Bâtir un **Canada sécuritaire** et **résilient**

Stratégie nationale de cybersécurité du Canada

Sécuriser l'avenir numérique du Canada

Sécurité publique Canada | Public Safety Canada

Canada

Lire cette publication en ligne à l’adresse suivante :
https://securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-fr.aspx

La nouvelle stratégie nationale de cybersécurité du Canada présente le plan à long terme du gouvernement du Canada qui vise à établir des partenariats avec les provinces, les territoires, l’industrie, les communautés autochtones et le milieu universitaire pour faire du Canada l’endroit le plus sûr où vivre et travailler en ligne.

Also available in English under the title: Canada’s National Cyber Security Strategy

Sécurité publique Canada, Communications
269 Laurier Ave, Ottawa, Canada K1A 0P8
communications@ps-sp.gc.ca

https://www.securitepublique.gc.ca

Date de publication : 2025-01
Numéro de catalogue : PS4-239/2025F-PDF
ISBN: 978-0-660-72268-9

Table des matières

Message du ministre de la Sécurité publique

L'honorable David J. McGuinty
Ministre de la Sécurité publique

Les progrès technologiques continuent d'évoluer à un rythme sans précédent. Alors que de plus en plus de Canadiens et Canadiennes vivent et travaillent en ligne et que les entreprises et l'industrie se tournent vers les services numériques, les cybermenaces ne cessent d'augmenter. Ceci entraîne des répercussions réelles pour les Canadiens et Canadiennes et devient une menace majeure pour la sécurité nationale et l'économie du pays.

La nouvelle stratégie nationale de cybersécurité du Canada présente notre plan à long terme pour relever ces défis, en partenariat avec les provinces, les territoires, les communautés autochtones, l'industrie et le monde universitaire pour sécuriser l'avenir numérique du Canada.

Nous avons récemment investi, en nous appuyant sur des mécanismes bien établis, pour répondre aux incidents de cyberactivité malveillante visant les systèmes du gouvernement du Canada. Nous continuerons à utiliser tous les outils disponibles afin de protéger les infrastructures essentielles du Canada, de mieux nous adapter aux cyberrisques et de mieux les combattre, de garantir la sécurité et l'intégrité des systèmes essentiels du Canada et de créer un mécanisme pour faire appliquer notre déclaration 2022 sur la sécurité des télécommunications.

Cependant, il reste encore beaucoup à faire. Cette nouvelle stratégie nationale de cybersécurité nous permettra de faire avancer ce travail important.

Nous devons travailler ensemble pour protéger les Canadiens et les entreprises du Canada et pour éviter que les infrastructures critiques ne perturbent les services dont nos concitoyens dépendent chaque jour.

Ensemble, nous veillerons à ce que le cyberespace soit sûr, ouvert et sécurisé pour tous les Canadiens et Canadiennes.

Introduction

La sécurité et la prospérité du Canada en ligne reposent sur une cybersécurité solide.

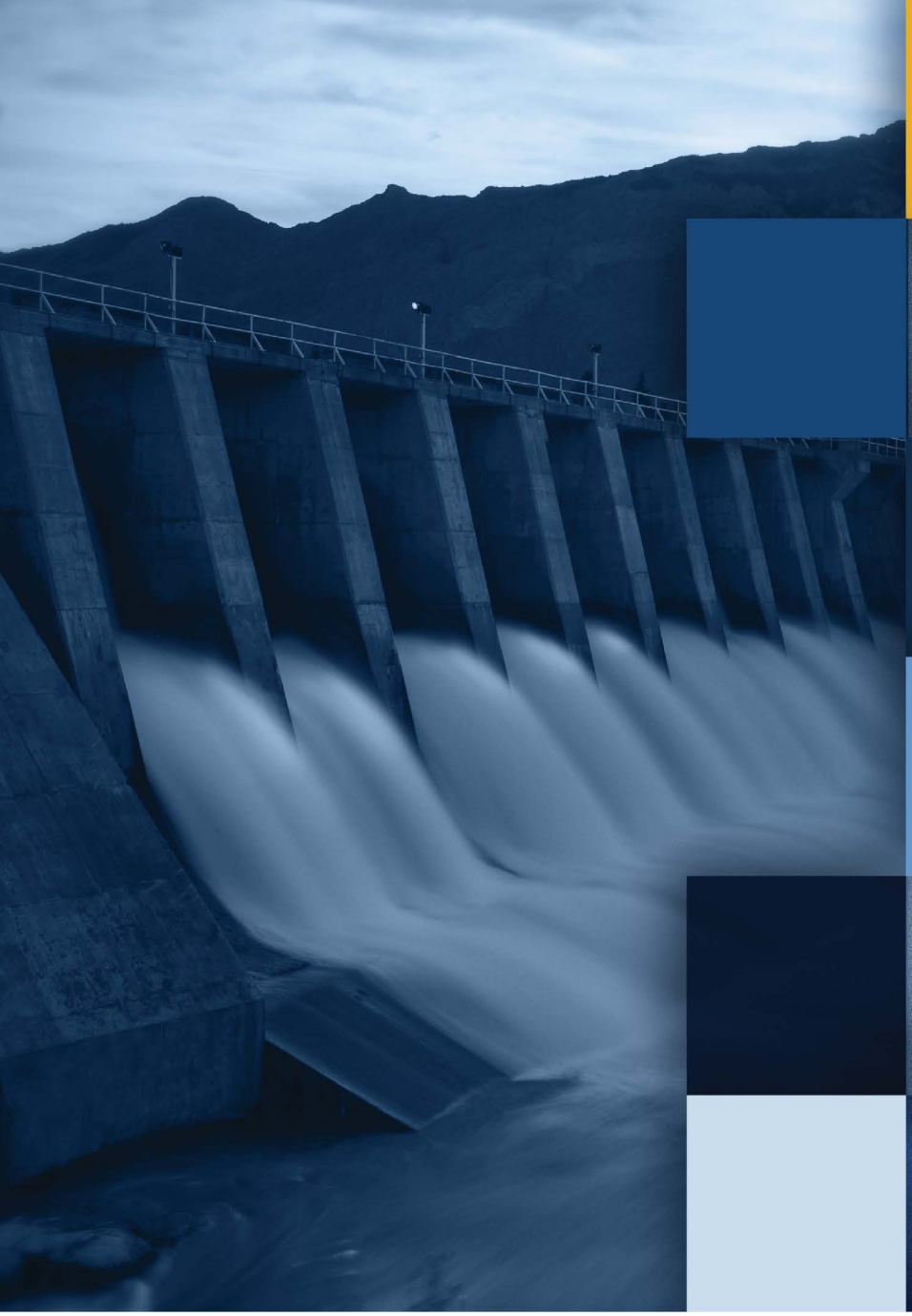
Les progrès des technologies numériques ont enrichi nos vies et ont apporté d'énormes bénéfices à la société. Malheureusement, les mêmes innovations qui nous ont apporté tant d'avantages nous ont aussi exposés à des risques qui menacent non seulement nos infrastructures numériques, mais aussi les services essentiels sur lesquels nous comptons.

Aujourd'hui, il est tout à fait évident que pour faire progresser en toute sécurité l'économie numérique et propre du Canada, pour protéger notre démocratie et nos moyens de subsistance quotidiens, et pour assurer notre prospérité économique de demain, la cybersécurité doit être un élément fondamental de la sécurité nationale, de la sécurité économique et de la sécurité publique du pays.

La Stratégie nationale de cybersécurité 2018[1] du Canada a permis de mettre sur pied le Centre canadien pour la cybersécurité[2] (Centre pour la cybersécurité), établi au sein du Centre de la sécurité des télécommunications[3] (CST), et le Centre national de coordination contre la cybercriminalité[4] (CNC3), qui relève de la Gendarmerie royale du Canada[5] (GRC). Ces changements fondamentaux ont permis aux Canadiens de bénéficier un soutien consolidé pour réagir aux cyberincidents et enquêter sur la cybercriminalité.

Malgré ces gains, les cybermenaces auxquelles le Canada est confronté continuent d'évoluer et de prendre de l'ampleur. Le Canada doit en faire plus.

