennie alors que les organisations ont misé sur la numérisation de leurs activités et se sont tournées vers une présence en ligne. Pour ce faire, elles ont dû compter sur des professionnelles et professionnels capables de concevoir, de construire, de mettre en œuvre et de maintenir des systèmes d'information sûrs, sécurisés et fiables qui peuvent répondre à une multitude de besoins organisationnels, opérationnels et personnels.

Les citoyennes et citoyens canadiens sont de plus en plus conscients de leurs droits en matière de respect de la vie privée et se préoccupent de plus en plus de la façon dont les organisations protègent leurs données personnelles. Il faut donc compter sur des spécialistes en cybersécurité et en protection des renseignements personnels qui peuvent formuler des conseils sur les diverses normes nationales et internationales, élaborer des politiques, déterminer les besoins et soutenir la surveillance pour mieux protéger la vie privée des Canadiennes et des Canadiens.

La cybercriminalité est une menace en constante évolution. Selon l'Évaluation sur les cybermenaces nationales 2020 du Centre pour la cybersécurité, « [l]es auteurs de cybermenace représentent un risque pour l'économie canadienne en raison des coûts élevés que doivent subir les particuliers et les entreprises, notamment lors du vol de propriété intellectuelle et de renseignements exclusifs » [1]. De l'expertise est donc requise pour soutenir la détection des cybermenaces et la prise de mesures d'intervention, et aider les personnes qui mènent les enquêtes et collectent les preuves numériques pouvant servir à renforcer les protections et à poursuivre les contrevenants, le cas échéant.

La cybersécurité ne concerne pas seulement les systèmes. Elle touche aussi les personnes qui se connectent au moyen de ces systèmes. Elle continuera d'être nécessaire à un large éventail de technologies. Des possibilités de carrière importantes et durables s'offrent donc aux personnes qui travaillent dans ce domaine et leur permettent de toucher positivement la vie des Canadiennes et des Canadiens connectés et de soutenir l'avenir de l'économie numérique.

Par conséquent, les entreprises et les industries ont du mal à satisfaire leurs besoins en matière de cybersécurité. Le perfectionnement de la main-d'œuvre est confronté à quatre grands défis :

- générer et retenir des talents dans le domaine des opérations de cybersécurité pour répondre aux besoins du marché du travail canadien;
- s'assurer que les rôles techniques et non techniques contributifs possèdent les connaissances, compétences et aptitudes requises;

- être attentif à l'évolution du contexte technologique;
- normaliser l'emploi et les activités en cybersécurité en milieu de travail au Canada.

Pour aider à surmonter ces défis, un groupe d'intervenantes et d'intervenants de l'industrie, du gouvernement et du milieu universitaire a formé l'Alliance des talents en cybersécurité (ATC) (voir l'annexe F). Le groupe a travaillé de concert pour fournir les éléments suivants :

- un cadre de compétences en matière de cybersécurité, dont une taxonomie et un lexique commun qui décrit le travail et les travailleurs en cybersécurité, qui repose sur les éléments du cadre de la NICE des États-Unis[1] (ci-après désigné le cadre de la NICE) tout en s'adaptant au marché du travail canadien;
- les descriptions de la NPN basées sur le cadre de compétences;
- les résultats d'apprentissage tirés de domaines de main-d'œuvre pertinents;
- les ressources connexes qui appuient la main-d'œuvre, le développement de carrière et l'apprentissage.

[1] Le cadre de perfectionnement de la main-d'œuvre dans le domaine de la cybersécurité de la NICE (ou en anglais, *NICE Workforce Framework for Cybersecurity*), anciennement appelé le NICE Cybersecurity Workforce Framework, a changé de nom en 2020 pour reconnaître que la cybersécurité est une préoccupation commune à tous les effectifs, et non pas unique aux effectifs de la cybersécurité.

2 Brève introduction au cadre de la NICE

Avant le cadre de la NICE, le travail en cybersécurité était perçu et décrit d'une multitude de façons au sein du gouvernement fédéral américain, ce qui s'avérait fort problématique pour ce qui est du recrutement, de la sélection, de la formation et des autres activités de perfectionnement de l'effectif dans les secteurs public et privé. Cette situation était insoutenable compte tenu des menaces grandissantes qui pesaient sur la sécurité nationale et économique. Fondé à la fin des années 2000, le premier groupe de travail de la NICE a été mis sur pied en 2011 par la National Institute of Standards and Technology (NIST) des États-Unis avec **d'autres** partenaires fédéraux américains. Depuis, plus de 20 ministères fédéraux américains, des intervenants des secteurs de la défense et de la sécurité, des établissements du milieu universitaire et, dans une moindre mesure, des alliés internationaux comme le Canada et l'Australie ont contribué au développement et à l'évolution du cadre de la NICE.

Le cadre de la NICE offre une vue intégrée de la main-d'œuvre en cybersécurité. Il permet ainsi d'identifier les rôles de travail qui ont une incidence sur la capacité de l'organisation à protéger ses données, ses systèmes et ses activités [2]. Cela comprend tant les rôles techniques que non techniques destinés à soutenir les efforts de l'organisation en matière de gestion des risques liés à la cybersécurité. De plus, le cadre de la NICE comprend des capacités de cyberopérations nationales, dont les rôles liés au renseignement et aux opérations offensives qui relèvent généralement du gouvernement fédéral ou d'institutions partenaires. Notamment, le cadre de la NICE comporte un processus de surveillance et de révision permettant de veiller à ce qu'il réponde aux besoins grandissants de la collectivité de la cybersécurité.

2.1 Le cadre américain de la NICE dans le contexte canadien

Le cadre de la NICE propose une vue exhaustive du travail effectué en cybersécurité. Ce projet visait à comprendre la mesure dans laquelle les entreprises et les organisations industrielles du Canada étaient prêtes à adopter un tel cadre. Il a d'ailleurs permis de répondre à quelques questions clés.

1. **Quels sont les principaux enjeux associés à la main-d'œuvre canadienne en cybersécurité?**

L'exploration des différences et des similitudes entre le marché du travail des États-Unis et du Canada dans le domaine de la cybersécurité soulève plusieurs problèmes.

