National Cyber Security Action Plan

2019-2024

Budget 2018 Investments

Public Safety Canada
Sécurité publique Canada

Canada

No de cat. : PS9-1/2019F-PDF
ISBN : 978-0-660-31468-6

TABLE DES MATIÈRES

MESSAGE DU MINISTRE

L'honorable Ralph Goodale
Ministre de la Sécurité publique et de la Protection civile

Chaque jour, les Canadiens sont en ligne – plus que partout ailleurs dans le monde – pour le travail, les loisirs, le magasinage, les transactions bancaires, les affaires, les nouvelles et pour rester en contact avec leurs proches. Cependant, la même infrastructure numérique qui améliore tellement notre qualité de vie peut aussi nous rendre vulnérables à ceux qui nous feraient du mal. Les cybermenaces contre les systèmes canadiens sont nombreuses et en croissance : des infrastructures critiques qui forment le fondement de l'économie canadienne jusqu'aux chaînes d'approvisionnement commerciales et les réseaux sociaux et les commodités personnelles, mettant ainsi les Canadiens en danger. La cybercriminalité au Canada provoque chaque année plus de trois milliards de dollars en pertes économiques.

Afin de mieux relever cet énorme défi contemporain, le gouvernement du Canada a mené une analyse cybernétique complète, à partir de 2016, qui comprenait la toute première consultation publique sur le sujet, s'enrichissant ainsi des perspectives de nombreux experts et intervenants clés des secteurs privé et public.

Cet examen a mené à la création de la nouvelle Stratégie nationale de cybersécurité du Canada, publiée en 2018, et à l'octroi de près de 1 milliard de dollars pour la cybersécurité dans les budgets fédéraux de 2018 et 2019. La Stratégie est élaborée pour être adaptable, en tenant compte de l'évolution constante du cyberespace. Elle reconnaît également que la demande de nouvelles solutions intelligentes en matière de cybersécurité créera d'excellents emplois et stimulera la croissance économique. Le budget de 2019 octroie 145 millions de dollars pour aider à protéger les cybersystèmes essentiels du Canada, y compris les systèmes de finances, de télécommunications, d'énergie et de transport. Le budget octroie également 80 millions de dollars sur quatre ans pour soutenir trois réseaux de cybersécurité canadiens ou plus partout au Canada qui seront affiliés à des institutions postsecondaires. Ces réseaux, choisis selon un processus concurrentiel, encourageront la recherche et le développement et créeront de nouveaux partenariats de commercialisation entre le milieu universitaire et le secteur privé.

La Stratégie comporte trois objectifs principaux : des systèmes canadiens sécurisés et résilients au sein du gouvernement et au-delà; un environnement cybernétique propice à la science, à l'innovation, au talent et à l'entrepreneuriat canadiens; et une solide collaboration nationale dans l'ensemble du pays, ce qui permettra au Canada de jouer un rôle de premier plan dans l'évolution des développements internationaux en matière de cybersécurité.

Ce document passe à la prochaine étape. Le Plan d'action national sur la cybersécurité (2019-2024) décrit les initiatives précises prévues pour les cinq prochaines années afin de réaliser la stratégie. Au gouvernement, dans le secteur privé et dans notre utilisation personnelle, le plan vise à donner aux Canadiens les moyens d'améliorer leur cybersécurité et de commercialiser leurs compétences et innovations cybernétiques pour le monde, ce qui créera des emplois bien rémunérés pour la classe moyenne et un Canada plus prospère.

INTRODUCTION

En tant que société ouverte sur le monde, nous sommes passés au numérique. Nous jouons, apprenons, socialisons, communiquons et faisons des affaires en ligne. En dépit de ses avantages considérables, l'économie numérique comporte d'importantes vulnérabilités qui peuvent être exploitées.

En 2010, le gouvernement du Canada (le gouvernement) lançait sa première Stratégie nationale de cybersécurité, un effort national de défense contre les cybermenaces. Autant l'économie numérique évolue, autant les cybermenaces se perfectionnent, ce qui exige de la stratégie qu'elle s'adapte au nouveau paysage. En 2016, nous avons franchi la première étape pour l'élaboration d'une nouvelle stratégie de cybersécurité. Nous avons lancé un examen exhaustif de la cybersécurité, qui comprenait la première consultation publique au Canada sur la cybersécurité et qui a permis de recueillir les points de vue et les conseils d'experts, d'intervenants clés et de citoyens mobilisés.

