Sécurité publique Canada | Public Safety Canada

Canada

Stratégie nationale de cybersécurité

Vision du canada pour la sécurité et la prospérité dans l'ère numérique

No de cat. : PS4-239/2018F
ISBN : 978-0-660-26555-1

Table de matières

Avant-propos

L'HONORABLE RALPH GOODALE

Ministre de la Sécurité publique et de la Protection civile

Pratiquement tout ce que les Canadiens font est touché par la technologie d'une certaine façon. En fonction du nombre d'habitants, nous passons le plus de temps en ligne de tous les pays du monde, à 43,5 heures par Canadien par mois. Nous sommes fortement interconnectés et réseautés, un fait qui améliore notre qualité de vie, mais qui crée aussi des vulnérabilités. Des chaînes d'approvisionnement commercial à l'infrastructure essentielle qui sous-tend notre économie et notre société, les risques dans l'espace cybernétique se sont multipliés, accélérés et ont connu une croissance de plus en plus malveillante.

Les grandes sociétés et industries et nos alliés et partenaires internationaux sont engagés dans le défi cybernétique mondial. Cependant, beaucoup d'autres personnes ne le sont pas, ce qui représente un risque important, mais aussi une occasion manquée dans cette industrie mondiale en croissance rapide. Bien qu'il soit important d'être très conscient des cybermenaces, la politique du Canada en matière de cybersécurité ne peut pas être motivée par la peur et la défensive.

Dans cette perspective, le renouvellement de la Stratégie nationale de cybersécurité actuelle a été entrepris en mettant l'accent sur l'énorme potentiel du leadership accru du Canada dans ce domaine. En partenariat avec les ministres de la Défense, de l'Innovation, de l'Infrastructure, des Services publics et du Conseil du Trésor, nous avons consulté directement les Canadiens et les intervenants clés sur la façon dont la nouvelle stratégie pourrait mieux répondre à leurs besoins en matière de sécurité, tout en leur permettant de profiter des possibilités qu'offre l'économie numérique. Forte de plus de 2 000 présentations soumises à notre consultation publique, la Stratégie aborde directement les lacunes et les points à améliorer dans le climat actuel de la cybersécurité du Canada.

Les objectifs fondamentaux de la Stratégie sont pris en compte dans les investissements substantiels destinés à la cybersécurité du budget de 2018, totalisant plus de 500 millions de dollars sur 5 ans. Le budget de 2018, le

plus important investissement jamais fait par le gouvernement du Canada dans la cybersécurité, démontre notre engagement à l'égard de la sécurité à l'ère numérique. Parmi les nouvelles mesures instaurées :

- Le financement du nouveau Centre canadien pour la cybersécurité afin d'appuyer le leadership et la collaboration entre les différents ordres de gouvernement et les partenaires internationaux, tout en fournissant une ressource claire et fiable aux citoyens et aux entreprises du Canada.
- La création de l'Unité nationale de coordination de la lutte contre la cybercriminalité afin d'accroître la capacité de la Gendarmerie royale du Canada d'enquêter sur la cybercriminalité, en établissant un centre de coordination pour les partenaires nationaux et internationaux.
- Le financement pour favoriser l'innovation et la croissance économique, et le développement de talents canadiens en cybersécurité.

La Stratégie est la feuille de route du Canada afin d'aller de l'avant en ce qui concerne la cybersécurité et elle est conçue pour atteindre les objectifs et les priorités des Canadiens. Nous sommes fiers de montrer la voie.

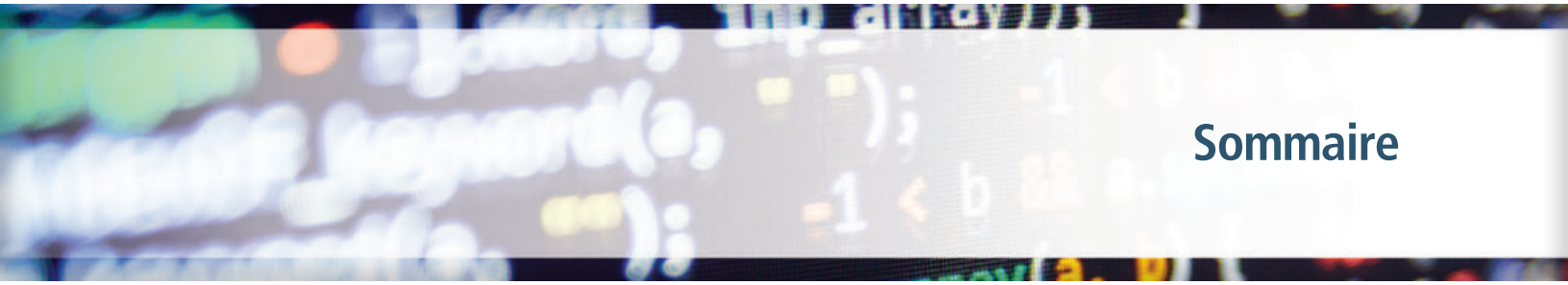
Sommaire

La place du Canada dans le monde numérique

Notre monde a été transformé par l'innovation numérique.

Les technologies numériques font maintenant partie de notre quotidien, tout comme les nouveaux développements que nous constatons chaque jour. Qu'il s'agisse d'exploitation d'entreprises, d'accès aux services gouvernementaux, d'interaction avec les amis et les membres de la famille, ces technologies rapprochent les Canadiens d'un océan à l'autre et les relient à un réseau mondial dynamique.

Ce n'est que le début. Les technologies sont source infinie de nouvelles idées révolutionnaires. Nous continuerons de voir l'innovation numérique atteindre de nouveaux sommets, au profit de nos collectivités, de nos sociétés et de notre planète.



Sommaire

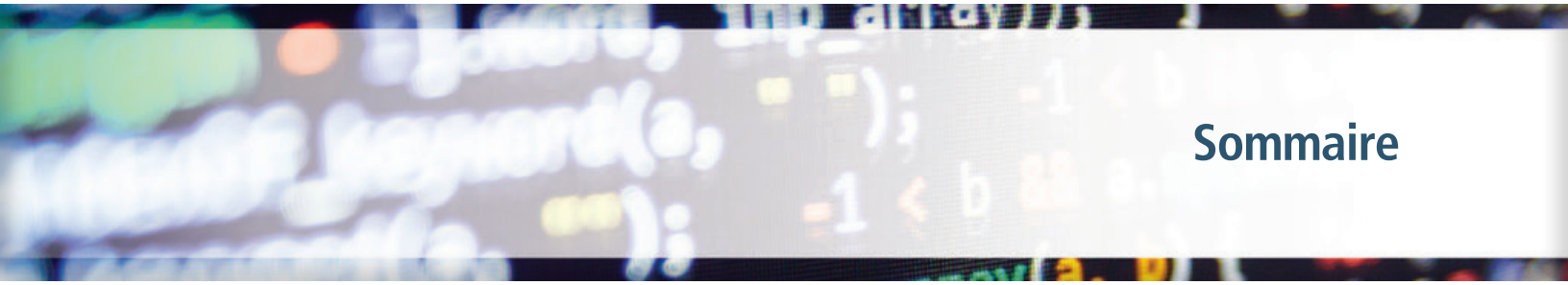
L'importance de la cybersécurité

Cependant, à mesure que nous adoptons les technologies numériques en raison des avantages formidables qu'elles procurent, nous nous exposons à des menaces.

Les criminels et d'autres auteurs de cybermenaces malveillantes, plusieurs d'entre eux qui opèrent hors de nos frontières, se servent des lacunes en matière de sécurité, du manque de connaissances sur la cybersécurité et des développements technologiques pour compromettre les cybersystèmes. Ces criminels volent des données personnelles et financières, des éléments de propriété intellectuelle et des secrets commerciaux. Ils perturbent et parfois détruisent les infrastructures dont nous dépendons pour obtenir des services essentiels et soutenir notre mode de vie.

En 2010, le gouvernement du Canada a lancé la toute première Stratégie de cybersécurité du Canada dans le cadre d'un effort national pour défendre les Canadiens contre les menaces à la cybersécurité. Les réalisations accomplies dans le cadre de la Stratégie de 2010 sont à la base des mesures futures.

Notre nouvelle approche tient compte du caractère essentiel des technologies numériques dans notre vie. Une nouvelle stratégie de cybersécurité nous permettra de procéder avec confiance dans l'ère numérique. Dans la réalité qu'est l'ère numérique, la cybersécurité est le complément de l'innovation et le protecteur de la prospérité.