Similitudes :

- On manque d'information sur le marché du travail en ce qui a trait aux emplois en cybersécurité, aux titres d'emplois connexes et aux rôles dans ces deux pays;
- Selon les rôles de travail tirés du cadre de la NICE, on estime que le Canada a un écart plus grand à combler comparativement aux États-Unis;
- Au Canada, moins de ressources sont consacrées aux enjeux liés à la main-d'œuvre en cybersécurité et on y porte moins attention;
- La cybersécurité est un environnement professionnel hautement concurrentiel dans les deux pays.

Différences :

- Bien qu'il soit similaire à celui des États-Unis, le marché du travail du Canada est beaucoup plus petit et la population active est plus dispersée;
- Au Canada, les ressources doivent être fournies dans les deux langues officielles;
- Une grande partie de l'économie canadienne est composée de petites et moyennes organisations (PMO) et leurs besoins diffèrent de ceux des grandes organisations;
- Le cadre de la NICE porte peu attention aux entreprises et aux industries canadiennes et à la façon dont il s'applique au marché du travail canadien.

2. **Dans quelle mesure l'adoption du cadre de la NICE sera-t-elle facile?**

Conformément à ce qui est indiqué dans le cadre de la NICE, d'autres pays peuvent adapter le cadre selon leur contexte respectif [3]. Par ailleurs, les pays de la collectivité des cinq[2] honorent une longue tradition et échangent leurs publications et leurs processus avec leurs partenaires. Le Canada partage son travail avec les États-Unis et, comme on peut le voir, plusieurs publications du gouvernement fédéral canadien, comme les conseils en matière de sécurité des TI, sont basées sur les publications du NIST[3] ou s'en inspirent fortement.

3. **Quels sont les avantages et les inconvénients d'adopter le cadre de la NICE dans sa forme actuelle?**

Avantages :

- Il est facilement accessible pour les intervenants du marché du travail canadien et du perfectionnement de l'effectif;
- Il normalise les descriptions des rôles de travail en cybersécurité et établit un lexique commun pour la collectivité du Canada, des États-Unis et d'autres pays;
- Il offre une description détaillée des connaissances, compétences et aptitudes communes aux rôles liés à la cybersécurité et a récemment introduit les compétences connexes qui faciliteront la formation, l'éducation et l'avancement professionnel;
- Il établit une base de référence connue pour évaluer les candidats qualifiés;
- Il est soutenu à l'échelle internationale par les autres gouvernements;
- Il tient compte de la transférabilité des travailleurs à l'échelle nationale et internationale;
- Plusieurs des rôles de travail, des tâches et des connaissances, compétences et aptitudes sont valides au sein de l'effectif canadien en cybersécurité.

Inconvénients :

- Il manque de précision en ce qui concerne les lacunes à combler sur le plan de l'effectif;
- Il est trop « vaste » ou trop granulaire pour le marché du travail général du Canada;
- Il est difficile à naviguer (p. ex. utilisation de codes pour établir des références entre les connaissances, compétences et aptitudes et les descriptions de mots);

[2] La collectivité des cinq est le nom informel de l'accord international d'échange de renseignement conclu entre le Canada, les États-Unis, le Royaume-Uni, l'Australie et la Nouvelle-Zélande.
[3] Pour des exemples de telles publications, prière de visiter le https://www.cyber.gc.ca/fr/publications.

- Il est axé sur l'« industrie de la défense » ou adapté aux grandes organisations dont les activités sont largement effectuées en ligne;
- Il est structuré selon une perspective statique ou horizontale, puisqu'il est difficile de voir les cheminements de carrière ou les avancements latéraux ou verticaux dans le domaine de la cybersécurité;
- Il ne convient pas aux petites organisations;
- Il ne tient pas compte des fonctions des généralistes de la cybersécurité (p. ex. agents ou agentes de sécurité d'entreprise) ou des personnes qui soutiennent plusieurs rôles liés à la cybersécurité dans un cadre de travail typique que l'on retrouve souvent dans les petites et moyennes organisations non techniques;
- Il minimise des rôles importants et distincts en les intégrant à des rôles plus élargis (p. ex. le génie en cybersécurité fait partie du rôle de recherche et de développement);
- Il ne tient pas compte des rôles liés à la sécurité des technologies opérationnelles et industrielles (p. ex. systèmes de contrôle industriels [SCI] et télésurveillance et acquisition de données [SCADA pour *Supervisory Control and Data Acquisition*]);
- Il omet les rôles nouveaux et émergents qui émanent du domaine dynamique de la cybersécurité.

Le cadre de la NICE ne reflète pas nécessairement une structure et des fonctions professionnelles communes à toutes les organisations des secteurs privé et public non fédéral du Canada.

Bien qu'il existe plusieurs autres rôles contributifs ou adjacents à la cybersécurité, tel qu'il est indiqué dans le cadre de la NICE, le présent document met l'accent sur les rôles principaux liés à la cybersécurité et les compétences connexes qui relèvent d'un contexte opérationnel canadien plus large où la majorité du travail dépend des objectifs et des résultats de la cybersécurité organisationnelle. Le cadre de la NICE répertorie principalement les spécialisations en cybersécurité qui relèvent du renseignement, de la sécurité nationale ou du maintien de l'ordre.

2.2 Remarque spéciale à l'intention des éducateurs et éducatrices

On reconnaît le rôle inestimable que jouent les éducateurs et éducatrices en cybersécurité. Par contre, comme ils sont régis par leur propre Classification nationale des professions (CNP) et un vaste réseau de normes professionnelles, il est inutile de répéter cette information dans la présente publication. Force est de constater qu'il nous faut compter sur des éducateurs et éducatrices qualifiés ayant l'expérience et les capacités nécessaires pour faciliter et évaluer l'apprentissage requis pour soutenir la demande de l'industrie conformément aux normes reconnues.

2.3 Normes professionnelles nationales (NPN)

Les normes professionnelles nationales (NPN) décrivent ce qu'une personne occupant un poste particulier doit savoir et être en mesure de faire pour être jugée « compétente » dans ce poste. On définit ces normes en fonction des compétences, y compris les connaissances, compétences et aptitudes exigées pour effectuer le travail efficacement, correctement et en toute sécurité. Les NPN établissent les bases d'un rendement compétent dans les lieux de travail comme en a convenu un échantillon représentatif de travailleurs, d'employeurs et d'autres intervenants. Les NPN peuvent également être régies ou dictées par d'autres exigences externes, comme la conformité juridique ou le respect des politiques.