Lancée en 2018, la nouvelle Stratégie nationale de cybersécurité (la Stratégie) découle de l'examen de la cybersécurité. Elle est fondée sur le point de vue qu'une cybersécurité robuste est un élément essentiel de l'innovation et de la prospérité au Canada. De conception adaptable, la Stratégie tient compte de la constante évolution du cyberpaysage.

Avec cette nouvelle orientation stratégique, elle définit trois objectifs pour réaliser sa vision *de sécurité et de prospérité dans l'ère numérique*.

- **Des systèmes canadiens sécurisés et résilients** : Grâce à des capacités améliorées et en collaboration avec ses partenaires, le gouvernement pourra mieux protéger les Canadiens contre la cybercriminalité, combattre les menaces au rythme de leur évolution et défendre ses systèmes essentiels et ceux du secteur privé.
- **Un écosystème du cyberespace novateur et adaptable :** Le gouvernement appuiera la recherche de pointe, favorisera l'innovation numérique et développera des compétences et des connaissances cybernétiques afin de positionner le Canada comme chef de file mondial dans le domaine de la cybersécurité.
- **Leadership, gouvernance et collaboration efficaces :** En collaboration avec les provinces, les territoires et le secteur privé, le gouvernement jouera un rôle de chef de file pour améliorer la cybersécurité au pays; en coordination avec ses alliés, il travaillera à façonner l'environnement de cybersécurité international de manière avantageuse pour le Canada.

Le présent *Plan d'action national en matière de cybersécurité (2019-2024)* pour une nouvelle Stratégie nationale de cybersécurité au Canada est un plan détaillé pour la mise en œuvre de la Stratégie. Il décrit les initiatives et les jalons propres à chacun de nos trois objectifs et présente une feuille de route pour la façon dont nous réaliserons et nourrirons notre vision de la sécurité et de la prospérité à l'ère numérique. Financées dans le cadre du budget 2018 (507.7M sur 5 ans, et 108.8M en continu), ces initiatives représentent une première étape vers la réalisation de la vision. Comme la Stratégie est conçue pour être souple, on prévoit que d'autres initiatives pourraient être identifiées à mesure que le cyberespace continue d'évoluer.

Objectif 1

Des systèmes sécurisés et résilients

En collaboration avec nos partenaires et grâce à nos capacités améliorées en cybersécurité, nous pourrons mieux protéger les Canadiens contre la cybercriminalité, combattre les menaces au rythme de leur évolution et défendre les systèmes essentiels du gouvernement et du secteur privé.

Les cyberoutils malicieux de plus en plus accessibles et les taux de cybercriminalité qui ne cessent d'augmenter représentent une réelle menace pour la santé économique du Canada. De plus en plus d'infrastructures vitales et de services essentiels peuvent être contrôlés à distance ou gérés en ligne, et les cyberincidents risquent davantage de compromettre la sécurité publique nationale. En raison de ces dangers, le gouvernement intensifiera ses efforts pour aider les propriétaires et les exploitants d'infrastructures essentielles (IE) à réduire leurs risques en matière de cybersécurité. Pour ce faire, il sensibilisera davantage les propriétaires et les exploitants d'IE aux risques et aux vulnérabilités cybernétiques ainsi qu'aux mesures d'atténuation disponibles pour améliorer la résilience des

systèmes d'infrastructures essentielles. Le gouvernement renforcera également la capacité des organismes d'application de la loi à lutter contre la cybercriminalité en appuyant la coordination entre ces organismes et les partenaires FPT et internationaux. Le gouvernement renforcera les capacités d'enquête sur la cybercriminalité et rendra plus facile aux Canadiens de signaler les cybercrimes.