Sommaire

La vision de la Stratégie nationale de cybersécurité : la sécurité et la prospérité dans l'ère numérique

Une cybersécurité solide est un élément essentiel de l'innovation et de la prospérité au Canada. Les particuliers, les gouvernements et les entreprises veulent tous faire confiance aux systèmes informatiques qui sont si importants pour leur vie quotidienne. Le gouvernement du Canada entrevoit un avenir où tous les Canadiens jouent un rôle actif pour façonner et soutenir la résilience de notre nation en matière de cybersécurité.

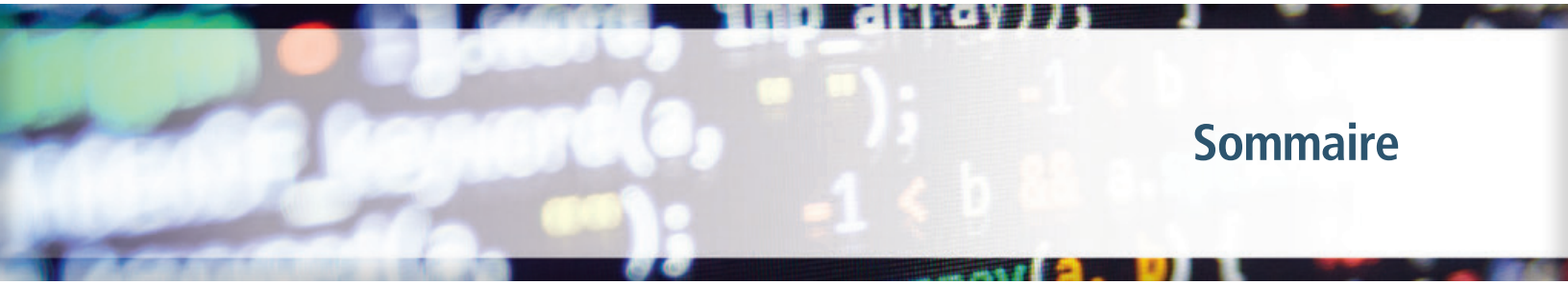
Pour réaliser la vision, le gouvernement du Canada et ses partenaires travailleront ensemble sur trois thèmes :

Sécurité et resilience

En collaborant avec les partenaires et en améliorant les capacités en matière de cybersécurité, nous pouvons mieux protéger les Canadiens contre la cybercriminalité, contrer les menaces en évolution et défendre les systèmes essentiels du gouvernement et du secteur privé.

Innovation en matière de cybersécurité

En appuyant la recherche de pointe, en encourageant l'innovation numérique, en perfectionnant les compétences et les connaissances en matière de cybersécurité, le gouvernement fédéral positionnera le Canada comme un chef de file mondial dans le domaine de la cybersécurité.



Sommaire

Leadership et Collaboration:

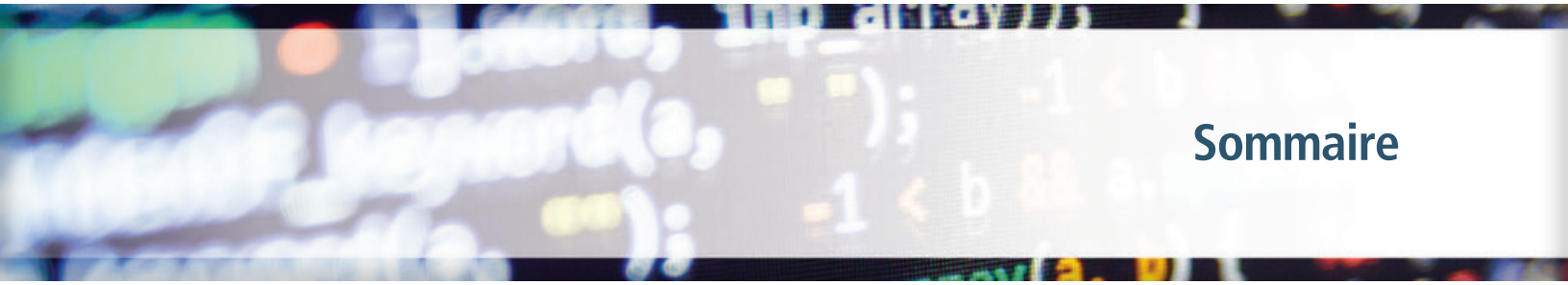
> En étroite collaboration avec les provinces, les territoires et le secteur privé, le gouvernement fédéral jouera un rôle de premier plan pour faire progresser la cybersécurité au Canada; par ailleurs, de concert avec les alliés, il travaillera à façonner l'environnement de cybersécurité international en faveur du Canada.

Dans un environnement de cybersécurité dynamique, l'approche du gouvernement du Canada sera fondée sur un engagement soutenu :

- à protéger la sécurité des citoyens et des infrastructures essentielles du Canada;
- à promouvoir et de protéger les droits et les libertés en ligne;
- à favoriser la cybersécurité pour la croissance et la prospérité économiques des entreprises;
- à appuyer la coordination entre les administrations et les secteurs et de collaborer avec ces derniers pour renforcer la cyberrésilience du Canada;
- à prendre des mesures proactives pour s'adapter aux changements dans le contexte de la cybersécurité et à l'émergence de nouvelles technologies.

Portée de la Stratégie

La Stratégie comprend tout d'abord les activités déjà entamées par le gouvernement du Canada, comme les efforts actuels et futurs déployés pour sécuriser les systèmes du gouvernement du Canada, élargir notre réseau de partenariats pour protéger les infrastructures essentielles et aider les



Sommaire

Canadiens à se protéger en ligne. Toutefois, dans un contexte mondial de cybersécurité plus dynamique et plus diversifié, la nouvelle approche du Canada devra être plus inclusive et plus élargie.

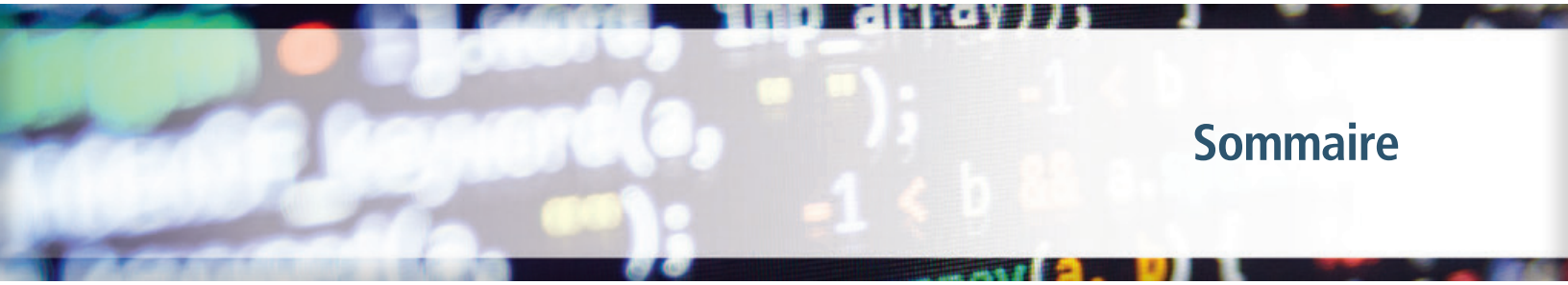
Le présent document énonce les principaux éléments de l'environnement de cybersécurité mondial et présente certains moyens que le gouvernement du Canada utilisera pour faire face à un éventail de nouvelles possibilités et de nouveaux défis dans le cyberespace.

Mise en œuvre de la Stratégie

Comme le rythme des changements que nous vivons ne fera que s'accélérer, la Stratégie est conçue principalement pour appuyer les efforts continus du gouvernement visant à renforcer la cybersécurité au Canada. Les mesures prises par le gouvernement devront évoluer de pair avec les innovations technologiques et les changements de paradigmes connexes qui sont devenus monnaie courante dans notre monde branché.

Des plans d'action sur la cybersécurité viendront compléter la Stratégie. Ils décriront avec précision les initiatives que le gouvernement fédéral prendra au fil du temps et qui sont assorties de paramètres de rendement clairs et d'un engagement de produire des rapports sur les résultats obtenus. Les plans d'action énonceront aussi le plan du gouvernement visant à travailler avec les partenaires internes et externes pour réaliser la vision.

La mise en œuvre de la Stratégie s'alignera sur la mise en œuvre d'autres initiatives de cybersécurité du gouvernement du Canada, comme le mandat du ministre des Institutions démocratiques consistant à défendre



Sommaire

le processus électoral contre les cybermenaces; la politique étrangère sur le cyberespace dans le programme international du Canada; l'usage militaire du cyberespace au Canada; le plan pour l'innovation et les compétences.