1 https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/ntnl-cbr-scrt-strtg-fr.pdf
2 https://www.cyber.gc.ca/fr
3 https://www.cse-cst.gc.ca/fr
4 https://rcmp.ca/fr/police-federale/cybercriminalite/centre-national-coordination-en-cybercriminalite
5 https://www.rcmp-grc.gc.ca/fr



Le défi : les cybermenaces qui touchent les Canadiens évoluent constamment

Les Canadiens font face à des cybermenaces persistantes, sophistiquées et quotidiennes.

Depuis 2018, nous avons connu d'énormes changements. La pandémie a accéléré la mise en ligne de presque tous les aspects de la vie des Canadiens, et, par conséquent, nos infrastructures essentielles deviennent de plus en plus interconnectées. Les auteurs de cybermenaces parrainés par des États et les cybercriminels orgaisés n'ont pas tardé à tirer parti de ces nouvelles possibilités et de notre dépendance accrue à l'égard des services en ligne.

Les Canadiens continuent d'être affectés par cette augmentation des cybermenaces et ils paient un lourd tribut. Les cyber acteurs mailveillants impactent négativement les services essentiels, dont les soins de santé et l'éducation. Ils volent aussi les renseignements personnels et la propriété intellectuelle des Canadiens. Les revenues qui devraient stimuler l'économie canadienne disparaissent entre les mains des criminels. Les coûts financiers et réputationnels qui résultent des brèches cybernétiques sont ressentis par les petites, moyennes et des grandes entreprises, ainsi que tous les ordres de gouvernement. Malheureusement, de nombreuses organisations n'ont pas les ressources nécessaires pour se défendre contre les menaces sophistiquées.

En outre, ces dernières années, nous avons vu des auteurs de cybermenaces parrainés par des États de plus en plus audacieux et sophistiqués mener des interventions militaires et faire de l'ingérence étrangère en ligne. Le Canada a été ciblé pour son adhésion à l'Organisation du Traité de l'Atlantique Nord[6] (OTAN) et pour son soutien à l'Ukraine.

Pour faire face à ces cybermenaces et réduire le niveau de risque encouru par les Canadiens et les entreprises canadiennes, le Canada doit être prêt à s'adapter continuellement et à favoriser et exploiter toutes ses capacités collectives.

6 https://www.nato.int/

Relever le défi : une nouvelle approche de cybersécurité nationale qui mobilise tous les Canadiens

Deux principes fondamentaux serviront à orienter l'approche du Canada en matière de cybersécurité :

1. **Mobilisation pansociétale :** Tous les Canadiens ont un rôle à jouer dans l'amélioration de la cyberrésilience nationale du Canada. Le gouvernement du Canada approfondira ses partenariats avec des parties prenantes clés afin de s'attaquer aux principaux enjeux du secteur de la cybersécurité. Les partenariats avec d'autres ordres de gouvernement, les communautés autochtones, le secteur privé, le milieu universitaire et la société civile seront essentiels à l'élaboration de solutions qui permettront de relever les défis de la cybersécurité de demain. Les Canadiens joueront également un rôle important en tant que citoyens numériques et propriétaires d'entreprises. L'amélioration de la sensibilisation du public et du savoir-faire en matière de cybersécurité pour tous aidera à faire en sorte que les Canadiens soient mieux informés des cybermenaces auxquelles ils font face et qu'ils soient plus résilients contre les auteurs de cybermenaces malveillantes.

2. **Leadership agile :** Étant donné que les menaces et les possibilités dans le cyberespace continuent d'évoluer à un rythme rapide à l'échelle mondiale, il est essentiel que le Canada soit outillé pour réagir aux risques émergents au fur et à mesure qu'ils se présentent. Par conséquent, plutôt qu'un plan statique unique, les solutions du Canada en matière de cybersécurité seront élaborées en étroite collaboration avec les partenaires et les parties prenantes, et seront présentées dans une série de plans d'action portant chacun sur un enjeu spécifique au cours des prochaines années. Ces plans d'action présenteront des initiatives pour le Canada et sa population et énonceront des résultats clairs et un engagement à rendre compte des résultats obtenus. Ils seront collaboratifs et holistiques et permettront au Canada d'être au premier plan d'approches novatrices en matière de risques et de possibilités liés à la cybersécurité. Ainsi, nos solutions demeureront pertinentes et efficaces au fur et à mesure que les menaces évoluent.

La Stratégie nationale de cybersécurité mettra l'accent sur l'utilisation de cette approche pour obtenir des résultats dans le cadre de trois piliers :

Pilier 1 : Collaborer avec les partenaires pour protéger les Canadiens et les entreprises canadiennes contre les cybermenaces

Le Canada :

- établira des partenariats pansociétaux
- défendra ses intérêts et ses valeurs sur le plan international et plaidera en leur faveur
- fera progresser la cybersensibilisation et la cyberhygiène à l'échelle nationale

Pilier 2: Faire du Canada un chef de file mondial de l'industrie de la cybersécurité

Le Canada :

- se fera un innovateur de confiance qui donne la priorité à la cybersécurité
- accroîtra la main d'œuvre essentielle de l'avenir
- recensera et soutiendra des domaines de recherche ciblés pour répondre aux besoins canadiens

Pilier 3 : Détecter et perturber les auteurs de cybermenaces

Le Canada :

- cernera et dissuadera les cybermenaces et se défendra contre celles-ci
- améliorera les capacités de lutte contre la cybercriminalité
- rendra les systèmes essentiels plus résilients

Pilier 1 : **Collaborer avec des partenaires pour protéger les Canadiens et les entreprises Canadiennes contre les cybermenaces**

Aucune institution, aucun segment de la société ne peuvent à eux seuls relever les défis posés par les cybermenaces. Le gouvernement du Canada a réussi à établir des partenariats avec l'industrie et d'autres ordres de gouvernement pour échanger de l'information, réagir à des cyberincidents et lancer les cybercapacités canadiennes. Il approfondira ces liens et en fera plus.

Le gouvernement du Canada dirigera un niveau sans précédent de partenariats public-privé sur les questions de cybersécurité afin de mieux tirer parti de l'expertise et des capacités des intervenants.

Nous élaborerons des plans d'action pour identifier et éliminer les obstacles à la collaboration entre le gouvernement et d'autres segments de la société, y compris les partenaires internationaux. Nous établirons des partenariats pour tirer parti de notre capacité collective à réagir aux cybermenaces, et nous guiderons notre engagement international à promouvoir un comportement fondé sur des normes dans le cyberespace.

Objectif 1.1 : Établir des partenariats pansociétaux

Un leadership national est la clé d'une approche unifiée, holistique et stratégique de la cybersécurité.

Le gouvernement du Canada ne devrait pas élaborer seul ces plans d'action en matière de cybersécurité. Le gouvernement du Canada mettra le thème de la cybersécurité à l'avant-plan des engagements auprès des provinces et des territoires et des communautés autochtones afin de mieux représenter les besoins en cybersécurité. Par exemple, les infrastructures essentielles du Canada, qui appartiennent principalement au secteur privé, sont réparties dans un pays vaste, mais inégalement peuplé. Les collectivités de petite taille et éloignées, y compris les populations du Nord et les communautés autochtones, doivent être protégées dans la même mesure que celles des grands centres urbains.

Dans le cadre de l'évolution du gouvernement du Canada vers un partenariat avec l'ensemble de la société, Sécurité publique Canada[7] (SP) et le Centre canadien pour la cybersécurité[8] (Centre pour la cybersécurité) mettront sur pied le **Collectif canadien pour la cyberdéfense (CCCD)**. Le CCCD servira d'organisme national de mobilisation multipartite pour faire progresser la résilience du Canada en matière de cybersécurité grâce à un partenariat public-privé direct concernant les défis nationaux, les priorités stratégiques et efforts de défense en matière de cybersécurité. Le gouvernement

7 https://www.securitepublique.gc.ca/index-fr.aspx
8 https://www.cyber.gc.ca/fr

du Canada s'appuiera activement sur le CCCD pour faire participer régulièrement les intervenants à l'élaboration de plans d'action de sorte que les connaissances et les expériences les plus récentes éclairent les futures mesures de politiques et de programmes.