INITIATIVES

Appui aux propriétaires et exploitants canadiens d'infrastructures essentielles

Le ministère de la Sécurité publique et de la Protection civile adoptera une approche globale de gestion des risques qui permettra aux propriétaires et aux exploitants d'IE de mieux protéger leurs systèmes et leurs renseignements. Plus spécifiquement, le Ministère accroîtra sa capacité 1) d'effectuer des évaluations de la cybersécurité pour aider les organisations à reconnaître et à corriger les vulnérabilités de leurs cybersystèmes, par exemple au moyen d'un outil technique d'évaluation des réseaux; 2) de renseigner les intervenants du secteur sur les dernières menaces et tendances touchant la sécurité des systèmes de contrôle industriel (SCI) et d'offrir une formation technique pratique pour atténuer les risques et renforcer la résilience des SCI, notamment par la tenue de symposiums sur la sécurité des SCI; et 3) de coordonner et offrir des exercices en ligne pour la communauté des IE afin de tester et de développer les capacités individuelles et collectives à intervenir et à se rétablir en cas de cyberattaques.

Évaluation intégrée des menaces améliorée

Le nouveau Centre canadien pour la cybersécurité (le cybercentre), qui fait partie du Centre de la sécurité des télécommunications (CST), augmentera sa capacité à produire des évaluations stratégiques de toutes les sources de cybermenaces et à les contextualiser pour aider le gouvernement et les Canadiens à les comprendre dans leur complexité et leur évolution (p. ex. Le point sur les cybermenaces contre le processus démocratique du Canada en 2019). Une meilleure compréhension du paysage de la cybermenace par le gouvernement et les Canadiens permettra de meilleures interventions et un Canada plus sécurisé et plus résilient dans le cyberespace.

Préparer les communications gouvernementales aux progrès de l'informatique quantique

Dans le but de protéger la confidentialité des communications actuelles du gouvernement contre de futures attaques de l'informatique quantique, le CST mettra sur pied un projet de capacité provisoire en matière de sécurité quantique en collaboration avec d'autres ministères pour s'assurer que le matériel de chiffrement cryptographique classifié du gouvernement est adéquatement mis à jour.

Étendre la portée des conseils et des directives aux secteurs des finances et de l'énergie

Le cybercentre renforcera ses partenariats avec les propriétaires et les exploitants d'infrastructures essentielles dans les secteurs canadiens des finances et de l'énergie, ce qui permettra l'échange et le codéveloppement mutuellement avantageux de connaissances et de capacités uniques en matière de cybersécurité pour une meilleure défense contre les cybermenaces avancées.

Collecte de cyberrenseignements et l'évaluation des cybermenaces

Grâce au financement accru à l'appui de la Stratégie, le Service canadien du renseignement de sécurité (SCRS) accentuera le travail déjà accompli en matière de collecte de cyberrenseignements et l'évaluation des cybermenaces. Ses analyses permettront de mieux comprendre les cybermenaces de même que les intentions et les capacités des cyberacteurs actifs au Canada et à l'étranger qui constituent une menace pour la sécurité de notre pays. Cela permettra au gouvernement d'améliorer sa connaissance générale de la situation, de mieux déceler les vulnérabilités cybernétiques, de limiter ou de prévenir le cyberespionnage, le sabotage, l'ingérence étrangère, et autres cybermenaces, et de prendre des mesures pour sécuriser les infrastructures essentielles.

> *« 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 chaque année sur Internet, les enjeux sont considérables. (La Stratégie) »*

Unité nationale de coordination de la lutte contre la cybercriminalité

La Gendarmerie royale du Canada (GRC) mettra sur pied l'Unité nationale de coordination de la lutte contre la cybercriminalité (UNCLC) pour coordonner les opérations policières canadiennes contre les cybercriminels et pour établir un mécanisme national permettant aux Canadiens et aux entreprises de signaler les cybercrimes aux services de police.

L'UNCLC :

- coordonnera les opérations contre la cybercriminalité au Canada et collaborera avec des partenaires internationaux;
- fournira conseils et directives en matière d'enquête numérique aux services de police canadiens;
- produira des renseignements sur les cybercrimes donnant lieu à des poursuites pour les services de police canadiens;
- collaborera avec le Centre canadien pour la cybersécurité du CST;
- établira un mécanisme national de signalement public qui permettra aux citoyens et aux entreprises du Canada de signaler les cybercrimes et les cyberfraudes aux services de police.