Stratégie de cybersécurité du Canada 2010

Le gouvernement a affecté 431,5 millions de dollars sur dix ans dans le cadre de la première Stratégie de cybersécurité du Canada, qui reposait sur trois piliers et visait un vaste éventail de réalisations.

I. Protéger les systèmes gouvernementaux

Le gouvernement du Canada a renforcé sa capacité de prévenir et de détecter les cyberattaques, d'intervenir et de se rétablir après coup. Le nombre d'atteintes à la sécurité des données baisse de façon constante depuis 2010, en dépit de la hausse du nombre de cyberattaques parrainées ou non par des États contre les réseaux du gouvernement, qui sont de plus en plus sophistiquées.

II. Nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral

Des partenariats étroits ont été noués avec les propriétaires et exploitants d'infrastructures essentielles du Canada, le secteur privé et les gouvernements provinciaux et territoriaux. Le Centre canadien de réponse aux incidents cybernétiques (CCRIC) a élargi ses opérations; en effet, plus de 1 300 organisations reçoivent régulièrement des alertes et des communications.

III. Aider les Canadiens à se protéger en ligne

Dans le cadre de la campagne Pensez cybersécurité, le gouvernement du Canada a favorisé la sensibilisation à la cybersécurité en organisant des activités de sensibilisation et en élaborant des ressources ciblées.

Stratégie de cybersécurité du Canada 2010

Des efforts déployés en 2010 dans le cadre de la Stratégie ont également permis de renforcer la capacité de la Gendarmerie royale du Canada (GRC) et des organismes d'application de la loi de lutter contre la cybercriminalité, ce qui comprend des investissements dans le renseignement en matière de cybercriminalité, ainsi que les enquêtes et la formation connexes.

Introduction

Miser sur les réalisations du canada dans un contexte de cybersécurité dynamique

Qu'est-ce que la cybersécurité?

La cybersécurité est définie comme la protection de l'information numérique et de l'infrastructure sur laquelle elle repose.

La cybersécurité était autrefois la chasse gardée d'experts techniques, mais aujourd'hui, dans notre univers numérique, nous avons tous un rôle à jouer pour protéger notre cybersécurité individuelle et collective.

De la marginalité à la normalité

La mesure dans laquelle la technologie numérique est désormais intégrée dans notre vie quotidienne aurait été inimaginable il y a quelques années. Qu'il s'agisse des médias sociaux, des applications de téléphones intelligents, des achats en ligne, des appareils en réseau ou du nuage, entre autres, nous avons besoin des technologies numériques, et pas seulement pour notre plaisir personnel; en effet, celles-ci font partie intégrante des systèmes qui sont essentiels à notre économie et à notre mode de vie. Ces

Introduction

systèmes interdépendants comprennent les réseaux de communication qui sont connectés au sein du pays et au reste du monde, l'énergie qui sert à chauffer nos maisons et à alimenter notre industrie et les moyens de transport aérien, ferroviaire et routier que nous utilisons chaque jour.

Nous avons tendance à tenir cette connectivité pour acquise, sans nous arrêter pour réfléchir à ses répercussions. Il ne faut jamais tenir la cybersécurité pour acquise. À mesure que les possibilités et les avantages qu'offrent les technologies augmentent, il est de plus en plus essentiel de sécuriser ces technologies.

Faire le point sur un contexte en constante évolution

En 2016, le gouvernement du Canada a entrepris la première étape en vue de l'élaboration d'une nouvelle stratégie de cybersécurité. On a lancé l'examen de la cybersécurité pour comprendre les répercussions en matière de cybersécurité d'une nation branchée, et afin que le gouvernement du Canada soit bien placé pour mettre en place une nouvelle approche compte tenu des difficultés et des possibilités qui se présentent à nous.

L'examen de la cybersécurité visait à faire le point sur les menaces changeantes dans le cyberespace, à nous permettre de comprendre et d'analyser comment la cybersécurité devient un moteur de prospérité économique et à déterminer le rôle approprié du gouvernement fédéral dans l'ère numérique. L'examen comportait un volet de mobilisation accrue du milieu fédéral de la cybersécurité, une évaluation de notre rendement dans le cadre de la Stratégie de 2010 et le lancement des toutes premières consultations publiques sur la cybersécurité. Le gouvernement du Canada a recueilli les idées et les conseils d'experts, d'intervenants clés et de citoyens engagés.

APERÇU SUR LA CYBERSÉCURITÉ : LES AVANTAGES DE LA SAUVEGARDE

Jacqueline est propriétaire d'une petite entreprise en ligne où elle vend des objets d'artisanat. Un jour, elle reçoit un courriel d'un client qui se plaint au sujet d'un objet brisé. Le client lui envoie une image de l'objet; mais, lorsqu'elle tente d'ouvrir la pièce jointe, Jacqueline s'aperçoit que son ordinateur est verrouillé. Un message apparaît à l'écran indiquant que l'ordinateur ne sera déverrouillé que si elle verse une rançon de 1 000 $. Heureusement, Jacqueline fait régulièrement des copies de sauvegarde pour le contenu de son ordinateur. Elle efface le contenu du disque dur, supprime le maliciel envoyé dans la pièce jointe et récupère les données sauvegardées, ce qui lui permet de rétablir l'accès à tous ses documents.

Introduction

Notre réponse

La nouvelle stratégie de cybersécurité tient compte des perspectives découlant de l'examen de la cybersécurité et du fait que si les cybermenaces sont de plus en plus sophistiquées et de plus en plus importantes, le potentiel est énorme pour ce qui est de l'expertise et de l'innovation numériques dans le domaine de la cybersécurité au Canada. La stratégie est conçue en fonction du contexte de la cybersécurité, qui change constamment.

Notre stratégie nationale de cybersécurité établit trois objectifs en réponse aux menaces en évolution, aux nouvelles possibilités et au besoin d'une action concertée :

- des systèmes canadiens sécuritaires et résilients;
- un écosystème du cyberespace novateur et adaptable;
- un leadership et une collaboration efficaces.

Le gouvernement fédéral dirigera les efforts pour réaliser ces objectifs dans un monde où la cybersécurité n'est pas seulement une nécessité, mais un avantage concurrentiel pour le Canada.

APERÇU SUR LA CYBERSÉCURITÉ : MOTS DE PASSE INTELLIGENTS

Christine apprécie l'aspect pratique du nuage. Elle a créé un compte central en ligne qui gère toutes les données de son ordinateur, de son téléphone intelligent, de son moniteur d'activité physique et même de son système de sécurité à domicile. Grâce à l'informatique en nuage, ses comptes de courriel et de médias sociaux sont liés, ses photos et ses vidéos sont téléchargées automatiquement, et tous les changements de calendrier apparaissent sur tous ses appareils. Christine utilise toujours le même mot de passe, ce qui est plus facile à retenir. Lorsqu'elle prend connaissance d'une brèche de données touchant son compte de courriel, elle comprend que quelqu'un pourrait utiliser son mot de passe pour avoir accès à son compte en nuage. Afin de protéger ses renseignements personnels et ses données, Christine créé un nouveau mot de passe solide, qu'elle modifie légèrement pour d'autres services en ligne.

A propos de l'examen de la Cybersécurité

Les commentaires reçus dans le cadre des consultations étaient exhaustifs, pertinents et utiles, et ont été formulés par des représentants du milieu du cyberespace du gouvernement fédéral, d'experts en matière de cybersécurité, de dirigeants d'entreprise, de fonctionnaires, d'agents d'application de la loi, de chercheurs universitaires et de citoyens engagés.

L'examen de la cybersécurité a révélé trois tendances clés. Elles sont les suivantes :

Les efforts déployés par les organismes d'application de la loi pour lutter contre la cybercriminalité tout en assurant la protection de la vie privée dans le cyberespace sont vus d'un bon œil.

- Il est entendu que la cybersécurité sert à protéger les renseignements personnels et, par ricochet, la vie privée. Les Canadiens sont favorables aux efforts qui sont déployés pour protéger leurs renseignements personnels en ligne.
- Les Canadiens reconnaissent que les organismes d'application de la loi sont confrontés à des défis dans la lutte contre la cybercriminalité, et ils sont préoccupés par la menace croissante pour les particuliers, les organisations des secteurs public et privé et les gouvernements.