Figure 2 : Utilisations des NPN

Praticiens/praticiennes	Employeurs	Éducateurs/éducatrices	Intervenants/intervenantes en perfectionnement de l'effectif
Poser les bases du développement de carrière Orienter leur apprentissage et leur perfectionnement au sein de la profession Appuyer la mobilité et la transition professionnelles	Déterminer les rôles et les tâches clés Déterminer les besoins en matière de perfectionnement professionnel Assurer une description objective des postes Orienter le recrutement	Déterminer les domaines nécessitant de l'expertise Poser les bases des programmes d'études, du développement de la formation et de l'éducation – fournisseurs des secteurs privé et public Améliorer les programmes d'études Poser les bases des programmes de certification et de l'accréditation des programmes	Créer des occasions de perfectionnement professionnel Déterminer les compétences requises pour des postes particuliers Adopter comme référence des pratiques exemplaires reconnues à l'échelle nationale et axées sur les secteurs Fournir de l'information sur le perfectionnement professionnel aux praticiens et praticiennes qui montent les échelons vers des postes de gestion

3 Adapter le cadre de la NICE au marché du travail canadien

3.1 Attributs d'un cadre de compétence réaliste pour le marché canadien

L'adoption et la simplification du cadre de la NICE pour le marché du travail du Canada rendent l'utilisation du cadre canadien plus facile pour les entreprises et les industries ayant du mal à interpréter le cadre de la NICE dans sa forme initiale.

Comme il est indiqué à la figure 3, l'adoption du cadre de la NICE dans un contexte canadien repose sur la considération de cinq attributs principaux. Ces attributs ont été déterminés en fonction de certaines critiques et de certains problèmes structurels entourant le cadre de la NICE, et en tenant compte de la rétroaction obtenue de la collectivité dans le cadre de consultations.

Figure 3 : Attributs souhaités pour le Cadre canadien des compétences en matière de cybersécurité

Spécificité et précision	Bien que le cadre de la NICE décrive l'ensemble complet des rôles de travail en cybersécurité, il devrait être possible de mettre l'accent sur ceux qui sont les plus pertinents pour combler les écarts de compétences en cybersécurité au Canada et répondre au contexte canadien.
Utilisabilité et accessibilité	Le cadre devrait faciliter l'utilisation, la lisibilité et l'accessibilité du contenu pour tous les lecteurs et utilisateurs potentiels, dont ceux qui ne sont pas familiers avec le travail en cybersécurité. Plus précisément, le cadre ne devrait pas isoler la cybersécurité, mais bien intégrer les concepts dans un contexte opérationnel et organisationnel plus large.
Clarté des concepts	Il convient de décrire clairement les rôles liés à la cybersécurité et de tenir compte tant des rôles techniques et multidisciplinaires que des rôles de spécialistes et de généralistes.
Adaptabilité	Compte tenu de la nature dynamique de ce document, il convient de mettre en place un mécanisme permettant d'intégrer rapidement les rôles nouveaux ou émergents qui résultent des technologies comme l'automatisation, l'infonuagique, l'intelligence artificielle, l'informatique quantique, ainsi que des connaissances, compétences et aptitudes qui soutiennent l'ensemble des activités de cybersécurité. Le cadre doit constamment évoluer en fonction du travail.
Évolutivité	Un cadre devrait pouvoir s'adapter facilement aux organisations de toutes tailles et aux différents contextes de l'industrie. Cela comprend la capacité des organisations à identifier et à développer les talents non techniques de sorte à soutenir leurs besoins en matière de sécurité.

3.1 Adapter le cadre canadien aux petites et moyennes organisations

Le cadre canadien peut être adapté aux PMO. En cybersécurité, la plupart des PMO présentent les caractéristiques suivantes :

- On y retrouve rarement des spécialistes en cybersécurité;
- Les rôles liés à la conception et au développement sont externalisés ou on doit acquérir des systèmes ou des applications grand public;
- Les personnes doivent souvent assumer plusieurs rôles, dont des tâches liées à la cybersécurité.

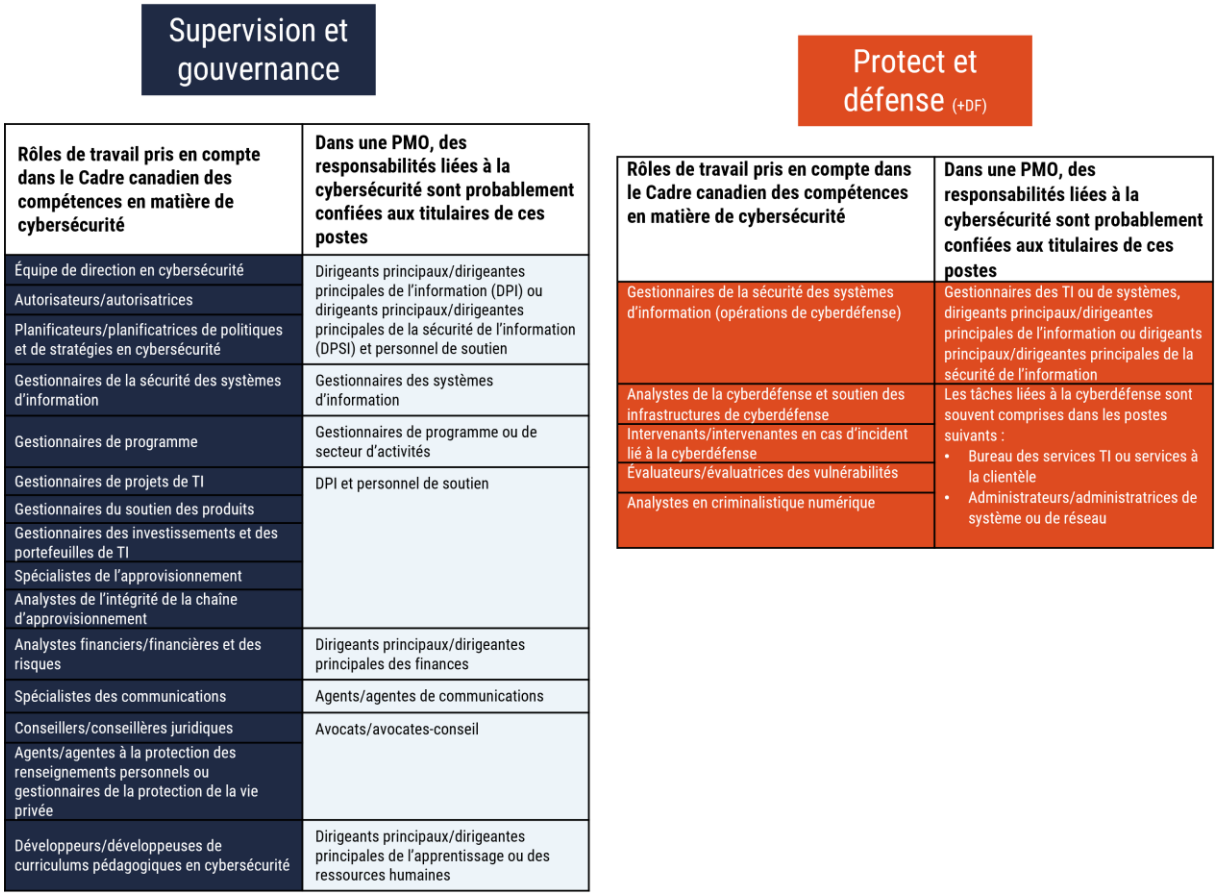
Par conséquent, lorsque les organisations examinent le cadre de la NICE, elles peuvent se sentir dépassées par l'ampleur de la tâche. Il est toutefois possible d'établir des scénarios ou de présenter des exemples qui aideront les PMO à adapter le cadre de la NICE en fonction du cadre canadien des compétences en matière de cybersécurité, ainsi qu'à définir les connaissances, compétences et aptitudes basées sur le rôle qui soutiendront la cybersécurité au sein des organisations.