Capacité d'application de la loi de la Police fédérale en matière de cybercriminalité

La GRC augmentera aussi sa capacité opérationnelle (enquêtes, renseignement, services d'enquêtes techniques spécialisées, présence internationale et expertises spécialisées en cybercriminalité) qui lui permettra de prendre des mesures fédérales d'exécution de la loi contre les activités cybercriminelles prioritaires, tant nationales qu'internationales. Plus particulièrement, la GRC :

- augmentera sa capacité à cibler les activités cybercriminelles;
- améliorera la cybercapacité spécialisée des équipes d'enquête fédérales et accroîtra sa capacité d'intervenir dans des enquêtes conjointement avec des partenaires internationaux clés canadiens de l'application de la loi;
- préviendra et détectera les menaces à la sécurité de la population et à la sûreté d'intérêts canadiens, et interviendra pour les neutraliser.

Objectif 1 Des systèmes sécurisés et résilients

Appui aux propriétaires et exploitants canadiens d'infrastructures essentielles

Ministère	Activités	Date cible	État
Sécurité publique Canada (SP)	Acquérir ou créer un outil technique de cyberévaluation	2019	Prévu
	Établir un comité consultatif sur les systèmes de contrôle industriel (SCI)	2019	Prévu
	Accroître le nombre d'exercices de cybersécurité offerts aux intervenants en infrastructures essentielles	2020	Prévu
	Élaborer une solution technique de formation et de sensibilisation à la sécurité des SCI	2020	Prévu

Évaluation intégrée des menaces améliorée

Ministère	Activités	Date cible	État
Centre de la sécurité des télécommunications (CST)	Rendre le CST plus apte à répondre à la demande croissante d'évaluations des cybermenaces	2024	En cours
	Rendre le CST capable d'évaluer un plus large éventail de cybermenaces tenant compte de la clientèle croissante du cybercentre	2024	En cours

Préparer les communications gouvernementales aux progrès de l'informatique quantique

Ministère	Activités	Date cible	État
Centre de la sécurité des télécommunications (CST)	Protéger les renseignements classifiés du gouvernement contre les progrès anticipés de l'informatique quantique	2024	En cours

Étendre la portée des conseils et des directives aux secteurs des finances et de l'énergie

Ministère	Activités	Date cible	État
Centre de la sécurité des télé-communications (CST)	Les secteurs financier et de l'énergie travaillent en collaboration avec le cybercentre et à l'intérieur de leur secteur respectif pour améliorer leur niveau de cybersécurité	2024	En cours
	Élever le niveau de cybersécurité dans les secteurs financier et de l'énergie	2024	En cours

Collecte de cyberrenseignements et l'évaluation des cybermenaces

Ministère	Activités	Date cible	État
Service canadien du renseignement de sécurité (SCRS)	Accroître la collecte de cyberrenseignements sur la sécurité nationale et l'évaluation des cybermenaces par le SCRS	2024	Prévu

Unité nationale de coordination de la lutte contre la cybercriminalité (UNCLC)

Ministère	Activités	Date cible	État
Gendarmerie royale du Canada (GRC)	Atteindre la capacité opérationnelle initiale	2020	En cours
	Créer le groupe consultatif de l'UNCLC	2021	En cours
	Lancer un système national de signalement public d'incidents de cybercriminalité et de cyberfraudes	2022	En cours
	Atteindre la capacité opérationnelle totale	2023	En cours

Capacité d'application de la loi de la Police fédérale en matière de cybercriminalité

Ministère	Activités	Date cible	État
Gendarmerie royale du Canada (GRC)	Déployer des cyberspécialistes à l'étranger	2020	En cours
	Établir et appuyer des équipes d'enquête sur la cybercriminalité	2021	En cours
	Recruter et former des spécialistes de la cybercapacité	2021	En cours

Objectif 2

Un écosystème du cyberespace novateur et adaptable

En appuyant la recherche de pointe, en favorisant l'innovation numérique et en développant des compétences et des connaissances cybernétiques, le gouvernement positionnera le Canada comme chef de file mondial de la cybersécurité.