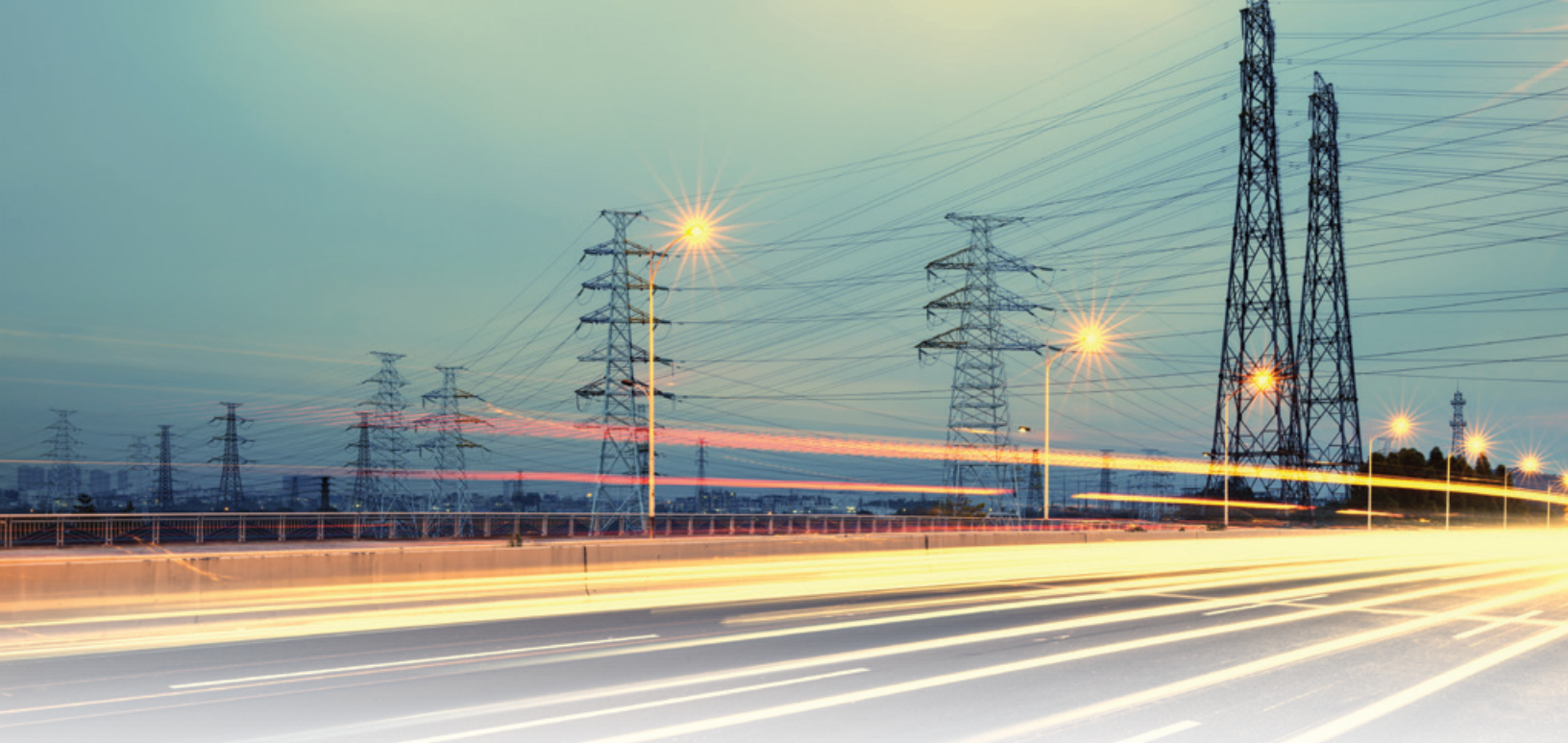
Il est grandement nécessaire d'améliorer les connaissances et les compétences sur la cybersécurité.

- Il faut améliorer les connaissances et les compétences en matière de cybersécurité des enfants, des aînés, des propriétaires de petites et moyennes entreprises, des organismes d'application de la loi et des hauts dirigeants d'entreprise.

- En raison de la pénurie de talents dans le domaine de la cybersécurité, il est difficile pour les organisations, y compris le gouvernement fédéral, d'attirer et de maintenir en poste les personnes dont elles ont besoin pour renforcer la cybersécurité ou pour contrer les cybermenaces.

Certains exigent un leadership fédéral solide dans le domaine de la cybersécurité.

- Les partenaires externes souhaitent l'établissement d'un point central fiable exerçant un leadership dans le domaine de la cybersécurité.
- Les partenaires veulent recevoir des messages, des conseils, et des directives uniformes de la part du gouvernement du Canada.
- Les organisations veulent que soient établies des normes ou des lois en matière de cybersécurité pour clarifier les exigences et les attentes qui les aideront à améliorer leur cybersécurité.
- Les intervenants veulent que le gouvernement fédéral exerce un leadership en matière de cybersécurité pour favoriser la collaboration nationale, orienter les investissements, faciliter l'échange d'information et protéger les droits et les libertés.



Sécurité et résilience

Contexte stratégique : l'évolution de la cybermenace

Les menaces auxquelles nous devons faire face dans le cyberespace sont complexes et en évolution rapide. Les gouvernements, les entreprises, les organisations et les Canadiens sont vulnérables. Étant donné que notre économie et nos services essentiels reposent de plus en plus à chaque année sur Internet, les enjeux sont considérables.

Cybercriminalité et cybermenaces avancées

PLes auteurs d'activités cybernétiques malveillantes sont très diversifiés, ont différents objectifs et disposent d'un vaste éventail de techniques. Les auteurs de cybermenaces malveillants comptent des pirates individuels et des menaces internes, des réseaux criminels, des États-nations, des organisations terroristes et des acteurs parrainés par des États. Les cyberattaques sophistiquées sont souvent difficiles à comprendre sur le plan technique et exigent des connaissances spécialisées approfondies.

Sécurité et résilience

Le risque d'être victime d'une cyberattaque touche toutes les organisations et toutes les personnes. Les victimes peuvent être ciblées individuellement ou dans le cadre d'une campagne visant des millions d'internautes. Les Canadiens stockent de plus en plus d'information en ligne, ce qui les rend de plus en plus attirants comme victimes pour les auteurs de cybermenaces. La capacité des organismes d'application de la loi du Canada de protéger les Canadiens contre ces acteurs, qui peuvent se trouver n'importe où dans le monde, est un défi de taille.

Les cyberactivités malveillantes sont souvent menées pour des gains monétaires. Par exemple, les courriels d'hameçonnage qui semblent provenir d'institutions financières peuvent tromper les utilisateurs et les amener à fournir leurs renseignements bancaires. Le déploiement d'un rançongiciel pour chiffrer des fichiers d'un appareil ou d'un système est un type de cyberactivité malveillante dans le cadre de laquelle le pirate demande un paiement pour rétablir l'accès. Les atteintes à la sécurité des données peuvent se traduire par un vol de données personnelles ou financières (numéro d'assurance sociale, renseignements de cartes de crédit) à partir des bases de données d'organisations; ces données sont par la suite vendues sur les marchés criminels à des fins de fraude, de vol d'identité et d'extorsion.

Les cyberacteurs malveillants, parfois appelés « hacktivistes », peuvent également être motivés par une cause précise : exposer un acte répréhensible, protester ou causer un embarras. Il peut aussi s'agir d'amateurs qui cherchent à prouver leurs compétences en piratage et à acquérir une notoriété.

Sur une plus grande échelle, les auteurs parrainés par des États nations ou des États ont la capacité de voler notre propriété intellectuelle ou des stratégies organisationnelles confidentielles afin de donner à leur propre économie un avantage concurrentiel.

Par ailleurs, certains États-nations conçoivent des cyberoutils avancés à des fins hostiles. Si la menace vise les ordinateurs essentiels aux systèmes gouvernementaux, aux infrastructures essentielles et aux institutions démocratiques, elle met en péril la sécurité nationale et la sécurité publique du Canada. Les organisations terroristes souhaitent aussi acquérir des cyberoutils avancés pour mener des attaques.

L'incidence croissante

Comme les cyberoutils malveillants deviennent de plus en plus accessibles et que les taux de cybercriminalité ne cessent d'augmenter, une menace réelle pèse sur la santé économique du Canada. Par ailleurs, étant donné qu'un plus grand nombre d'infrastructures essentielles du Canada peuvent être contrôlées à distance et que les services essentiels sont gérés en ligne, il existe un risque que les cyberincidents compromettent la sécurité nationale et la sécurité publique.