La section suivante traitera des deux scénarios qui se produisent généralement dans les PMO.

1. **Organisation de taille moyenne avec personnel informatique interne**

On y retrouve une expertise technique à l'interne, mais plusieurs rôles liés à la cybersécurité sont assumés par des personnes qui occupent d'autres fonctions et ne sont généralement pas des spécialistes en cybersécurité, ou par de petites équipes de TI responsables de la détection et de l'intervention en cas d'incident. Dans cet exemple, le dirigeant principal ou la dirigeante principale de l'information (DPI) dirigerait la petite équipe de TI et serait responsable des aspects techniques du programme de cybersécurité, alors que les gestionnaires du niveau de la direction resteraient responsables de l'établissement des priorités organisationnelles et de la définition du contexte de risque. Il incomberait probablement à l'équipe de TI d'assumer toutes les fonctions Protection et défense, alors que les activités spécialisées seraient externalisées et confiées à une tierce partie.

Figure 4 : Rôles techniques possibles dans une organisation de taille moyenne



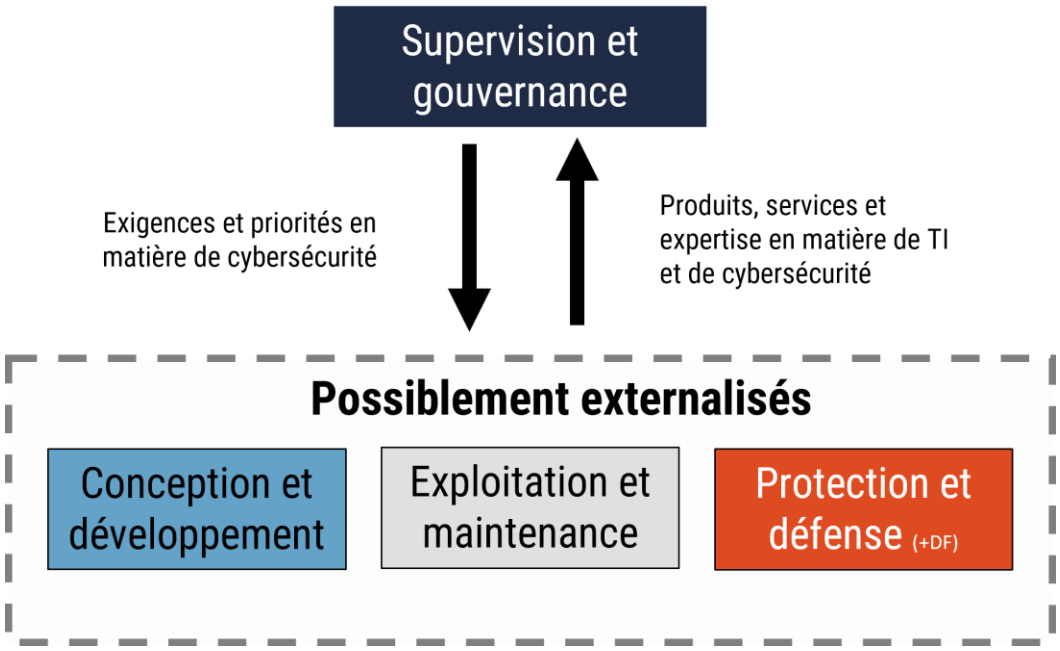
Rôles de travail pris en compte dans le Cadre canadien des compétences en matière de cybersécurité	Dans une PMO, des responsabilités liées à la cybersécurité sont probablement confiées aux titulaires de ces postes
Équipe de direction en cybersécurité	Dirigeants principaux/dirigeantes principales de l'information (DPI) ou dirigeants principaux/dirigeantes principales de la sécurité de l'information (DPSI) et personnel de soutien
Autorisateurs/autorisatrices	
Planificateurs/planificatrices de politiques et de stratégies en cybersécurité	
Gestionnaires de la sécurité des systèmes d'information	Gestionnaires des systèmes d'information
Gestionnaires de programme	Gestionnaires de programme ou de secteur d'activités
Gestionnaires de projets de TI	DPI et personnel de soutien
Gestionnaires du soutien des produits	
Gestionnaires des investissements et des portefeuilles de TI	
Spécialistes de l'approvisionnement	
Analystes de l'intégrité de la chaîne d'approvisionnement	
Analystes financiers/financières et des risques	Dirigeants principaux/dirigeantes principales des finances
Spécialistes des communications	Agents/agentes de communications
Conseillers/conseillères juridiques	Avocats/avocates-conseil
Agents/agentes à la protection des renseignements personnels ou gestionnaires de la protection de la vie privée	
Développeurs/développeuses de curriculums pédagogiques en cybersécurité	Dirigeants principaux/dirigeantes principales de l'apprentissage ou des ressources humaines