Comme première étape de son engagement à créer des partenariats avec le milieu universitaire, le gouvernement du Canada a financé un Centre de données de cyber attribution (CDCA) à l'Institut canadien sur la cybersécurité[9] (ICC) de l'Université du Nouveau-Brunswick[10] (UNB). Le CDCA, dont le but ultime est de repérer les activités de cybermenaces malveillantes, effectuera les plus récentes analyses en lignes des données recueilles à partir de diverses sources. Le CDCA formera et outillera également la prochaine génération de spécialistes en cybersécurité liée à intelligence artificielle (IA). Dans l'ensemble, le CDCA comblera une lacune évidente en matière de formation et d'effectif dans l'environnement de cybersécurité qui ne cesse d'évoluer. À long terme, il améliora la capacité du Canada à collaborer et à innover afin de protéger la population et les entreprises canadiennes contre les cybermenaces.

Objectif 1.2 : Défendre les intérêts et les valeurs du Canada sur le plan international et plaider en leur faveur

La cybersécurité nationale du Canada existe dans un contexte mondial.

> Le gouvernement du Canada a publié une Déclaration sur le droit international applicable dans le cyberespace[11] afin de contribuer au dialogue international sur la façon dont le droit international s'applique dans le cyberespace. Le Canada continue de faire progresser la mise en œuvre du Cadre des Nations Unies pour un comportement responsable des États dans le cyberespace[12] [lien disponible seulement en anglais] en favorisant une meilleure compréhension et le respect de ses normes de comportement responsable des États.

9 https://www.unb.ca/cic/
10 https://www.unb.ca/
11 https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=fra
12 https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

Puisque les cybermenaces ne respectent pas les frontières, le Canada doit continuer de travailler avec ses alliés pour défendre ses intérêts nationaux et promouvoir la sécurité mondiale. Le Canada continuera de jouer un rôle important en réunissant des partenaires internationaux aux vues similaires pour défendre le droit international, les comportements fondés sur des normes, et les normes internationales dans le cyberespace. Le Canada approfondira également ses partenariats internationaux afin de dissuader les cyberactivités malveillantes et d'y répondre. Le Canada continuera de promouvoir sa vision d'un Internet ouvert, libre, sûr et fiable, à dénoncer les comportements inacceptables et à étudier le rôle que les régimes de sanctions et d'inscription peuvent jouer dans la dissuasion les cybermenaces. À l'appui de ces mesures, Affaires mondiales Canada[13] (AMC) a créé un nouveau poste de coordonner l'engagement international au sein du gouvernement et de représenter le Canada à l'étranger. Il s'agit du poste de haut fonctionnaire pour le cyberspace, le numérique et les technologies émergentes.

Le gouvernement du Canada soutiendra également les efforts de renforcement des capacités d'autres pays visant à détecter et à contrer les cybermenaces, notamment par une plus grande coopération dans la région indopacifique.

Objectif 1.3 : Faire progresser la cybersensibilisation et la cyberhygiène à l'échelle national

La cybersécurité nationale dépend de la sensibilisation des Canadiens à la cybersécurité pour réduire le nombre de victimes.

> Le programme « Pensez cybersécurité »[14] offre aux Canadiens un accès gratuit aux conseils et à l'éducation de base en matière de cyberhygiène. Le Centre antifraude du Canada[15] (CAFC), le Bureau de la concurrence et l'Agence du revenu du Canada coordonnent les efforts de sensibilisation à la fraude.

13 https://www.international.gc.ca/global-affairs-affaires-mondiales/home-accueil.aspx?lang=fra
14 https://www.pensezcybersecurite.gc.ca/fr
15 https://antifraudcentre-centreantifraude.ca/index-fra.htm

Le gouvernement du Canada s'efforcera de rendre la cybersécurité plus accessible à tous les Canadiens. L'amélioration de la cyberhygiène collective et de la sensibilisation assure la sécurité et la sûreté d'un plus grand nombre de Canadiens et réduit le risque que des Canadiens soient victimes de cybercrimes. Les questions de cybersécurité doivent s'inscrire dans les activités quotidiennes des entreprises canadiennes et dans l'innovation canadienne, en particulier dans des secteurs d'importance nationale comme la santé, l'énergie et la technologie verte.

De plus, le gouvernement du Canada s'appuiera sur la réussite du programme « Pensez cybersécurité »[16] et du Centre antifraude du Canada[17] (CAFC) et continuera de tirer profit de l'expertise du Centre canadien pour la cybersécurité[18] (Centre pour la cybersécurité) comme l'intelligence artificielle, les menaces posées par les modèles de langage de grand taille, et la façon de repérer les cas de mésinformation, désinformation et malinformation (MDM) afin de renforcer la collaboration avec les Canadiens. À mesure que les technologies numériques progressent, leurs capacités sont exploitées de nouvelles façons pour des intentions malveillantes. À l'avenir, le gouvernement du Canada continuera de soutenir les campagnes de sensibilisation à la cybersécurité afin d'améliorer la cyberhygiène du Canada partout au pays et de renforcer la cyberrésilience du Canada.

16 https://www.pensezcybersecurite.gc.ca/fr
17 https://antifraudcentre-centreantifraude.ca/index-fra.htm
18 https://www.cyber.gc.ca/fr

Pilier 2 : **Faire du Canada un chef de file mondiale de l’industrie de la cybersécurité**

Le Canada est un innovateur. Nous nous appuierons sur l'industrie de la cybersécurité déjà solide pour faire du Canada un chef de file mondial dans le domaine de la cybertechnologie innovatrice. Pour contribuer à établir les conditions de la réussite, le gouvernement du Canada soutiendra toute la gamme de la recherche et du développement, de la recherche fondamentale au lancement de produits.

Il y a une pénurie mondiale de professionnels de la cybersécurité. Le Canada ne fait pas exception. Nous prendrons des mesures pour former et accroître les talents en cybersécurité au Canada. En même temps, nous pouvons prendre des mesures dès maintenant pour utiliser la technologie, comme l'intelligence artificielle (IA) et l'automatisation, afin de mieux répondre aux menaces auxquelles nous sommes confrontés aujourd'hui.

Voici quelques initiatives en cours :

- La Charte canadienne du numérique[19] définit la manière dont le gouvernement du Canada veille à ce que les Canadiens puissent se fier à l'intégrité et à la sécurité des services qu'ils utilisent en ligne et des informations les concernant détenues par le secteur privé.
- Le Réseau d'innovation pour la cybersécurité[20] soutient la croissance de l'écosystème de cybersécurité du Canada grâce à une collaboration entre les universités, le secteur privé, les secteurs sans but lucratif et d'autres ordres de gouvernement. Il finance des projets à fort impact pour améliorer la recherche et le développement, commercialiser des produits et des services et développer des talents en cybersécurité.
- La nouvelle Corporation d'innovation du Canada[21] soutient le développement et la protection de la nouvelle propriété intellectuelle dans le secteur de la défense, ce qui donne lieu à une cybertechnologie canadienne nouvelle, innovatrice et sûre.
- La grappe des technologies numériques du Canada[22] accélère le développement et l'adoption des cybertechnologies.
- Le Centre de recherche en technologies numériques[23] collabore avec l'industrie pour étudier les menaces qui pèsent sur les chaînes d'approvisionnement, le transport, l'énergie et d'autres infrastructures.

19 https://ised-isde.canada.ca/site/innover-meilleur-canada/fr/charte-canadienne-numerique-confiance-dans-monde-numerique
20 https://ised-isde.canada.ca/site/reseau-innovation-cybersecurite/fr
21 https://www.canada.ca/fr/ministere-finances/services/publications/corporation-innovation-canada-plan-directeur.html
22 https://ised-isde.canada.ca/site/grappes-dinnovation-mondiales/fr/grappe-technologies-numeriques-canada
23 https://nrc.canada.ca/fr/recherche-developpement/produits-services/services-techniques-consultatifs/cybersecurite

- Solutions innovatrices Canada[24] aide les petites et moyennes entreprises (PME) à commercialiser leurs innovations.
- L'Incitatif à l'investissement accéléré[25] permet aux PME de bénéficier d'incitations fiscales pour les investissements en immobilisations, y compris ceux liés à la cybersécurité.
- Soutien en approvisionnement Canada[26] s'efforce de simplifier le processus d'approvisionnement pour les petites entreprises. Le programme veut réduire les obstacles et offrir aux entreprises canadiennes un accès privilégié aux occasions de marchés du gouvernement. Ainsi, il aidera à faire mûrir et à développer les entreprises canadiennes de cybersécurité.