Sur le plan financier, les victimes de compromissions dans le cyberespace doivent non seulement assumer des coûts immédiats pour rétablir et restaurer leurs systèmes, mais également des coûts à long terme pour remplacer ou mettre à niveau leurs cybersystèmes, sans compter les coûts associés à la réputation. Bien que les entreprises en démarrage soient particulièrement vulnérables, la perte de propriété intellectuelle a contribué à la ruine financière d'entreprises de toutes les tailles.

APERÇU SUR LA CYBERCRIMINALITÉ : FRAUDES PAR COURRIEL

C'est la période de l'impôt; Mohsen présente sa déclaration en ligne. Quelques jours plus tard, il reçoit un courriel de quelqu'un qui prétend être un agent des services fiscaux; l'auteur du courriel indique qu'il manque des renseignements dans le dossier de Mohsen et lui demande de fournir immédiatement des renseignements personnels, y compris son adresse et son numéro d'assurance sociale, afin de compléter le dossier. Le message précise que le défaut de fournir ces données pourrait entraîner des peines sévères, voire une peine d'emprisonnement. Mohsen a des soupçons au sujet du courriel et, avant de fournir les renseignements, il consulte le site Web de l'Agence du revenu du Canada (ARC). Celui-ci indique que l'ARC n'envoie jamais de messages par courriel pour demander aux citoyens de fournir des renseignements personnels ou financiers. Mohsen se fie aux conseils de l'ARC, ne répond pas au courriel.

Sécurité et résilience

Les cyberincidents peuvent également être profondément perturbateurs. Ils peuvent miner la confiance des citoyens à l'égard du commerce électronique et des institutions gouvernementales. S'ils estiment que leur sécurité ou leurs renseignements personnels sont à risque, les utilisateurs pourraient remettre en question l'utilisation continue des technologies numériques.

L'Internet des objets (IdO) renvoie aux objets et aux appareils qui, par l'entremise d'une connexion Internet, communiquent les uns avec les autres et fournissent des services plus efficaces et plus personnalisés. L'IdO prend de l'ampleur rapidement, et on s'attend à ce que plus de 25 milliards d'appareils soient connectés d'ici 2020.

La connexion des appareils à Internet ouvre la voie à de nouveaux risques de cybersécurité. Les acteurs malveillants peuvent exploiter les lacunes en matière de cybersécurité pour perturber les services au moyen de campagnes de cyberattaques par déni de service distribué (DSD) ou pour obtenir un accès à un vaste éventail de systèmes ou de données personnelles. En octobre 2016, des millions d'appareils non sécurisés ont été utilisés pour surcharger le serveur de Dyn, entreprise responsable de l'infrastructure Internet, et mettre hors ligne des services et des sites Web couramment utilisés, et ce, à l'échelle internationale.

Comme l'innovation sur le plan numérique ne cesse de progresser et que de nouvelles technologies sont développées, la nature des cybermenaces ne cessera de changer. Par exemple, les technologies connectées à Internet sont de plus en plus populaires, des thermostats et des appareils médicaux comme les stimulateurs cardiaques aux voitures et aux systèmes qui gèrent nos infrastructures essentiels et nos services. Sans mesures de cybersécurité appropriées, les appareils branchés sont vulnérables au piratage à une

APERÇU SUR LA CYBERCRIMINALITÉ : RÉSILIENCE GRÂCE À L'ÉCHANGE D'INFORMATION

Beom-Jun travaille au département des technologies de l'information d'une grande institution financière. Il a remarqué qu'il y avait eu beaucoup de tentatives de piratage du système. Bien que ces tentatives aient été infructueuses, Beom Jun a décidé de transmettre les données techniques au Centre canadien de réponse aux incidents cybernétiques (CCRIC) à des fins d'analyse. Il sait que le CCRIC s'attend à ce que les organisations responsables des infrastructures essentielles, comme sa banque, signalent les incidents cybernétiques afin qu'il puisse informer d'autres secteurs et les partenaires internationaux des tendances et des menaces. Beom-Jun reconnaît que la collaboration du CCRIC avec les institutions financières telles que la sienne, permet d'assurer la cybersécurité des organisations sur lesquelles comptent les Canadiens.

échelle sans précédent. De même, beaucoup de Canadiens se fient au chiffrement pour protéger leurs communications et leurs données en ligne. Or, l'avènement de l'informatique quantique compromettra la sécurité du chiffrement traditionnel; ainsi, les Canadiens doivent disposer de solutions résistantes aux attaques quantiques. Une capacité de cybersécurité innovante et souple sera nécessaire pour suivre le rythme des changements.

A propos de l'examen de la Cybersécurité

Consultations publiques sur la cybersécurité

Ce que nous avons entendu

Le principal défi pour le Canada est le nombre croissant d'incidents qui causent du tort à l'économie et à la société, qu'il s'agisse de violations, de crimes, d'interruptions de services essentiels ou de destruction d'actifs corporatifs et nationaux.

La protection de la vie privée et la sécurité ne sont pas un jeu à somme nulle, et nous pouvons avoir les deux. Il n'y a pas de sécurité sans protection de la vie privée, et la liberté est tout aussi tributaire de la sécurité que de la protection de la vie privée.

Les organismes d'application de la loi canadiens doivent centraliser leurs ressources de lutte contre la cybercriminalité… La mise en place d'un guichet unique permettra aux entreprises de signaler la compromission de leurs systèmes, et les autorités pourront mener des enquêtes en matière de cybercriminalité et intervenir le cas échéant.

Objectifs de la Stratégie sur la cybersécurité

Des systèmes canadiens sécurisés et résilients

En collaborant avec les partenaires et en améliorant les capacités en matière de cybersécurité, nous pouvons mieux protéger les Canadiens contre la cybercriminalité, contrer les menaces en évolution et défendre les systèmes essentiels du gouvernement et du secteur privé.

Le gouvernement du Canada assurera et améliorera la cybersécurité à l'échelle des ministères et organismes fédéraux pour protéger les renseignements personnels des Canadiens qu'il détient, ainsi que la confidentialité, l'intégrité et la disponibilité des services essentiels pour les Canadiens.

Le gouvernement du Canada renforcera la capacité des organismes d'application de la loi de lutter contre la cybercriminalité. Il appuiera la coordination à l'échelle des organismes d'application de la loi et avec les partenaires fédéraux, provinciaux, territoriaux et internationaux. Il renforcera aussi la capacité d'enquête en matière de cybercriminalité et facilitera le processus de signalement des cybercrimes.

Les petites et moyennes organisations n'ont pas toujours les connaissances et les ressources requises pour mettre en œuvre des systèmes de cybersécurité, même si ces derniers procurent un avantage concurrentiel. Le gouvernement du Canada aidera ces organisations en améliorant l'accès aux systèmes de cybersécurité.

Afin de contrer les cybermenaces de plus en plus sophistiquées, le gouvernement du Canada examinera les moyens permettant d'utiliser ses

capacités informatiques poussées pour défendre les réseaux essentiels au Canada et dissuader les auteurs de cybermenaces étrangers.

Certains cybersystèmes, comme les réseaux électriques, les réseaux de communication ou les institutions financières, sont si importants que toute perturbation pourrait avoir de graves conséquences pour la sécurité publique et nationale. Le gouvernement fédéral collaborera avec les provinces, les territoires et le secteur privé pour déterminer les besoins en vue de protéger l'infrastructure numérique.

Innovation en matière de cybersécurité

Contexte stratégique : Élargir les frontières de la cybersécurité

L'innovation numérique est devenue le moteur de la croissance économique au XXIe siècle. La cybersécurité n'est pas seulement essentielle pour protéger les sources de l'innovation numérique du Canada, elle est devenue une source d'innovation en soi.

Nouveaux horizons du développement des technologies et des entreprises

La cybersécurité continue de stimuler l'innovation et les débouchés économiques au Canada. Elle représente 1,7 milliard de dollars du PIB du Canada et génère plus de 11 000 emplois bien rémunérés[1]. Comme on s'attend à ce que l'industrie de la cybersécurité augmente de 66 % d'ici 2021

1 International Data Corporation (IDC) Canada , "2016 Canadian ICT Predictions and Forecast: Digital Transformation and Disruption," décembre 2015 Information and Communications Technology Council (ICTC), "Critical Infrastructure in a Hyperconnected Economy," août 2016.

APERÇU SUR LA CYBERSÉCURITÉ : COMPÉTENCES POUR L'ÈRE NUMÉRIQUE

Marc est à la recherche d'un camp d'été pour ses filles. Il cherche un camp d'été original où ses filles peuvent acquérir de nouvelles compétences. Il trouve un programme d'été conçu pour aider les enfants à acquérir des compétences de base en codage, ce qui les outillerait pour créer des sites Web et développer leurs propres programmes. Marc encourage les filles à s'inscrire, ouvrant ainsi la porte à un nouveau passe-temps et à de nouvelles compétences intéressantes.