Rôles de travail pris en compte dans le Cadre canadien des compétences en matière de cybersécurité	Dans une PMO, des responsabilités liées à la cybersécurité sont probablement confiées aux titulaires de ces postes
Gestionnaires de la sécurité des systèmes d'information (opérations de cyberdéfense)	Gestionnaires des TI ou de systèmes, dirigeants principaux/dirigeantes principales de l'information ou dirigeants principaux/dirigeantes principales de la sécurité de l'information
Analystes de la cyberdéfense et soutien des infrastructures de cyberdéfense	Les tâches liées à la cyberdéfense sont souvent comprises dans les postes suivants : • Bureau des services TI ou services à la clientèle • Administrateurs/administratrices de système ou de réseau
Intervenants/intervenantes en cas d'incident lié à la cyberdéfense	
Évaluateurs/évaluatrices des vulnérabilités	
Analystes en criminalistique numérique	

2. Petite organisation avec une dépendance limitée à l'égard des TI et sans personnel informatique

La plupart des rôles de travail techniques seraient externalisés, mais l'organisation continuerait d'assumer les principales fonctions Supervision et gouvernance liées à la cybersécurité. Cette personne assumerait effectivement le rôle de généraliste de la sécurité.

Figure 5 : Rôles techniques possiblement externalisés dans une petite organisation



3.2 Généralistes en cybersécurité

Dans plusieurs PMO et même des organisations plus grandes dont les activités ne dépendent pas fortement d'Internet, on retrouve des personnes à qui des responsabilités en cybersécurité ont été confiées sans qu'elles aient nécessairement d'expérience en informatique ou en cybersécurité.

Si on tient compte du nombre de PMO dans l'environnement commercial du Canada, cela représente un très grand nombre de personnes sur le marché du travail canadien dont la principale responsabilité consiste à établir et à gérer la cybersécurité au sein de leur organisation et qui pourraient ne pas occuper l'un des rôles définis dans le cadre de la NICE ou le cadre canadien. En règle générale, ces personnes :

- accomplissent des tâches liées à la cybersécurité à temps partiel parallèlement à d'autres responsabilités;
- utilisent les connaissances, compétences et aptitudes en cybersécurité qui conviennent au contexte opérationnel, technique et de menace;
- ne sont pas considérées comme étant des professionnelles de la cybersécurité et ne suivent pas le parcours professionnel en cybersécurité.

À défaut d'avoir un terme précis, le présent document utilise « généraliste de la sécurité » pour les distinguer des spécialistes en cybersécurité mentionnés dans les rôles principaux. Dans un environnement organisationnel, le ou la généraliste de la sécurité n'est généralement pas spécialisé dans le domaine de la sécurité, mais est souvent responsable

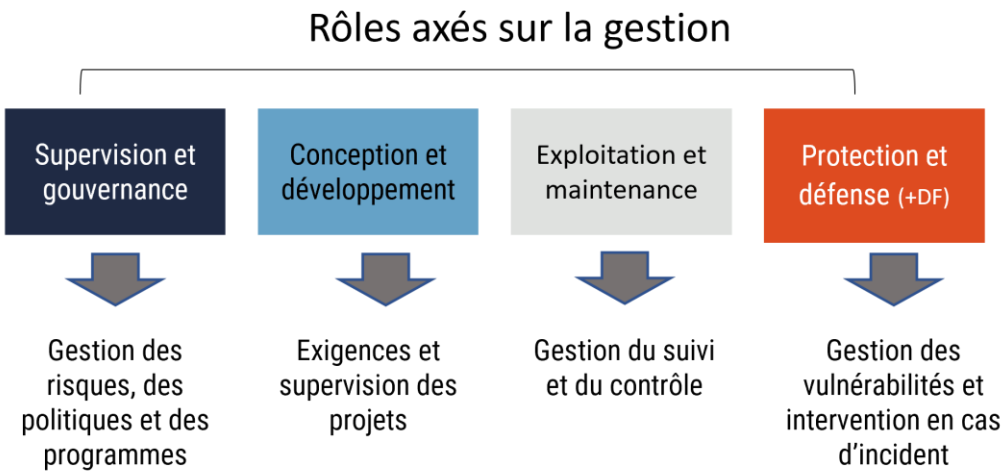
des activités liées à la sécurité physique, contractuelle, du personnel et de la prévention des pertes, en plus de la cybersécurité. Il arrive souvent, par exemple, que le ou la chef de la direction, le dirigeant principal ou la dirigeante principale de l'information (DPI), le dirigeant principal ou la dirigeante principale de l'information (DPF), l'agent ou l'agente de sécurité d'entreprise, le ou la gestionnaire des ressources humaines ou un haut fonctionnaire occupe un tel poste.

Ils doivent, entre autres, faire ce qui suit :

- évaluer la posture de cybersécurité de l'organisation;
- faciliter la détermination des risques de l'organisation en matière de cybersécurité;
- déterminer les contrôles de cybersécurité non techniques;
- identifier les spécialistes techniques internes ou externes et assurer la liaison avec eux pour ce qui est des contrôles techniques;
- élaborer des politiques et des plans organisationnels en matière de cybersécurité;
- conseiller les membres de la direction sur la formation et la sensibilisation à la sécurité;
- superviser et soutenir les spécialistes techniques, tant internes qu'externes, dans l'exercice de leurs fonctions en cybersécurité;
- coordonner la prise de mesures d'intervention en cas d'incident de cybersécurité;
- surveiller les mesures d'intervention et d'atténuation, en faire rapport et recommander des plans d'action basés sur conseils techniques;
- coordonner les activités d'analyse rétrospective des événements et des incidents et intégrer les leçons apprises aux politiques et procédures organisationnelles.

Pour bon nombre de ces tâches, on retrouve de multiples ressources en ligne pour guider les généralistes de la sécurité dans l'exécution de leurs tâches. L'efficacité de ces tâches repose toutefois sur les connaissances, compétences et aptitudes requises pour soutenir le processus décisionnel et la prise de mesures. Il est peu probable que les généralistes aient une formation ou une éducation approfondie en cybersécurité. On devrait donc leur offrir les occasions d'apprentissage nécessaires pour acquérir les compétences qui conviennent à leurs responsabilités, ainsi qu'au contexte technique, opérationnel et de menace. Comme le démontrent les exemples illustrés dans la figure ci-dessous, on doit souvent faire appel à des compétences tirées de certains des rôles de travail appartenant à chacune des grandes catégories d'emplois.