Pour protéger notre industrie, notre recherche innovante et nos moyens de subsistance, nous devons faire de la cybersécurité une priorité. En résumé, les Canadiens doivent avoir accès à des produits sûrs par défaut. Bien que le Canada ait fait d'importants progrès pour renforcer la cybersécurité, le nombre d'incidents qui se produisent chaque année au Canada continue de croître.

En réaction, le gouvernement du Canada se penchera sur des lois, des règlements et des mesures incitatives pour favoriser l'adoption de technologies et de pratiques sûres. Il s'associera à tous les ordres de gouvernement, à l'industrie et au milieu universitaire pour renforcer la cybersécurité de pointe dans son industrie, ses pratiques commerciales quotidiennes et ses produits et services.

Notre législation et nos actions doivent être bien éclairées. Nous investirons dans la recherche afin de développer une compréhension approfondie des aspects économiques de la cybercriminalité et de la cybersécurité, afin d'encourager plus efficacement l'adoption de technologies sûres et de lutter contre les auteurs de cybermenaces.

24 https://ised-isde.canada.ca/site/solutions-innovatrices-canada/fr/propos-nous
25 https://www.canada.ca/fr/agence-revenu/services/impot/entreprises/sujets/entreprise-individuelle-societe-personnes/declarer-vos-revenus-depenses-entreprise/reclamer-deduction-amortissement/incitatif-investissement-accelere.html
26 https://www.canada.ca/fr/services-publics-approvisionnement/services/achats/soutien-aux-entreprises.html

Objectif 2.1 : Faire du Canada un innovateur de confiance qui donne la priorité à la cybersécurité

Promouvoir des produits sécurisés dès la conception et l'adoption de technologies sûres.

Nous partageons tous la responsabilité d'utiliser et de mettre en œuvre des produits et des pratiques sûrs; ce fardeau ne peut pas être imposé uniquement aux citoyens à titre individuel. Les entreprises canadiennes de toutes tailles doivent adopter un virage culturel qui donne la priorité aux produits sécurisés dès la conception et une mentalité « le premier à sécuriser » plutôt qu'être seulement « le premier à commercialiser ». Il s'agit du seul moyen pour renforcer la sécurité de l'écosystème numérique.

Le gouvernement du Canada, en collaboration avec l'industrie, élaborera une stratégie visant à faciliter le passage vers une cyberresponsabilité partagée à l'échelle de l'ensemble de la société. Dans un premier temps, le gouvernement du Canada étudiera les moyens d'inciter les organisations à mettre la sécurité des consommateurs au cœur de leurs activités. Le gouvernement du Canada envisagera également des certifications en matière de cybersécurité et la désignation d'entreprises de confiance ayant le statut de contractant privilégié du gouvernement du Canada.

De plus, le gouvernement du Canada étudiera la possibilité d'étiqueter l'Internet des objets (IdO) afin d'aider les Canadiens à identifier et à comparer facilement les protections de cybersécurité intégrées dans les produits. Cela aidera les consommateurs, tout en rendant les cyberproduits nationaux plus attrayants. Le gouvernement du Canada travaillera également avec des partenaires internationaux pour coordonner les efforts d'étiquetage et obtenir une reconnaissance réciproque des normes canadiennes.

Le gouvernement du Canada continuera de collaborer avec les entreprises qui fournissent des services essentiels pour améliorer leur cybersécurité. Notamment, le gouvernement du Canada a annoncé le Programme canadien de certification en matière de cybersécurité[27] afin de rehausser la cybersécurité dans le secteur de la défense. Ce programme permettra de s'assurer que les entreprises qui soumissionnent pour certains marchés de défense du gouvernement du Canada maintiennent un niveau élevé de cybersécurité. Le gouvernement du Canada collabore avec les États-Unis pour assurer que la certification est compatible avec le Cybersecurity Maturity Model Certification (CMMC) des États-Unis, allégeant la charge sur l'industrie canadienne lorsqu'elle soumissionne pour des contrats de défense américains. Le gouvernement du Canada envisagera d'étendre ce programme au-delà du secteur de la défense.

27 https://www.canada.ca/fr/services-publics-approvisionnement/nouvelles/2023/05/le-gouvernement-du-canada-aide-lindustrie-de-la-defense-a-se-proteger-contre-les-menaces-a-la-cybersecurite.html

Le gouvernement du Canada renforce également la réglementation canadienne sur la protection des renseignements personnels dans le secteur privé et établit de nouvelles lignes directrices pour un développement et un déploiement responsables de l'intelligence artificielle (IA). Le gouvernement du Canada s'efforce de moderniser le cadre de protection des renseignements personnels dans le secteur privé sous responsabilité fédérale et d'améliorer la gouvernance de la conception, de la création et de l'utilisation de l'IA. Le gouvernement du Canada continue également de mettre à jour ses guides et directives fédéraux sur l'IA[28]. Il doit veiller à ce que les systèmes d'IA soient élaborés de façon sécuritaire et conformément aux valeurs canadiennes, ce qui permettra aux Canadiens d'avoir confiance dans les technologies numériques avec lesquelles ils interagissent quotidiennement. Le gouvernement du Canada continuera d'intervenir face aux technologies émergentes, y compris l'IA, afin d'assurer une adoption responsable et sûre au Canada.

Objectif 2.2 : Accroître la main-d'œuvre essentielle de l'avenir

Le développement de talents en cybersécurité, l'attraction, le maintien en poste et la formation sont essentiels à la réussite sur le plan national.

> Déjà, l'Initiative de perfectionnement des compétences pour l'industrie[29] permet aux employeurs de déterminer les besoins en compétences dans des secteurs en croissance rapide. En encourageant la collaboration entre les employeurs et les fournisseurs de formation, le programme contribue à offrir des programmes de perfectionnement adaptés aux besoins des employeurs, en particulier dans les industries à forte croissance. L'initiative devrait aider plus de 15 000 Canadiens, y compris des personnes de milieux sous-représentés, à accéder à de nouvelles possibilités d'emploi.

La demande pour des professionnels de la cybersécurité est en forte hausse, et il y a une pénurie de compétences en cybersécurité dans le monde entier. En conséquence, le développement et le maintien en poste des cybertalents sont essentiels pour les entreprises canadiennes et le gouvernement du Canada. Le Canada dispose déjà d'une main-d'œuvre hautement qualifiée en cybersécurité, mais, en faisant d'autres investissements, nous pouvons faire en sorte que les entreprises canadiennes ont accès au personnel dont elles ont besoin pour continuer à croître et à innover.

---

28 https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/innovations-gouvernementales-numeriques/utilisation-responsable-ai.html

29 https://ised-isde.canada.ca/site/initiative-perfectionnement-competences-industrie/fr

L'investissement dans les talents de la cybersécurité s'aligne sur l'évolution des exigences de la main-d'œuvre et favorise une main-d'œuvre plus diversifiée et plus adaptable, capable de naviguer les transitions de l'industrie.

Le gouvernement du Canada collaborera avec des partenaires d'autres ordres de gouvernement, du milieu universitaire et du secteur privé pour créer un bassin de compétences spécialisées et diversifiées en cybersécurité. Il s'agira notamment d'améliorer les possibilités de formation et d'élargir les programmes de stages et de formation dans le secteur privé. Ces programmes aideront à la fois les jeunes qui cherchent à faire carrière en cybersécurité et les travailleurs en milieu de carrière qui cherchent à relever leurs compétences et à se perfectionner. En outre, le Gouvernement du Canada étudiera l'appui aux programmes visant à assurer la participation des groupes sous-représentés.

De plus, dans le cadre du **Programme de coopération en matière de cybersécurité**[30] **(PCCS)**, Sécurité publique Canada[31] (SP) octroiera des subventions et des contributions à une série d'initiatives visant à réduire la cybercriminalité contre les Canadiens, à renforcer la capacité du Canada à protéger ses infrastructures essentielles, à sensibiliser davantage les Canadiens à la cybersécurité, à accroître leurs compétences en la matière et à améliorer la compétitivité du Canada dans l'économie mondiale.