à l'échelle mondiale, des milliers d'autres emplois pourraient être créés pour les Canadiens au cours des années à venir[2]. Les gouvernements, le milieu universitaire et le secteur privé peuvent travailler ensemble pour créer de nouvelles possibilités, stimuler les investissements et favoriser la recherche et le développement de pointe.

Le Canada est déjà un chef de file de la recherche et du développement dans le domaine de la cybersécurité. Les percées dans la recherche en matière de cybersécurité ne profitent pas seulement aux entreprises de cybersécurité canadiennes, mais encore à l'ensemble de l'économie. Le gouvernement a un rôle à jouer pour appuyer les recherches avancées et aider les entreprises novatrices à redoubler d'efforts afin d'offrir les services et les technologies de cybersécurité sur le marché mondial.

Miser sur les avantages de la technologie numérique

La participation du Canada à la vie numérique a amené de nombreux avantages, a engendré une immense prospérité et a ouvert une nouvelle porte sur le monde. Les gouvernements, les entreprises et d'autres organisations jouent un rôle central dans la protection de ces avantages, en mettant en place des mécanismes de sécurité solides pour leurs plateformes, produits et services en ligne.

La cybersécurité ne peut être plus forte que son maillon le plus faible. Les petites et moyennes entreprises et, en réalité, beaucoup d'organisations au Canada, sont confrontées à des défis semblables à ceux que les grandes

2 Research and Markets, "Cyber Security Market – Global Forecast to 2021," août 2016.

APERÇU SUR LA CYBERSÉCURITÉ : RATIONALISER LA PRESTATION DES SERVICES

Stuart a été soulagé d'apprendre qu'il pourrait avoir accès à son compte du Régime de pensions du Canada (RPC) sur Internet, sans avoir à retenir un autre mot de passe. Il n'a qu'à se connecter à la page Web du RPC, cliquer sur l'icône de sa banque et rentrer ses renseignements. Il utilise les mêmes noms d'utilisateur et mot de passe que ceux de son compte de banque, étant donné que la banque est un partenaire de connexion pour les services en ligne du gouvernement du Canada. Stuart apprécie cet aspect pratique et, comme il fait confiance aux mesures de sécurité de la banque, il sait que ses renseignements sont protégés. Son fils, David, ne cesse de lui dire que ses données bancaires sont bien protégées tant qu'il utilise une connexion Wi-Fi sécurisée, comme le réseau protégé par un mot de passe qu'il utilise à la maison. Il semble que les pirates peuvent intercepter le trafic des services Wi-Fi non sécurisés, par exemple, dans un café-restaurant ou un aéroport.

entreprises doivent surmonter pour protéger leurs systèmes et leurs réseaux; mais, elles doivent le faire avec moins d'expertise et de ressources. Les gouvernements peuvent aider à corriger cette asymétrie, en fournissant des conseils et en améliorant l'accès aux renseignements sur la cybersécurité et aux outils connexes, ce qui aidera les organisations canadiennes des secteurs privé et public à adopter les technologies numériques.

Les connaissances individuelles sont vastes dans le domaine de la cybersécurité, qu'il s'agisse de culture numérique, de codage ou d'atténuation des menaces. Les initiatives mises en œuvre dans les collectivités, les écoles et les établissements postsecondaires aident les Canadiens à acquérir les compétences requises pour l'ère numérique. Le gouvernement du Canada apporte sa contribution en effectuant des investissements à long terme pour aider les Canadiens de toutes les sphères à acquérir l'éducation et l'expérience de travail dont ils ont besoin pour participer davantage à l'économie numérique.

La science et la technologie quantiques permettent de traiter et de protéger l'information de façon beaucoup plus rapide et sûre. Les appareils quantiques pourraient offrir des avantages révolutionnaires dans un éventail de domaines, par exemple, en aidant à comprendre comment les maladies se développent ou en optimisant les traitements médicaux. Si les algorithmes quantiques peuvent protéger l'information et repousser les limites de la technologie, ils constituent en même temps une menace pour les nombreuses formes de chiffrement utilisées aujourd'hui dans la protection des systèmes et des applications au Canada et dans le monde entier.

En raison des possibilités et des défis que représente l'informatique quantique, le Canada a déployé des efforts pour établir un bassin solide d'expertise et de spécialistes en informatique quantique, similaire à celui de l'Institute of Quantum Computing à la l'Université de Waterloo.

Perfectionner les compétences et les connaissances au XXIe siècle

La demande de spécialistes qualifiés en cybersécurité est soutenue. Une pénurie mondiale de professionnels qualifiés représente des débouchés immédiats et grandissants pour la main-d'œuvre hautement scolarisée du Canada. Nous pouvons encourager davantage d'étudiants à s'engager dans les domaines des sciences, des technologies, du génie et des mathématiques (STEM), ainsi que les diplômés des programmes STEM et d'autres disciplines (psychologie, sociologie ou gestion) à se spécialiser en acquérant les compétences nécessaires pour occuper des postes en cybersécurité. Il est essentiel que les gouvernements et les entreprises du Canada attirent ces talents multidisciplinaires, au pays et à l'étranger. Cela aide aussi à garantir que les entreprises canadiennes peuvent grandir et innover en toute sécurité tandis qu'elles utilisent de plus en plus la technologie numérique.

À mesure que l'environnement de cybersécurité continue d'évoluer, il y a un besoin constant d'avoir accès à des renseignements fiables et à jour. Les statistiques et les recherches canadiennes dans le domaine de la cybersécurité fourniront un portrait plus précis des enjeux en matière de cybersécurité auxquels notre nation fait face dans un contexte mondial. Ces

renseignements peuvent être utilisés par les universitaires, les chercheurs et les décideurs pour comprendre les tendances, gérer les risques, orienter les investissements futurs et rectifier le tir au besoin.

Consultations sur la cybersécurité

Ce que nous avons entendu

Nous devons veiller à ce que les entreprises en démarrage et les innovations conçues au Canada demeurent au Canada.

Le gouvernement fédéral peut jouer un rôle unique pour faire en sorte que les entreprises considèrent le Canada comme un pays où elles peuvent prospérer dans un cyberenvironnement sécuritaire.

Peu de gens apprécient la pertinence stratégique du renseignement en matière de cybersécurité. On ne peut pas gérer ce qu'on ne mesure pas.

Objectifs de la Stratégie sur la cybersécurité

Un écosystème du cyberespace novateur et adaptable

En appuyant les recherches avancées, en encourageant l'innovation numérique, en développant les compétences cybernétiques et en améliorant la sensibilisation, le gouvernement fédéral positionnera le Canada comme un chef de file mondial dans le domaine de la cybersécurité.

Le gouvernement du Canada travaillera avec les partenaires pour stimuler les investissements et encourager la recherche et le développement dans le domaine de la cybersécurité. Le gouvernement se concentrera sur les nouveaux domaines où le Canada fait preuve d'excellence, comme l'informatique quantique et les technologies de chaînes de blocs. Le gouvernement fédéral réalise déjà des progrès dans ce domaine et, dans le budget de 2017, il a annoncé la création d'une stratégie pancanadienne sur l'intelligence artificielle pour la recherche et les talents.