Figure 6 : Fonctions des généralistes de la sécurité



Connaissance de base :

- Contexte technique (p. ex. structure informatique organisationnelle, logiciels, dispositifs et politiques)
- Contexte de la cybermenace (dont les risques délibérés, accidentels et naturels)
- Contexte opérationnel (priorités, objectifs, marché, tendances)
- Contexte juridique, politique et éthique de la sécurité
- Gestion des risques liés à la cybersécurité dans le cadre du risque organisationnel
- Gestion des incidents de cybersécurité (propres à un domaine)
- Processus de cybersécurité, technologies, tendances et enjeux émergents
- Sources d'expertise et ressources en cybersécurité

Compétences et aptitudes de base :

- Prodiguer des conseils aux entreprises dans le contexte juridique et politique de la cybersécurité
- Faire preuve de prévoyance et planifier la sécurité de manière à soutenir les activités numériques et la croissance de l'organisation
- Transformer le cyberrisque en risque organisationnel
- Faire la distinction entre la conformité et le risque
- Interpréter les évaluations des menaces et des risques dans un contexte opérationnel
- Évaluer l'efficacité des contrôles de sécurité par rapport aux objectifs de sécurité de l'organisation

Compétences communes :

Pour tous les rôles principaux liés à la cybersécurité, peu importe le secteur d'activités ou la catégorie d'emplois, de nombreuses compétences communes s'appliquent, selon le rôle, au niveau de base, intermédiaire ou avancé. Tous les professionnels de la cybersécurité, peu importe leur rôle, devraient avoir les connaissances de base nécessaires pour appliquer les éléments suivants dans leur domaine ou contexte de travail :

- systèmes de TI et réseautique;
- architecture de systèmes et modèles;
- protocoles Internet, systèmes et dispositifs;
- fondements de la cybersécurité;
  - cadre de sécurité intégrée;
  - stratégies et approches liées à la cybersécurité;
  - contexte des menaces et exposition aux menaces courantes (du personnel, physiques, informatiques ou logiques, chaîne d'approvisionnement);
  - processus et sources de renseignement sur les cybermenaces;
  - analyse de la cybersécurité;
  - politiques, processus et pratiques exemplaires en matière de gestion de la cybersécurité;
  - systèmes, outils et applications de cybersécurité;
  - règlementation et conformité (p. ex. respect de la vie privée, échange d'information, production de rapports, normes obligatoires, etc.);
  - normes nationales et de l'industrie;
- résolution de problème et réflexion complexe dans des environnements dynamiques;
- assurance d'une connaissance plus vaste de la situation en matière de sécurité;
- conscience de soi pour ce qui est des connaissances, compétences et aptitudes requises pour répondre aux changements organisationnels, techniques et liés aux menaces.

3.3 Rôles principaux liés à la cybersécurité

Reconnaissant que la cybersécurité est une responsabilité partagée, la présente publication décrit la profession de la cybersécurité en fonction du travail qui est généralement effectué à temps plein et qui exige des connaissances, compétences et aptitudes uniques par rapport aux autres professions. Par ailleurs, conformément au cadre canadien des compétences en matière de cybersécurité, on décrit également la profession de la cybersécurité en fonction des titres et des rôles de travail qui sont pertinents au marché du travail du Canada et au milieu élargi des affaires dans les quatre principaux secteurs d'activités ou catégories d'emplois en cybersécurité : Supervision et gouvernance, Conception et développement,

Exploitation et maintenance et Protection et défense. On retrouve une définition détaillée de ces secteurs d'activités, de ces catégories d'emplois et des rôles de travail connexes dans les annexes A, B, C et D.

Les rôles principaux liés à la cybersécurité sont divisés en grandes catégories et sous-groupes professionnels semblables à ceux établis dans le cadre de la NICE[4].

- **Supervision et gouvernance** – La principale responsabilité de ce sous-groupe professionnel est d'assurer la direction et la gestion du programme de cybersécurité. Il comprend des rôles techniques et non techniques.
- **Conception et développement (« Securely provision » dans la NICE) –** Ce sous-groupe professionnel soutient la conception et le développement de l'infrastructure numérique, des systèmes et des logiciels. Il comprend des rôles essentiellement techniques.
- **Exploitation et maintenance –** La principale responsabilité de ce sous-groupe professionnel est d'assurer une exploitation sécurisée des systèmes numériques et de la gestion des données. Tous les rôles compris dans ce sous-groupe sont de nature technique.
- **Protection et défense –** Ce sous-groupe professionnel est axé sur les opérations de cybersécurité. Tous les rôles compris dans ce sous-groupe professionnel sont de nature technique.

Compétences communes (fondements pour les personnes spécialisées dans la cybersécurité)

Pour tous les rôles principaux liés à la cybersécurité, peu importe le secteur d'activités ou la catégorie d'emplois, de nombreuses compétences communes s'appliquent, selon le rôle, au niveau de base, intermédiaire ou avancé (comme indiqué à la section 3.2). Tous les professionnels de la cybersécurité, peu importe leur rôle, devraient avoir les connaissances de base nécessaires pour appliquer les éléments suivants dans leur domaine ou contexte de travail :

- apprentissage continu soutenant le perfectionnement des connaissances liées aux menaces émergentes, aux innovations technologiques sur le plan de la sécurité et à un environnement de cybersécurité en constante évolution;
- communications (orales et verbales) adaptées au contexte de l'organisation, dont la rédaction de rapports techniques;
- réflexion stratégique et sens des affaires pour comprendre le contexte opérationnel et des risques liés à la cybersécurité;
- travail d'équipe et collaboration avec autrui, y compris des personnes non spécialisées dans la cybersécurité;
- respect de l'éthique et responsabilités professionnelles;
- formation et sensibilisation en matière de cybersécurité dans leur domaine.

[4] Il importe de mentionner que les catégories d'emplois « Enquête », « Analyse » et « Collecte et exploitation » ne sont que résumées dans le présent document, puisqu'elles sont définies entièrement dans le cadre de la NICE et qu'elles relèvent généralement de la responsabilité des professions de nature militaire et politique.