Le gouvernement du Canada continuera d'accroître la main-d'œuvre canadienne dans le domaine de la cybersécurité grâce à des programmes comme Entrée express[32], qui permet aux travailleurs étrangers qualifiés de venir au Canada et de travailler dans leurs domaines d'expertise.

Le Centre canadien pour la cybersécurité[33] (Centre pour la cybersécurité) est un endroit où le gouvernement du Canada peut trouver de l'expertise en cybersécurité. Le Carrefour de l'apprentissage[34] du Centre pour la cybersécurité a aidé à développer les compétences en matière de cybersécurité de fonctionnaires, tout en aidant à façonner les programmes d'études des établissements postsecondaires canadiens afin de mieux répondre aux exigences du marché du travail. Le Centre de la sécurité des télécommunications[35] (CST) et le Centre pour la cybersécurité contribuent à encourager les groupes sous-représentés à poursuivre des études et des carrières dans les domaines des sciences, des technologies, de l'ingénierie et des mathématiques (STIM) par la sensibilisation de la communauté.

30 https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-fr.aspx
31 https://www.securitepublique.gc.ca/index-fr.aspx
32 https://www.canada.ca/fr/immigration-refugies-citoyennete/services/immigrer-canada/entree-express.html
33 https://www.cyber.gc.ca/fr
34 https://www.cyber.gc.ca/fr/education-communaute/carrefour-apprentissage
35 https://www.cse-cst.gc.ca/fr

Objectif 2.3 : Recenser et soutenir les domaines de recherche ciblés pour répondre aux besoins canadiens

La cyberinnovation à l'échelle nationale rend le Canada plus sûr.

Le Canada est un chef de file mondial dans le domaine des technologies émergentes, telles que l'informatique quantique et l'IA. Dans le cadre d'un marché mondial, cependant, les Canadiens obtiennent de nombreux produits de cybersécurité de la part de fournisseurs étrangers. Afin d'accroître la compétitivité du Canada à l'échelle mondiale, sa cyberrésilience, et sa sécurité économique, le gouvernement du Canada collaborera avec d'autres ordres de gouvernement et le milieu universitaire pour stimuler la recherche et l'innovation à l'appui de l'industrie canadienne de la cybersécurité. Le gouvernement du Canada continuera également de collaborer avec des groupes, comme CANARIE[36], qui contribuent à protéger les écosystèmes canadiens de la recherche et de l'éducation.

> Le gouvernement du Canada prend des mesures pour protéger l'écosystème de la recherche au Canada en mettant en œuvre la nouvelle Politique sur la recherche en technologies sensibles et sur les affiliations préoccupantes[37] qui protège la recherche tout en veillant à ce que la recherche canadienne demeure ouverte et collaborative sur la scène internationale. À l'avenir, les travaux du nouveau Centre de la sécurité de la recherche[38] du Canada guideront la mise en œuvre des Lignes directrices sur la sécurité nationale pour les partenariats de recherche[39] afin de protéger l'innovation canadienne, y compris dans le domaine de la cybertechnologie.

Le gouvernement du Canada investit également dans la sécurisation des données des Canadiens en modernisant ses systèmes de chiffrement et en mettant en œuvre des technologies à résistance quantique. La Stratégie quantique nationale du Canada[40] contribuera à la protection de la vie privée et à la cybersécurité des Canadiens en soutenant la recherche et le développement de talents, ainsi qu'un réseau national de communications quantiques sécurisées et une initiative de cryptographie post-quantique. En s'appuyant sur cette stratégie, le gouvernement du Canada élaborera un

36 https://www.canarie.ca/
37 https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/recherche-technologies-sensibles-affiliations-preoccupantes/politique-recherche-technologies-sensibles-affiliations-preoccupantes
38 https://www.canada.ca/fr/services/defense/securiterecherche/apropos.html
39 https://science.gc.ca/site/science/fr/protegez-votre-recherche/lignes-directrices-outils-pour-mise-oeuvre-securite-recherche/lignes-directrices-securite-nationale-pour-partenariats-recherche
40 https://ised-isde.canada.ca/site/strategie-quantique-nationale/fr/strategie-quantique-nationale-canada

plan d'action sur la cryptographie pour orienter les travaux, aider à mieux protéger les communications et promouvoir la recherche sur la cryptographie.

Le Centre de données de cyber attribution (CDCA) à l'Institut canadien sur la cybersécurité[41] (ICC) de l'Université du Nouveau-Brunswick[42] (UNB) nouvellement financé est un excellent exemple de la manière dont les partenariats avec les universités peuvent accroitre les capacités de recherche et d'innovation du Canada tout en contribuant à notre sécurité nationale et économique.

Cependant, la défense contre les cybermenaces nécessite plus que de simples recherches en technologie. Il faut également comprendre les cybermenaces dans leur contexte criminel et économique plus large afin de trouver des moyens de réduire les incitatifs qui poussent les cybercriminels à agir. Pour y arriver, il faut une collaboration avec la société civile et le milieu universitaire pour encourager la recherche nécessaire à l'établissement de politiques éclairées.

41 https://www.unb.ca/cic/
42 https://www.unb.ca/

Pilier 3 : **Détecter et perturber les auteurs de cybermenaces**

Nos vies et nos entreprises se sont retrouvées en ligne, et les Canadiens et l'industrie canadienne ressentent l'impact croissant des cybermenaces. Les cybercriminels ont ciblé nos infrastructures essentielles, nos réseaux gouvernementaux, nos hôpitaux et notre base industrielle. Les cybercrimes, et plus particulièrement les rançongiciels, demeurent le principal enjeu de cybersécurité touchant tous les niveaux de la société canadienne. La prévention de la cybercriminalité est essentielle à la sécurité publique, à la sécurité nationale et à la prospérité économique des Canadiens.

Pour réduire le nombre et l'impact des cyberincidents, nous devons renforcer nos mécanismes de défense et faire du Canada une cible plus difficile pour les acteurs hostiles. Dans la pratique, cela signifie améliorer notre capacité à dissuader, à détecter, à identifier et à perturber toute la gamme des cybermenaces et à se défendre contre elles.

Le gouvernement du Canada collaborera avec ses partenaires, y compris tous les niveaux d'application de la loi, pour mieux protéger les Canadiens, ainsi que les infrastructures essentielles du gouvernement et du secteur privé, contre les cybercriminels. Il s'agira notamment de favoriser l'adoption généralisée de normes et de pratiques rigoureuses en matière de cybersécurité, d'accroître les capacités canadiennes de surveillance des menaces afin de mieux détecter les incursions dès qu'elles se produisent, et d'encourager l'échange de renseignements et d'informations sur les menaces entre les secteurs économiques afin d'assurer une meilleure vision des menaces auxquelles le Canada est confronté. Le gouvernement du Canada continuera également d'encourager une réponse coordonnée aux cyberincidents.

Objectif 3.1 : Cerner et dissuader les cybermenaces et se défendre contre elles

Les cybermenaces qui pèsent sur la sécurité nationale et économique du Canada continuent d'augmenter chaque année.

Le gouvernement du Canada prend des mesures directes dans le cyberespace international pour contrer les menaces qui pèsent sur le Canada et les Canadiens et pour imposer des coûts aux auteurs de cybermenaces malveillantes.

Dans le cadre de son mandat en matière de cyberopérations, le Centre de la sécurité des télécommunications[43] (CST) mène des cyberopérations contre l'ingérence étrangère et les activités hostiles des acteurs étatiques. Le CST a également contrecarré des opérations sophistiquées de cybercriminalité et a perturbé des activités d'extrémistes établis à l'étranger. Le CST et les Forces armées canadiennes[44] (FAC) participent conjointement à des cyberopérations défensives et offensives, souvent en partenariat avec des alliés. Le gouvernement du Canada renforce aussi ses relations avec d'autres forces militaires afin de s'appuyer sur les compétences uniques et les idées des alliés.

Le Service canadien du renseignement de sécurité[45] (SCRS) intervient également pour protéger le Canada contre les cybermenaces à la sécurité nationale, y compris les activités hostiles des acteurs étatiques. Grâce à ses mandats de collecte du renseignement et de réduction des menaces, appuyés par son éventail de partenariats internationaux, le SCRS enquête sur les cybermenaces préoccupantes à la sécurité nationale, contrecarre les auteurs de cybermenaces malveillantes et fournit des évaluations et des conseils en matière de renseignement à l'ensemble du gouvernement fédéral.