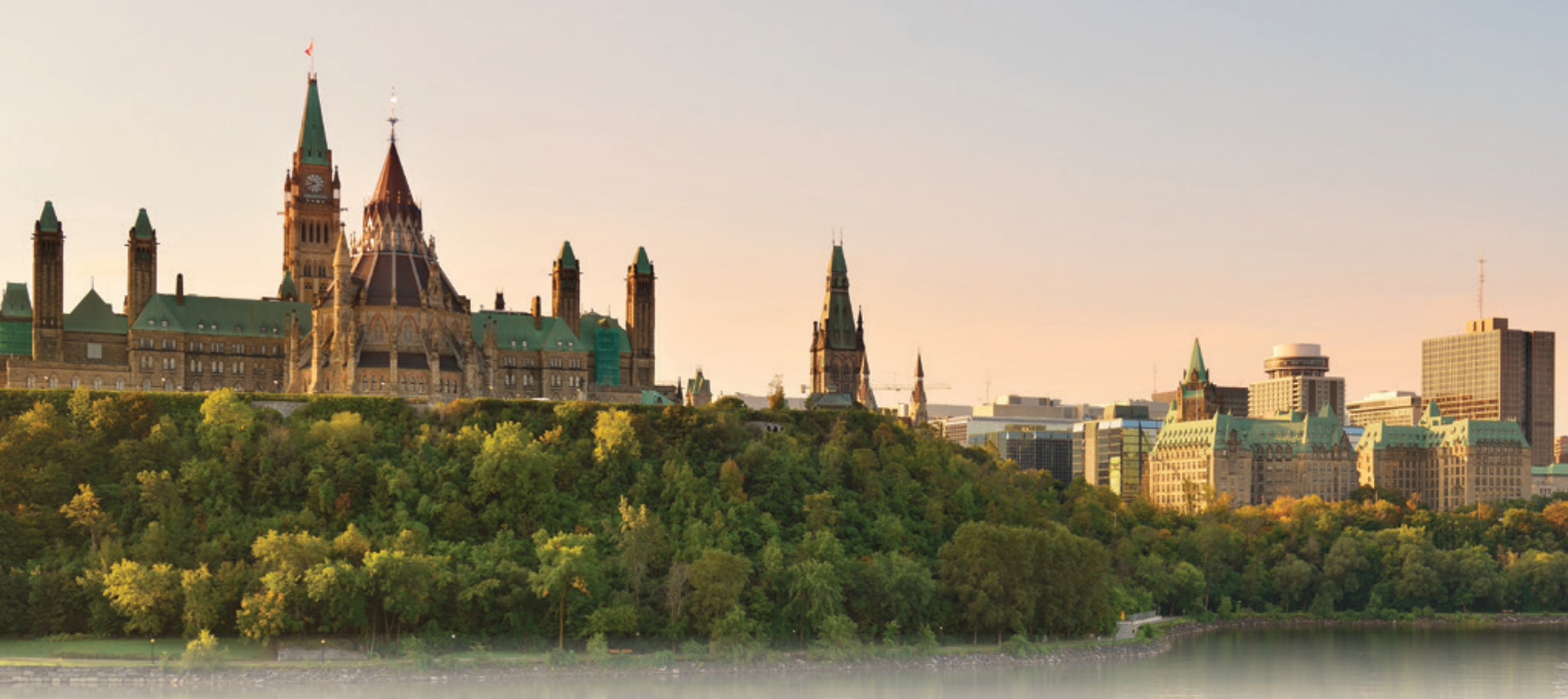
Ensemble, nous explorerons les initiatives permettant aux entreprises canadiennes d'offrir leurs produits sur le marché mondial. Le gouvernement explorera les initiatives qui aideront à stimuler la demande intérieure de technologies et de services en matière de cybersécurité.

Le gouvernement du Canada explorera de nouvelles idées pour renforcer la cybersécurité des entreprises et des Canadiens de tous les âges, et il a déjà engagé des investissements pour améliorer les compétences numériques chez les enfants, comme le codage.

Objectifs de la Stratégie sur la cybersécurité

La collaboration entre les gouvernements, le milieu universitaire et le secteur privé est nécessaire pour corriger les lacunes dans les compétences informatiques. En passant maintenant à l'action, nous pourrons former la main d'œuvre de demain, une main d'œuvre qui appuiera la cybersécurité et contribuera à la prospérité future du Canada.

La qualité de l'information dont nous disposons influence notre capacité de comprendre les tendances informatiques. Le gouvernement fédéral appuiera les efforts canadiens en matière de statistique et de recherche pour améliorer la compréhension collective à l'égard des menaces et des possibilités dans le cyberespace.



Leadership et collaboration

Contexte stratégique : Collaborer pour réaliser les avantages de la vie numérique

Les percées technologiques profitent à nos collectivités et à nos sociétés. Elles contribuent à la qualité de vie d'aujourd'hui, et contribueront largement à relever les défis de demain. Nous avons tous la responsabilité de protéger ces technologies. Dans le cadre de la Stratégie nationale de cybersécurité, le gouvernement du Canada fera progresser les efforts requis à cette fin.

Augmenter le niveau de cybersécurité de base au Canada

La grande majorité des systèmes numériques du Canada appartiennent à des particuliers et à des organisations de l'extérieur du gouvernement fédéral. Des particuliers qui utilisent quelques technologies aux férus de technologie qui sont fermement ancrés dans le monde virtuels, nombreux ne savent pas qu'ils peuvent être visés par des cybermenaces.

Par conséquent, ils ne prennent aucune mesure pour se protéger contre les cyberincidents et se rétablir le cas échéant. Même ceux qui sont conscients de l'importance de protéger leurs renseignements trouvent difficile de mettre en place des mesures abordables et efficaces.

Le gouvernement du Canada assume un rôle de premier plan dans le domaine de la cybersécurité afin d'aider les organisations et les Canadiens à comprendre l'importance de la cybersécurité et d'appuyer les efforts visant à augmenter le niveau de cybersécurité de base au Canada. Ceci complimente les efforts domestiques en travaillant avec nos partenaires internationales et alliés, tout en cherchant de réduire la menace des cybercriminels envers le Canada ainsi que les acteurs étatiques et leurs substituts qui veulent s'en prendre a nous.

De plus, le gouvernement fédéral vise l'excellence dans le domaine de la cybersécurité à l'échelle du pays. Pour réaliser cet objectif, il faudra améliorer et accroître les capacités de cybersécurité au gouvernement et dans l'industrie. Il faudra aussi appuyer les efforts en matière de recherche et de développement de pointe du Canada, ainsi que les nombreuses entreprises et organisations qui n'ont pas mis en place des mesures de cybersécurité solides. Les dirigeants du secteur privé auront un rôle central à jouer, puisque des efforts de collaboration sont requis afin que tous les Canadiens soient outillés pour prévenir et contrer les cybermenaces.

> **La technologie de chaînes de blocs** permet de créer des registres et des dossiers en ligne. Cette technologie qui est souvent associée à la monnaie virtuelle permet de nombreuses applications. Elle peut être utilisée pour fournir des services publics, comme la délivrance de passeports, la création de dossiers de contrats ou des documents

juridiques, ainsi que le traitement des paiements pour des services rendus. La technologie améliore l'efficacité en réduisant le temps de traitement des activités et le risque de fraude et de compromission, étant donné que personne ne peut modifier, supprimer ou joindre des dossiers.

Leadership fédéral en matière de cybersécurité dans un environnement dynamique

Le gouvernement du Canada est le mieux placé pour jouer un rôle de leadership dans le domaine de la cybersécurité, en raison de ses relations approfondies avec les secteurs privé et public, de son histoire de collaboration avec les provinces, les territoires et des représentants internationaux sur un éventail d'enjeux liés à la cybersécurité, et de ses capacités et son expertise avancée dans ce domaine.

Le leadership fédéral en matière de cybersécurité a été établi par l'entremise de la Stratégie de 2010 et des initiatives pancanadiennes qui y étaient prévues. Dans l'environnement de cybersécurité actuel, le gouvernement fédéral doit cependant approfondir la collaboration avec les partenaires afin de renforcer la cybersécurité du Canada. Des interventions concertées et intégrées de la part de toutes les parties sont nécessaires pour renforcer la cyberrésilience au Canada.

L'établissement d'un point de liaison clair au sein du gouvernement fédéral est l'un des moyens permettant au gouvernement de faire preuve de leadership tout en améliorant la capacité de collaboration avec les

partenaires. Le gouvernement fera de sorte que les partenaires reçoivent des conseils et des avis uniformes sur la cybersécurité et sachent à qui s'adresser pour obtenir de l'aide.

> **Les villes intelligentes** utilisent les technologies numériques pour améliorer la qualité de vie, en veillant à ce que les services soient plus efficaces et efficients et à ce qu'ils répondent aux besoins des résidents urbains. Par exemple, des feux de circulation « intelligents » adapteront le temps pour améliorer la circulation; les réseaux d'égouts détecteront les fuites et surveilleront les débits d'eau en temps réel.
>
> Pour accélérer le développement des villes intelligentes au Canada, le gouvernement fédéral a annoncé l'initiative Défi des villes intelligentes dans le cadre du budget de 2017.

Le gouvernement fédéral effectuera des investissements intelligents dans le domaine de la cybersécurité, tout en encourageant les partenaires du secteur privé et d'autres administrations à faire de même. Les organisations du secteur privé au Canada possèdent des capacités en matière de cybersécurité de calibre mondial, qui pourraient être utilisées au profit de tous les secteurs de l'économie canadienne. Nos écoles et nos établissements postsecondaires ont également d'excellentes idées et ils font preuve d'un leadership solide, atout majeur pour l'avenir de la cybersécurité au Canada.