3.4 Rôles connexes à la cybersécurité

Plusieurs rôles sont également liés aux autres fonctions organisationnelles qui contribuent généralement aux résultats de l'organisation en matière de cybersécurité à temps partiel ou de façon opportune[5]. Il s'agit de rôles connexes à la cybersécurité qui exigent certaines connaissances, compétences et aptitudes en cybersécurité, mais qui ne sont généralement pas considérés comme étant occupés par des spécialiste de la cybersécurité[6]. Par exemple, dans certaines organisations, un ou une analyste des activités et des politiques s'occupera probablement d'un large éventail d'enjeux et seulement quelques-uns de ces enjeux concerneront la prise en charge de la cybersécurité organisationnelle. Il ne s'agit pas de nuire à son rôle de soutien à la cybersécurité organisationnelle, mais plutôt de suggérer que le travail accompli concerne souvent bien plus que la cybersécurité à proprement dit.

De même, les cadres supérieurs, les gestionnaires de programme, les analystes de politiques, les analystes financiers, les spécialistes des communications, les architectes d'entreprise, les techniciens et techniciennes informatiques, etc. peuvent assumer des responsabilités liées à la cybersécurité sans avoir à s'y consacrer à temps plein. Leurs rôles ne sont donc pas compris dans les rôles principaux liés à la cybersécurité abordés dans la présente publication. Ces rôles sont mentionnés à l'annexe E. Par exemple, un échantillonnage de rôles de travail types associés à la cybersécurité est fourni dans le tableau 1 ci-dessous. Bien qu'ils exercent des responsabilités en cybersécurité et doivent démontrer des connaissances, compétences et aptitudes particulières en matière de cybersécurité, leurs principales responsabilités sont souvent plus vastes ou axées sur d'autres activités non liées à la cybersécurité. Il importe de souligner que la catégorie Protection et défense n'est pas incluse dans la figure, puisque ce secteur d'activités ou cette catégorie d'emplois est utilisé exclusivement dans le domaine de la cybersécurité.

Tableau 1 : Échantillonnage des rôles de travail types associés à la cybersécurité

Supervision et gouvernance	Conception et développement	Exploitation et maintenance
Dirigeants principaux/dirigeantes principales de l'information ou techniciens/techniciennes en chef	Architectes d'entreprise	Gestionnaires de systèmes
Agents ou agentes de sécurité d'entreprise	Planificateurs ou planificatrices des exigences système	Gestionnaires des systèmes
Gestionnaires de programme	Analystes des activités	Analystes des systèmes

[5] Cela ne tient pas compte des « utilisateurs » qui assument des responsabilités liées à la cybersécurité peu importe leur rôle dans l'organisation.

[6] Dans le cas de certains rôles et de certaines professions, il peut s'agir de personnes qui sont employées à temps plein dans le domaine de la cybersécurité et sont considérées des spécialistes, comme celles employées dans un domaine du droit, du respect de la vie privée ou de l'éthique, qui touche à la cybersécurité. Comme elles exercent déjà une autre profession et ne font souvent pas partie de l'effectif de l'organisation, elles ne sont pas prises en compte dans ce cadre. Elles sont toutefois représentées dans le cadre de la NICE.

Supervision et gouvernance	Conception et développement	Exploitation et maintenance
Gestionnaires de projets de TI	Développeurs/développeuses de logiciels ou programmeurs/programmeuses	Administrateurs ou administratrices de bases de données
Analystes financiers	Analystes des systèmes de contrôle	Analystes de systèmes de données
Spécialistes de l'apprentissage et du perfectionnement (p. ex. sensibilisation et formation en matière de sécurité)	Développeurs ou développeuses Web	Spécialistes du soutien technique

4 Résumé du Cadre canadien des compétences en matière de cybersécurité et de ses attributs

Le Cadre des compétences en matière de cybersécurité du Canada (figure 1) aborde la sécurité organisationnelle sous l'angle du cadre de la NICE. Par conséquent, le cadre canadien met l'accent sur quatre des sept catégories d'emplois initiales qui représentent la majorité du travail en cybersécurité accompli dans les entreprises et les industries canadiennes. Chacune des catégories d'emplois correspond à un domaine de responsabilité en matière de cybersécurité et elles sont toutes interconnectées.

Tirant avantage des principaux éléments et des principales caractéristiques du cadre de la NICE, le Cadre des compétences en matière de cybersécurité du Canada permet de faire ce qui suit :

- aider à préciser les lacunes dans la main-d'œuvre du domaine de la cybersécurité qui existent sur le marché du travail canadien en approchant la question du point de vue des entreprises proposé dans le cadre de la NICE et en établissant une distinction entre les rôles de base en cybersécurité et les rôles organisationnels qui assument certaines responsabilités en cybersécurité ou les rôles connexes dans le domaine;
- simplifier la représentation du travail lié à la cybersécurité qui est commun à la plupart des organisations;
- adapter facilement le cadre de manière à soutenir les responsabilités plus vastes ou généralistes qui sont communes aux PMO, alors qu'elles s'efforcent de répondre aux exigences fondamentales en matière de TI et de cybersécurité;
- analyser les catégories d'emplois « Analyse », « Collecte et exploitation » et « Enquête » qui mettent l'accent sur la sécurité nationale et les rôles associés à l'application de la loi;
- utiliser des termes compris par toute la collectivité élargie des affaires et des TI, en particulier le terme « Conception et développement » plutôt que « Securely provision »;
- continuer de mettre l'accent sur les responsabilités en cybersécurité des rôles de travail dans les secteurs de la supervision et de la gouvernance, de la conception et du développement, et de l'exploitation et de la maintenance;
- reconnaître le rôle central que joue la catégorie « Protection et défense » dans les opérations de cybersécurité.

5 Conclusion

Le cadre de la NICE est une représentation exhaustive de la main-d'œuvre en cybersécurité qui reflète essentiellement la structure de la main-d'œuvre du gouvernement fédéral des États-Unis. À mesure que le cadre évolue et qu'il est adopté par les intervenants du secteur privé, la présente publication abordera certaines des préoccupations liées à son application directe au marché du travail canadien.

Le Cadre canadien des compétences en matière de cybersécurité présenté dans ce document est une présentation simplifiée du travail réalisé en cybersécurité dans la majorité des organisations du secteur privé et les plus petits organismes du secteur public. Il traite plus précisément des lacunes qui existent au sein des entreprises et de l'industrie. Ce cadre aborde la sécurité sous un angle organisationnel plutôt que du point de vue de la sécurité nationale afin de mieux interpréter le travail en cybersécurité des entreprises et de l'industrie. Il permet également aux entreprises d'établir un lien avec l'information exhaustive et détaillée comprise dans le cadre de la NICE.