Le programme de lutte contre la cybercriminalité de la police fédérale de Gendarmerie royale du Canada[46] (GRC) enquête sur les activités criminelles liées à la cybercriminalité et sur les menaces à la sécurité nationale. Il s'agit notamment de la cybercriminalité dirigée contre les institutions gouvernementales, les infrastructures essentielles d'importance nationale et les institutions et actifs commerciaux clés du Canada.

Pour renforcer ces efforts, le gouvernement du Canada établira et renforcera des partenariats au-delà du gouvernement fédéral. Par exemple, le gouvernement du Canada, par l'entremise du Collectif canadien pour la cyberdéfense (CCCD), réunira des experts de l'industrie, des universitaires et d'autres ordres de gouvernement pour examiner les défis et les solutions aux problèmes de cybersécurité au niveau national.

43 https://www.cse-cst.gc.ca/fr
44 https://forces.ca/fr/
45 https://www.canada.ca/fr/service-renseignement-securite.html
46 https://www.grc-rcmp.gc.ca/fr

Le gouvernement du Canada reconnaît que l'état de préparation à la cybersécurité varie d'une région à l'autre du pays. Les communautés autochtones, ainsi que les municipalités de petite taille et en milieu rural, ne disposent pas toujours des outils et des ressources nécessaires pour protéger pleinement leurs systèmes et leurs informations. Le gouvernement du Canada étudiera des moyens de réduire cette inégalité par des investissements ciblés, en utilisant des mécanismes tels que le Programme de coopération en matière de cybersécurité[47](PCCS) de Sécurité publique Canada.[48]

En outre, à mesure que les auteurs de menace deviennent plus sophistiqués, il est de plus en plus important que nous utilisions le renseignement sur les menaces pour les bloquer avant qu'elles ne puissent nuire à leurs cibles. En 2022, le gouvernement du Canada a préparé le terrain pour filtrer les activités malveillantes au niveau des fournisseurs de services Internet (FSI) canadiens en exigeant les signalements initiaux. Le Conseil de la radiodiffusion et des télécommunications canadiennes[49] (CRTC) a également l'intention, à la suite de consultations, de mettre en œuvre des règles obligatoires pour le blocage des réseaux de zombies par les FSI. Une collaboration plus poussée sera nécessaire pour développer et élargir les capacités de blocage des menaces afin de fournir une protection automatique aux Canadiens.

Objectif 3.2 : Améliorer les capacités de lutter contre la cybercriminalité

Les Canadiens s'attendent à avoir accès à un Canada numérique sûr et sécurisé.

La cybercriminalité englobe un large éventail d'activités malveillantes, tels que les rançongiciels et la cyberfraude, et l'ingérence non sollicitée dans les réseaux et systèmes appartenant à des organisations, y compris les cyber-systèmes les plus vitaux et les infrastructures critiques du Canada. Elle est perpétrée par des États, des groupes criminels organisés, ainsi que des cybercriminels moins sophistiqués qui achètent des services de cybercriminalité pour mener à bien leurs activités.

Le rançongiciel est la forme la plus répandue et la plus perturbatrice de cybercrime au Canada. En effet, la majorité des demandes d'aide reçues par le Centre national de coordination contre la cybercriminalité[50] (CNC3) concernent des rançongiciels. Les Canadiens continuent également de signaler des pertes records dues à la

47 https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-fr.aspx
48 https://www.securitepublique.gc.ca/index-fr.aspx
49 https://crtc.gc.ca/fra/accueil-home.htm
50 https://rcmp.ca/fr/police-federale/cybercriminalite/centre-national-coordination-en-cybercriminalite

cyberfraude, et ce coût ne cesse de croître. Cela représente de l'argent qui n'alimente pas la croissance économique du Canada. Pour protéger les Canadiens et assurer la croissance de l'économie canadienne, une réponse ferme est nécessaire.

> Le Centre national de coordination contre la cybercriminalité[51] (CNC3) de la Gendarmerie royale du Canada[52] (GRC) coordonne et facilite les enquêtes sur la cybercriminalité dans toutes les juridictions, tant au Canada qu'à l'étranger, fournit des conseils d'enquête et des capacités techniques à d'autres organismes d'application de la loi, et produit du renseignement sur la cybercriminalité pour la police canadienne.
>
> La GRC collabore également avec des partenaires d'application de la loi pour lutter contre la cybercriminalité. Cela inclut notamment une collaboration avec le Centre européen de lutte contre la cybercriminalité d'Europol[53] [lien disponible seulement en anglais], la National Cyber-Forensics and Training Alliance établie aux États-Unis[54] [lien disponible seulement en anglais], ainsi que par l'intermédiaire d'agents de liaison et d'analystes de la GRC déployés dans des endroits stratégiques. Le CNC3 de la GRC fait également partie du Réseau international de prévention de la cybercriminalité[55] [lien disponible seulement en anglais]. Le réseau comprend des organismes d'application de la loi de 26 pays et vise à prévenir la cybercriminalité au moyen de ressources éducatives, de campagnes sur les médias sociaux et d'autres mesures novatrices.

À l'heure actuelle, le gouvernement du Canada mène des cyberopérations afin de réduire la capacité des cybercriminels étrangers de lancer des incursions par rançongiciel et de tirer profit de la vente d'informations volées. Le gouvernement du Canada étudie également d'autres moyens de décourager davantage les paiements de rançons et d'imposer des coûts aux cybercriminels. Il s'agit notamment d'améliorer l'approche du Canada à l'égard des polices de cyberassurance afin de rendre les modèles d'affaires cybercriminels, en particulier les rançongiciels, moins rentables. Le gouvernement du Canada s'est également engagé à collaborer avec l'industrie afin de dissuader les entreprises de payer des rançons, conformément à l'Initiative de lutte contre les rançongiciels.[56]

51 https://rcmp.ca/fr/police-federale/cybercriminalite/centre-national-coordination-en-cybercriminalite
52 https://www.rcmp-grc.gc.ca/fr
53 https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
54 https://www.ncfta.net/
55 https://www.europol.europa.eu/partners-collaboration/networks/intercop-international-cyber-offender-prevention-network
56 https://www.canada.ca/fr/securite-publique-canada/nouvelles/2023/11/declaration-internationale--declaration-commune-de-linitiative-de-lutte-contre-les-rancongiciels-au-sujet-des-paiements-lies-aux-rancongiciels.html

De plus, le gouvernement du Canada s'est engagé à renforcer la capacité du Canada en matière de sécurité nationale et d'application de la loi. L'éducation sera un moyen important de le faire. Le gouvernement du Canada aidera à améliorer la capacité des organismes d'application de la loi d'aider les victimes de cybercriminalité, au moyen d'une approche axée sur les victimes.

La cybercriminalité transcende les frontières et implique souvent des États hostiles ou des groupes criminels organisés. Le gouvernement du Canada continuera de collaborer avec ses alliés internationaux pour imposer des coûts aux cybercriminels et perturber le modèle d'affaire de la cybercriminalité.

Les signalements sont essentiels aux efforts du gouvernement du Canada pour mieux comprendre le portrait de la cybermenace, perturber les activités criminelles et prévenir les incursions, ainsi que démanteler les infrastructures cybercriminelles. Le gouvernement du Canada exhorte les personnes qui ont été la cible de cybercrimes à communiquer avec les services de police locaux et le Centre antifraude du Canada[57] (CAFC). Le gouvernement du Canada lancera un nouveau système de signalement des incidents de cybercriminalité et de fraude[58] afin que les Canadiens puissent signaler plus facilement les cybercrimes et la fraude aux organismes d'application de la loi, et que les organismes d'application de la loi puissent échanger de l'information.

Objectif 3.3 : Rendre les systèmes essentiels plus résilients

Les infrastructures essentielles sous-tendent les services que les Canadiens utilisent au quotidien.