Le gouvernement travaillera à réunir les efforts déployés à l'échelle pancanadienne pour renforcer les compétences en matière de cybersécurité, faire progresser les nouvelles solutions et assurer la cybersécurité. Nous pouvons être un exemple pour d'autres pays, en démontrant ce que nous pouvons accomplir grâce à une stratégie nationale de cybersécurité cohérente.

APERÇU SUR LA CYBERSÉCURITÉ : COLLABORER POUR RÉGLER LES PROBLÈMES DE CYBERSÉCURITÉ

Augustine a reçu une invitation a participer à Geek Week, un atelier annuel du Centre canadien de réponse aux incidents cybernétiques (CCRIC). Il avait participé à l'atelier de l'année dernière et avait apprécié son travail auprès de professionnels et d'universitaires du Canada et d'autres pays pour régler les problèmes en matière de cybersécurité. Augustine a compris que les compétences qu'il a acquises et les relations professionnelles qu'il a nouées dans le cadre de l'atelier ont été utiles pour son travail. À l'atelier de l'année dernière, son équipe avait mis à l'essai des outils prototypes du CCRIC pour mener une analyse automatisée de logiciels malveillants et de rançongiciels d'appareils mobiles, et avait examiné comment le chiffrement des données sur ces appareils peut être exploité par les pirates. Augustine est satisfait du fait que le travail de son équipe peut être utile dans le monde réel et que, par la suite, il a pu emporter les outils utilisés pour les améliorer.

A propos de l'examen de la Cybersécurité

Consultations publiques sur la cybersécurité

Ce que nous avons entendu

Le gouvernement du Canada peut assumer le rôle de leadership qui est nécessaire, en créant, en adoptant et en modélisant des pratiques exemplaires pour la cybersécurité, et en déployant des efforts pour transférer ces connaissances au secteur privé.

Il faudra mettre en place une structure de gouvernance plus sécurisée et un cadre de planification stratégique… pour les lois et les règlements modernes, et assumer un leadership pour déterminer, appuyer et diffuser les normes internationales les plus récentes de la technologie de cybersécurité.

Nous devons collectivement établir un cadre de gouvernance en matière de cybersécurité qui énonce les rôles et les responsabilités au sein du gouvernement et dans les secteurs public et privé.

Objectifs de la Stratégie sur la cybersécurité

Leadership, gouvernance et collaboration efficaces

En étroite collaboration avec les provinces, les territoires et le secteur privé, le gouvernement fédéral exercera un leadership pour améliorer la cybersécurité au Canada; en coordination avec les alliés, il travaillera à façonner l'environnement de cybersécurité international en faveur du Canada.

En répondant aux appels de leadership fédéral, le gouvernement du Canada rationalisera sa façon de faire et collaborera avec les partenaires et les intervenants externes, en créant un centre de liaison qui fournira des conseils éclairés et des instructions et interviendra en cas de cyberincident. Cette approche améliorera l'échange d'information de façon à ce qu'il soit plus facile pour le secteur privé d'obtenir l'aide dont il a besoin.

Le gouvernement du Canada renforcera les activités de sensibilisation publique et les efforts de mobilisation et établira de nouveaux forums de collaboration. Le gouvernement fédéral travaillera en collaboration avec un éventail d'intervenants canadiens pour améliorer collectivement la cybersécurité au Canada.

Le gouvernement fédéral dirigera, en partenariat avec les provinces, les territoires et le secteur privé l'élaboration d'un plan national visant à prévenir et à atténuer les cyberincidents, et à intervenir le cas échéant, un plan qui prévoit une coordination et des mesures efficaces.

Objectifs de la Stratégie sur la cybersécurité

Le gouvernement du Canada travaillera avec ses partenaires internationaux pour faire progresser les intérêts canadiens, ce qui comprend la promotion de services Internet ouverts, gratuits et sécurisés ainsi que la coopération internationale pour lutter contre la cybercriminalité.

Glossaire

Application

Outil qu'un utilisateur télécharge sur un appareil mobile (p. ex. une application de suivi de la condition physique).

Chaîne de blocs

Base de données à écriture seule répartie sur un réseau d'ordinateur reliés les uns aux autres et faisant appel à la cryptographie (encodage et décodage informatisés de renseignements) pour créer un registre public de transactions inviolable. La technologie de la chaîne de blocs est transparente, sûre et décentralisée, ce qui signifie qu'aucun intervenant ne peut modifier le registre public.

Commerce électronique

Achat ou vente de renseignements, de produits ou de services par Internet.

Cryptographie

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 résultant en cette nouvelle forme protégée fait référence au « chiffrement ». La conversion de l'information à sa forme originale est le « déchiffrement ».

Cyberattaque

Attaque qui suppose l'accès non autorisé à des renseignements électroniques ou à des appareils électroniques, à des systèmes informatiques et à des réseaux utilisés pour traiter, transmettre ou stocker cette information, ou encore leur utilisation, manipulation, interruption ou destruction (par voie électronique).

Cybercrime

Délit commis à l'aide d'un système informatique ou d'un réseau d'ordinateurs ou les impliquant directement. L'ordinateur ou ses données peuvent être la cible du délit ou l'ordinateur peut être l'instrument de perpétration du délit.

Cyberespace

Le monde électronique créé par les réseaux interreliés de la technologie de l'information et de l'information qui circule dans ces réseaux. Le cyberspace est un bien commun relient 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, réussie ou non, d'avoir accès à une ressource informatique ou à un réseau, de le modifier, de le détruite, de le supprimer ou de le rendre inutilisable.

Cybermenace

Acteur malveillant qui utilise Internet pour profiter d'une vulnérabilité connue afin d'exploiter un réseau et l'information qu'il contient.

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.

Déni de service distribué

Type d'attaque par déni de service dans le cadre de laquelle un attaquant se sert d'un code malicieux installé sur divers ordinateurs pour s'en prendre à une source unique.

Fuite de données

Divulgation non autorisée d'information qui met en danger la sécurité, la confidentialité ou l'intégrité de données permettant d'identifier une personne.

Hameçonnage ciblé, hameçonnage

Utilisation de faux courriels dans le but de persuader des membres d'une organisation de révéler leurs noms d'utilisateurs et leurs mots de passe. Contrairement à l'hameçonnage, qui nécessite l'envoi massif de courriels, l'hameçonnage ciblé se fait à petite échelle et est bien ciblé.

Informatique en nuage

Capacité d'accéder à l'ensemble des logiciels, des données et des ressources par l'entremise d'un réseau informatique plutôt qu'en utilisant le modèle traditionnel selon lequel ceux ci sont stockés localement sur l'ordinateur d'un utilisateur.

Informatique quantique

Un ordinateur quantique peut traiter un grand nombre de calculs simultanément. 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 qui sont essentiels pour assurer la santé, la sécurité et le bien être économique des Canadiens ainsi que le

fonctionnement efficace du gouvernement. Les infrastructures essentielles peuvent être autonomes ou interconnectées et interdépendantes dans les administrations provinciales, territoriales ou nationales ou entre celles ci. La perturbation des infrastructures essentielles pourrait donner lieu à des pertes de vie et à des répercussions économiques néfastes de même que considérablement ébranler la confiance du public.

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 un humain.

Internet des objets

L'interconnexion, au moyen d'Internet, de dispositifs informatiques intégrés dans des objets de tous les jours, ce qui leur permet d'envoyer et de recevoir des données.

Maliciel

Logiciel malicieux conçu pour infiltrer ou endommager un système informatique sans le consentement du propriétaire. Les formes courantes de maliciels sont les suivants : virus informatiques, vers, chevaux de Troie, logiciels espions et logiciels publicitaires.

Menace interne

Menace à une organisation qui vient de personnes de l'organisation, comme les employés, les anciens employés, les entrepreneurs ou les associés, qui détiennent de l'information privilégiée concernant les pratiques de sécurité de l'organisation, les données et les systèmes informatiques.

Pirate informatique

Personne qui se sert d'Internet et d'ordinateurs pour accéder sans permission à d'autres ordinateurs et à des serveurs.

Propriété intellectuelle

Selon l'Organisation mondiale de la propriété intellectuelle, la propriété intellectuelle désigne les inventions, les œuvres littéraires et artistiques, les dessins et emblèmes ainsi que les noms et images utilisés en affaires.

Rançongiciel

Logiciel qui bloque l'accès à vos données et ne les libère qu'une fois que vous avez versé de l'argent pour les récupérer

Villes intelligentes

Les villes intelligentes utilisent les technologies numériques pour accroître la qualité de vie en rendant les services plus efficaces, plus rentables et plus adaptés aux besoins des résidents de zones urbaines.