Dans l'ensemble, il devrait aider à mieux guider les intervenantes et les intervenants en développement de la main-d'œuvre pour combler le déficit de compétences en cybersécurité.

6 Contenu complémentaire

6.1 Liste des acronymes, des abréviations et des sigles

Terme	Définition
ATC	Alliance des talents en cybersécurité
Cadre de la NICE	Cadre de perfectionnement de la main-d'œuvre dans le domaine de la cybersécurité de la NICE
CNP	Classification nationale des professions
DG	Directeur général ou directrice générale
DPF	Dirigeant principal ou dirigeante principale des finances
DPI	Dirigeant principal ou dirigeante principale de l'information
IA	Intelligence artificielle
NIST	National Institute of Standards and Technology
NPN	Normes professionnelles nationales
PMO	Petites et moyennes organisations
SCADA	Télésurveillance et acquisition de données (*Supervisory Control and Data Acquisition*)
SCI	Systèmes de contrôle industriels
TI	Technologies de l'information

6.2 Glossaire

Pour une description détaillée des catégories de la NICE, les domaines spécialisés et les rôles de travail, prière de consulter le cadre de la NICE.

Terme	Définition
Auteur de cybermenace	Les auteurs de cybermenace sont des États, des groupes ou des personnes qui cherchent à profiter des vulnérabilités, d'une sensibilisation insuffisante à la cybersécurité et des progrès technologiques pour obtenir un accès non autorisé aux systèmes d'information ou encore porter préjudice aux données, aux dispositifs, aux systèmes et aux réseaux des victimes. L'universalisation d'Internet a fait en sorte que ces auteurs de menace peuvent compromettre, peu importe où ils se trouvent dans le monde, la sécurité des systèmes d'information au Canada.
Capacité	Une capacité permet d'adopter un comportement observable ou un comportement qui résulte d'un produit observable.
Catégories	En ce qui a trait à la NICE, les catégories fournissent la structure organisationnelle globale du cadre de la NICE. On retrouve sept catégories composées de domaines spécialisés et de rôles de travail.
Centre des opérations de sécurité (COS)	Un COS fournit des services opérationnels et d'autres services de sécurité au ministère, notamment la protection des personnes, de la propriété, des biens et de l'information. Le COS contient normalement les installations dans lesquelles les utilisateurs du système peuvent surveiller, afficher et gérer l'information (applications, vidéos et systèmes d'alarme), puis effectuer la répartition et répondre aux incidents. La conception et l'élaboration d'un

Terme	Définition
	COS devraient déterminer toutes les pièces destinées à accueillir le personnel, l'équipement et les fournitures associés aux activités de contrôle, d'alarme et de surveillance.
Code source libre	Code source que l'on rend disponible gratuitement pour qu'il puisse être modifié et redistribué, dans un contexte de développement communautaire. Ce terme s'applique également à tous les produits offerts gratuitement en ligne qui sont présentés au public comme pouvant être reproduits et distribués sans restriction.
Compétence	Capacité d'appliquer ou d'utiliser des connaissances, des compétences, des aptitudes, des comportements et des caractéristiques personnelles de manière à accomplir des tâches essentielles et des fonctions particulières ou à assumer un rôle ou un poste donné.
Connaissance	La connaissance est un corpus d'information que l'on applique directement à l'exercice d'une fonction.
Cybermenace	Une cybermenace est une activité qui vise à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient.
Cyberopérations actives (ou cyberopérations offensives)	Aux États-Unis, il s'agit de cyberopérations visant à démontrer sa puissance en faisant acte de force dans le cyberespace. Au Canada, les cyberopérations actives sont régies par le projet de loi C-59 et menées, en vertu d'un mandat, par le Centre de la sécurité des télécommunications, qui est l'autorité ministérielle responsable de la conduite des activités visant à réduire, à interrompre, à influencer ou à contrecarrer les capacités, les intentions ou les activités de toute personne ou de tout État, organisme ou groupe terroriste étrangers, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité.
Cybersécurité	La cybersécurité est la protection des données numériques et de l'infrastructure où elles sont stockées.
Domaine de spécialisation	Le cadre de la NICE se divise en 32 domaines de spécialisation. Chacun d'entre eux représente un domaine de travail intensif ou une fonction associée à la cybersécurité ou à un emploi connexe.
Effectif	Ensemble des personnes au service d'une entreprise ou d'un organisme; ensemble des salariés travaillant dans un secteur donné et, par extension, affectés à une catégorie d'activités.
Habilité	Souvent définie comme l'ensemble de savoir-faire qui permettent à une personne de maîtriser une activité et de réussir dans l'accomplissement d'une tâche. Du point de vue psychomoteur, les habilités sont la capacité de manipuler physiquement un outil ou un instrument, comme un marteau. Les habiletés nécessaires en cybersécurité relèvent moins d'une manipulation physique d'outils et d'instruments que de l'utilisation d'outils, de cadres, de processus et de contrôles susceptibles d'avoir une incidence sur la posture de cybersécurité d'une organisation ou d'une personne.
Marché du travail	Le terme marché du travail est un concept généralisé qui désigne l'interaction entre l'offre (nombre de personnes disponibles pour travailler) et la demande (nombre d'emplois disponibles)
National Institute for Standards and Technology (NIST)	Faisant partie du Département du commerce des États-Unis, l'agence NIST américaine est l'organisme fédéral de normalisation dont la mission est de promouvoir l'innovation et la compétitivité industrielle aux États-Unis en faisant progresser la science, les normes et la technologie des mesures de manière à renforcer la sécurité économique et à améliorer notre qualité de vie.
Petites et moyennes organisations (PMO)	Organisations qui comptent moins de 499 employés.
Rôle de travail	Dans le cadre de la NICE, les rôles de travail représentent les groupes les plus détaillés de la cybersécurité et du travail connexe. Ils comprennent une liste des attributs nécessaires pour assumer ce rôle, notamment les connaissances, compétences et aptitudes et les tâches effectuées.

6.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité, Évaluation des cybermenaces nationales 2020, novembre 2020.
2	National Institute of Standards and Technology, NIST Special Publication 800-181, NICE Cybersecurity Workforce Framework, août 2017 (en anglais seulement).
3	National Institute of Standards and Technology, NIST Special Publication 800-181 Revision 2, Workforce Framework for Cybersecurity (NICE Framework), novembre 2020 (en anglais seulement).