Les propriétaires et les exploitants d'infrastructures essentielles sont la cible de cyberactivités persistantes, bien financées et sophistiquées. Les cyberacteurs malveillantes peuvent entraver ou endommager les infrastructures critiques canadiennes, comme les usines de traitement de l'eau, les réseaux énergétiques, les pipelines, les infrastructures de transport et l'équipement agricole. Ils peuvent également perturber les services essentiels, comme les soins de santé et les chaînes d'approvisionnement, mettant en péril la sécurité et les moyens de subsistance des Canadiens. En outre, les cyberincidents érodent la confiance dans les réseaux et les systèmes d'exploitation utilisés, ainsi que dans les institutions publiques et privées chargées de protéger les renseignements personnels et de nature délicate. Les coûts économiques et sociétaux élevés des cyberincidents soulignent l'importance de protéger les infrastructures essentielles du Canada.

57 https://antifraudcentre-centreantifraude.ca/index-fra.htm
58 https://www.rcmp-grc.gc.ca/fr/nouveau-systeme-signalement-des-incidents-cybercriminalite-et-fraude

> Le gouvernement du Canada dispose de deux procédures complémentaires lorsqu'un cyberincident se produit. Premièrement, le Plan de gestion des événements de cybersécurité du gouvernement du Canada[59] fournit un cadre pour gérer les événements de cybersécurité qui nuisent ou qui menacent de nuire à la capacité du gouvernement du Canada de fournir des programmes et des services aux Canadiens. Deuxièmement, le Plan fédéral de réponse aux cyberincidents[60] (PFRC) est un plan de coordination et un cadre d'échange d'information lors des interventions du gouvernement du Canada en cas de cyberincidents importants touchant les systèmes non gouvernementaux du Canada qui sont essentiels à la santé, à la sûreté, à la sécurité, à la défense ou au bien-être économique des Canadiens.

Le gouvernement du Canada reconnaît l'importance de travailler collectivement pour renforcer les infrastructures essentielles du pays afin de dissuader les cybermenaces. Les infrastructures essentielles du Canada sont détenues et gérées par diverses organisations, de sorte que tous les ordres de gouvernement, de concert avec l'industrie privée, doivent collaborer pour garantir la sécurité de l'information, des technologies opérationnelles, des systèmes de contrôle industriels et des chaînes d'approvisionnement en logiciels.

Le gouvernement du Canada continuera de collaborer avec les partenaires et les intervenants de l'industrie dans le cadre de la Coalition mondiale sur les télécommunications[61] afin de favoriser diverses chaînes d'approvisionnement ainsi que la sécurité et l'interopérabilité des normes dans le secteur des télécommunications. Le gouvernement du Canada soutiendra également le travail effectué par des organismes et des forums de cybersécurité, tels que le Bouclier canadien de l'Autorité canadienne pour les enregistrements Internet[62] (ACEI), Rogers Cybersecure Catalyst[63] [lien disponible en anglais seulement], l'Échange canadien de menaces cybernétiques[64] [lien disponible en anglais seulement] et CANARIE[65]. À l'avenir, le Collectif canadien pour la cyberdéfense (CCCD) servira également de forum important pour que les secteurs puissent discuter des infrastructures essentielles.

59 https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/securite-confidentialite-ligne/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html
60 https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/fdrl-cbr-ncdnt-rspns-pln-2023/index-fr.aspx
61 https://ised-isde.canada.ca/site/isde/fr/coalition-mondiale-telecommunications-declaration-dintention-conjointe
62 https://www.cira.ca/fr/bouclier-canadien-de-cira/
63 https://cybersecurecatalyst.ca/
64 https://cctx.ca/
65 https://www.canarie.ca/fr/

De plus, le gouvernement du Canada continuera d'améliorer sa capacité de se défendre contre les cyberincidents et de s'en remettre. Le Centre canadien pour la cybersécurité[66] (Centre pour la cybersécurité) s'efforce de partager des capacités de cyberdéfense avancées avec un nombre croissant de propriétaires et opérateurs d'infrastructures essentielles. De cette façon, le Centre pour la cybersécurité renforcera les services essentiels non gouvernementaux, comme les services bancaires et les télécommunications.

66 https://www.cyber.gc.ca/fr

Conclusion

La Stratégie nationale de cybersécurité du Canada 2025 vise à sécuriser l’avenir numérique du Canada . Elle décrit les travaux en cours et à venir du gouvernement du Canada pour améliorer la cybersécurité grâce à des efforts nationaux et internationaux.

La cybersécurité est une responsabilité qui incombe à l’ensemble de la société. Le gouvernement du Canada invite les autres ordres de gouvernement, les communautés autochtones, le secteur privé et le milieu universitaire à participer à l’élaboration d’une série de plans d’action. Chaque plan d’action permettra de relever un défi majeur identifié dans la présente stratégie. Cette vaste collaboration est nécessaire pour garantir que les plans d’action améliorent la cyber-résilience nationale du Canada à tous les niveaux, et pas seulement au niveau du gouvernement du Canada.

Cette approche marque l’engagement du gouvernement du Canada à poursuivre le dialogue avec les parties prenantes afin de contribuer à la conception et à la mise en œuvre d’initiatives visant à mieux protéger les Canadiens. En mettant en œuvre la Stratégie au moyen d’une série de plans d’action échelonnés dans le temps, le Canada disposera d’un mécanisme souple lui permettant de réagir en temps utile à un cyberenvironnement en constante évolution. Ensemble, nous veillerons à ce que le cyberespace soit protégé, ouvert, sûr, stable et accessible à tous les Canadiens.

Les rôles et responsabilités en matière de cybersécurité au gouvernement du Canada

Ces entités ont des rôles et des fonctions de cybersécurité essentiels pour le public et servent de vitrines principales au gouvernement du Canada : le Centre canadien pour la cybersécurité, Sécurité publique Canada, la Gendarmerie royale du Canada et le Service canadien du renseignement de sécurité. Beaucoup d'autres ont des rôles propres à un domaine qui comportent la mobilisation du public ou des partenariats de différents types.

La stratégie s'accompagne d'un appel au partenariat. Un appel à la population canadienne et aux organisations canadiennes de toutes tailles au signalement des cyberincidents et des cybercrimes de toutes sortes. Un appel au financement pour faire progresser la cyberinnovation et aider les collectivités et les entreprises à être plus cybersécuritaires. Un appel à une politique et à une réglementation éclairée. Un appel à une cyberhygiène, une littératie numérique et une sensibilisation du public améliorée. C'est dans cette direction que les intervenants peuvent se tourner.

Rôles essentiels en matière de cybersécurité axés sur le public

Centre canadien pour la cybersécurité (Centre de la sécurité des télécommunications)

Signaler un incident (organisations)

- Signalement et atténuation des incidents

Sensibilisation du public

- Source de conseils généraux et propres aux menaces et aux secteurs matière de cybersécurité pour la population canadienne et les organisations canadiennes
- Sensibilisation du public à la cybersécurité

Opérations

- Coprésident (président des opérations) du Collectif canadien pour la cyberdéfense (CCCD)

Sécurité publique Canada

Cyberfinancement

- Financement de la cybersécurité pour les petites et moyennes entreprises

Politiques

- Responsable de la politique nationale de cybersécurité
- Responsable de la politique de sécurité des infrastructures essentielles (IE) nationales
- Coprésident (président des politiques) du Collectif canadien pour la cyberdéfense (CCCD)

Gendarmerie royale du Canada

Signaler un incident

- Signalement et coordination des cybercrimes et de la fraude via le Centre national de coordination contre la cybercriminalité (CNC3) et du Centre antifraude du Canada (CAFC)
- Signalement d'incidents suspects via l'Équipe nationale des infrastructures essentielles

Sensibilisation du public

- Prévention de la cybercriminalité et sensibilisation du public

Opérations

- Enquête sur les principales menaces de cybercriminalité envers le Canada

Service canadien du renseignement de sécurité

Sensibilisation du public

- Entretenir des contacts avec les entités des secteurs public et privé sur les cybermenaces à la sécurité nationale

Opérations

- Enquêter et prendre des mesures pour atténuer ou réduire les cybermenaces à la sécurité nationale visant des entités canadiennes

Autres rôles en matière de cybersécurité axés sur le public

Innovation, sciences et développement économique Canada

Signaler un incident

- Signalement de pourriels

Politiques

- Responsable de la politique nationale pour le développement et la commercialisation de nouvelles technologies (y compris la technologie de l'information et des communications [TIC] et les télécommunications)

Ressources naturelles Canada

Opérations

- Fournir une expertise dans le secteur de l'énergie et mettre en relation les parties prenantes au sein du gouvernement, de l'industrie, des universités et autres afin d'améliorer la résilience des infrastructures énergétiques essentielles en matière de cybersécurité
- Faciliter et faire progresser le partage d'informations en temps utile entre les parties prenantes du secteur de l'énergie dans le but de renforcer la résilience des infrastructures énergétiques essentielles

Politiques

- Responsable de la politique en matière de cybersécurité des infrastructures énergétiques essentielles, y compris les infrastructures énergétiques transfrontalières (Canada-États-Unis)

Transports Canada

Signaler un incident

- Signalement des incidents de cybersécurité via le Centre d'intervention de Transports Canada

Politiques

- Responsable de la politique nationale en matière de sécurité et de sûreté des systèmes de transport maritime, aérien, ferroviaire et routier

Conseil national de recherches du Canada

Cyberfinancement

- Financement de la recherche et du développement dans le domaine de la cybersécurité

Services publics et approvisionnement Canada

Politiques

- Responsable de la politique sur l'approvisionnement (exigences en matière de sécurité – cybersécurité)

Conseil canadien des normes

Politiques

- Responsable des normes de cybersécurité

Organisations fédérales ayant des rôles en matière de cybersécurité non axés sur le public

Certaines des fonctions les plus essentielles à la cyberdéfense et à la sécurité nationales du Canada sont invisibles aux yeux du public – sur les systèmes et les réseaux, en coordination avec les partenaires des infrastructures essentielles et avec les alliés de partout dans le monde. Le gouvernement du Canada participe activement aux cyberopérations offensives et défensives contre les auteurs de menaces malveillantes, fonction qui revêt une importance croissante pour la sécurité économique et nationale. La mobilisation pour élaborer des cyberpolitiques et des normes étrangères augmente d'année en année. Et un effort multiministériel défend le réseau du gouvernement et maintient les services essentiels en ligne.

- Ministère de la défense nationale
- Affaires mondiales Canada
- Bureau du conseil privé
- Services partagés Canada
- Secrétariat du conseil du trésor du Canada
- Ministère des finances Canada

Régulateurs fédéraux du secteur des infrastructures essentielles

- Régie de l’énergie du Canada
- Commission canadienne de sûreté nucléaire
- Conseil de la radiodiffusion et des télécommunications canadiennes
- Office des transports du Canada
- Bureau du surintendant des institutions financières

Glossaire

Cryptographie, y compris le chiffrement
Ensemble des principes, des techniques et des méthodes de la transformation de données afin d'en préserver le contenu, ainsi que de prévenir les modifications non détectées ou son utilisation non autorisée. La conversion de l'information en cette nouvelle forme protégée s'appelle le « chiffrement ». La conversion de l'information à sa forme originale est le « déchiffrement ».

Cybercrime ou cybercriminalité
Tout acte criminel lorsqu'un cyberélément (c.-à-d. Internet et les technologies de l'information comme les ordinateurs, les tablettes ou les téléphones intelligents, etc.) joue un rôle important dans la perpétration d'une infraction criminelle. En termes généraux, la GRC divise la cybercriminalité en deux catégories : infractions où la technologie est la cible et infractions où la technologie est l'instrument. Un acte criminel qui est commis à l'aide d'un système informatique ou d'un réseau d'ordinateurs ou qui les fait intervenir directement. L'ordinateur ou ses données peuvent être la cible de cet acte, ou l'ordinateur peut être l'outil avec lequel le crime est commis.

Cyberespace
Monde électronique créé par les réseaux interreliés de la technologie de l'information et de l'information qui circule dans ces réseaux. Le cyberespace est un bien commun reliant plus de trois milliards de personnes qui échangent des idées et des services et qui tissent des liens d'amitié.

Cyberincident
Toute tentative non autorisée, fructueuse ou non, en vue d'avoir accès à des ressources ou à des réseaux informatiques, ou de les modifier, de les détruire, de les supprimer ou de les rendre indisponibles.

Cybermenace
Toute circonstance ou événement susceptible d'avoir un impact négatif sur les opérations de l'organisation (y compris la mission, les fonctions, l'image ou la réputation), les actifs de l'organisation, les personnes, d'autres organisations ou la nation par le biais d'un système d'information via un accès non autorisé, une destruction, une divulgation, une modification de l'information et/ou un refus de service.

Cyberopération
Mesures prises dans le cyberespace pour perturber et contrecarrer la capacité d'un auteur de menace à opérer en ligne ou pour le défendre.

Cyberrésilience
Capacité d'anticiper, de résister, de se remettre et de s'adapter à des conditions défavorables, des contraintes, des attaques ou des compromis sur des systèmes qui utilisent ou sont activés par des ressources informatiques.

Cybersécurité
Protection de données numériques et préservation de l'intégrité de l'infrastructure servant à stocker et à transmettre des données numériques. Plus particulièrement, la cybersécurité englobe l'ensemble des technologies, des processus, des pratiques, des mesures d'intervention et d'atténuation dont la raison d'être est d'empêcher que les réseaux, ordinateurs, programmes et données soient attaqués ou endommagés, ou qu'on y accède sans autorisation, afin d'en assurer la confidentialité, l'intégrité et la disponibilité.

Économie numérique
Toutes les activités économiques qui dépendent de l'utilisation d'intrants numériques, ou sont grandement améliorées par le recours à ces intrants, y compris les technologies numériques, l'infrastructure numérique, les services numériques et les données. Il fait référence à tous les producteurs et consommateurs, y compris le gouvernement, qui utilisent ces intrants numériques dans leurs activités économiques.

Informatique quantique
Les ordinateurs quantiques sont des appareils expérimentaux conçus pour effectuer certains calculs très rapidement. Tandis qu'un ordinateur classique travaille avec des « 1 » et des « 0 », un ordinateur quantique a l'avantage d'utiliser le « 1 », le « 0 » et des superpositions de « 1 » et de « 0 ». Certaines tâches complexes que les ordinateurs classiques ne pouvaient pas effectuer peuvent désormais être effectuées rapidement et efficacement par un ordinateur quantique.

Infrastructure essentielle
Processus, systèmes, installations, technologies, réseaux, actifs et services essentiels à la santé, à la sécurité ou au bien-être économique des Canadiens et au bon fonctionnement des pouvoirs publics.

Intelligence artificielle
Sous-domaine de l'informatique qui porte sur le développement de programmes informatiques intelligents qui peuvent résoudre des problèmes, apprendre de ses expériences, comprendre des langages, interpréter des scènes visuelles et, en général, se comporter d'une façon qui serait considérée comme intelligente chez l'humain.

Internet des objets
Interconnexion par Internet de dispositifs informatiques intégrés dans des objets du quotidien qui peuvent alors envoyer et recevoir des données.

Rançongiciel
Logiciel malveillant qui empêche une personne ou une organisation d'avoir accès aux fichiers et aux systèmes clés jusqu'à ce qu'une rançon soit versée au cybercriminel. Les rançongiciels impliquent le cryptage, des écrans verrouillés et/ou d'autres méthodes

pour empêcher l’accès aux fichiers et extorquer de l’argent aux victimes, comme la fuite de données sensibles en ligne, et les paiements de rançons impliquent souvent des cryptomonnaies.

Sécurisé dès la conception
Produits technologiques construits d’une manière qui protège raisonnablement contre les auteurs de cybermenaces malveillantes qui réussissent à accéder aux appareils, aux données et aux infrastructures connectées.

Système de contrôle industriel (SCI)
Terme général qui englobe plusieurs types de systèmes de contrôle qui se retrouvent souvent dans les secteurs industriels et les infrastructures essentielles. Les SCI sont les systèmes automatisés utilisés pour fournir des services essentiels aux Canadiens et se composent de combinaisons de composants de commande (p. ex., électriques, mécaniques, hydrauliques, pneumatiques) qui agissent ensemble pour atteindre un objectif industriel (p. ex., fabrication, transport de matière ou d’énergie). Les SCI interviennent dans tout, de l’électricité qui alimente les ordinateurs, à l’eau qui circule dans les immeubles, aux feux de circulation qui contrôlent les trajets quotidiens.