La cybersécurité stimule de plus en plus l'innovation et l'activité économique au Canada. Les gouvernements, les universités et le secteur privé peuvent travailler ensemble pour créer de nouvelles occasions, stimuler l'investissement et encourager la recherche et le développement de pointe. De plus, la demande de professionnels qualifiés en cybersécurité représente un débouché immédiat et en croissance pour la main-d'œuvre hautement scolarisée du Canada.

Le gouvernement jouera un rôle de chef de file en appuyant la recherche de pointe et en aidant les entreprises novatrices à croître et à apporter les technologies et les services de cybersécurité sur le

marché mondial. Le gouvernement travaillera avec ses partenaires pour stimuler l'investissement et encourager la recherche et le développement dans le cyberespace. Il investira également dans des initiatives qui soutiennent le développement des compétences numériques afin de combler les lacunes des compétences cybernétiques et de former la main-d'œuvre de l'avenir.

INITIATIVES

Volet cybersécurité du programme de stages pratiques pour étudiants

Dirigée par le ministère de l'Emploi et du Développement social du Canada (EDSC), cette mesure fournira des ressources pour une composante du Programme de stages pratiques (PSP) pour étudiants en soutenant la création possible de 1 000 nouvelles occasions d'apprentissage intégré au travail (AIT) sur trois ans en cybersécurité.

Le Programme d'AIT appuie actuellement la création d'opportunités pour aligner les compétences des étudiants diplômés canadiens avec les besoins d'embauche des employeurs dans les industries en croissance. Les participants admissibles doivent être inscrits à des programmes en sciences, technologie, génie, et mathématiques (STGM) et de l'administration des affaires dans des établissements d'enseignement postsecondaire partout au Canada. Les AITs offrent aux étudiants de précieuses occasions de perfectionnement des compétences et peuvent faciliter une transition harmonieuse entre l'école et le marché du travail dès l'obtention du diplôme, et aider les employeurs à se constituer une réserve de talents pour leurs besoins d'embauche. Le Programme de stages pratiques appuie les partenariats de collaboration en rassemblant des employeurs et des établissements d'enseignement postsecondaire pour travailler de façons novatrice à l'harmonisation du perfectionnement des compétences en éducation avec les besoins des employeurs des secteurs clés et émergents de l'économie canadienne.

Le PSP offre aux employeurs des subventions salariales de 50 % pour chaque nouveau placement professionnel standard qu'ils créent (jusqu'à concurrence de 5 000 $ par placement). Cette subvention salariale est plus élevée, soit 70 % (jusqu'à concurrence de 7 000 $), pour les nouveaux placements créés pour les étudiants sous-représentés, y compris les femmes en STGM, les Autochtones, les personnes handicapées et les nouveaux arrivants, ainsi que les étudiants de première année.

Le volet de la cybersécurité du PSP sera axé sur l'augmentation du nombre de possibilités d'AIT pour les étudiants canadiens en cybersécurité afin de s'assurer que les jeunes Canadiens talentueux obtiennent leur diplôme avec l'éventail complet de compétences recherchées par les employeurs.

Évaluation et certification en cybersécurité pour les petites et moyennes entreprises

Les entreprises canadiennes, en particulier les petites et moyennes entreprises (PME), n'ont pas les mêmes capacités en cybersécurité que les grandes entreprises. Le programme volontaire de certification pour les entreprises aidera les participants à positionner leur avantage concurrentiel et à promouvoir la confiance dans l'économie numérique. Le programme de cybercertification s'adresse aux PME, qui représentent environ 98 % des entreprises au Canada.

Même s'il existe peu de normes en cybersécurité, le programme de cybercertification prévoit des exigences précises qui exigent la mise en œuvre de contrôles précis de la cybersécurité par des participants certifiés par un organisme de certification accrédité par une tierce partie afin d'assurer une application uniforme de mesures de protection qui démontreront que les entreprises certifiées sont dotées d'une sécurité de base. Ce programme a été conçu pour servir de point de départ à l'amélioration du niveau de cybersécurité des PME.

Le programme de cybercertification a pour but multiple et ultime d'élever le niveau de cybersécurité parmi les PME canadiennes, d'accroître la confiance des consommateurs dans l'économie numérique, de promouvoir la normalisation internationale et de mieux positionner les PME face à la concurrence mondiale. Cette initiative publique-privée est dirigée par Innovation, Sciences et Développement économique Canada (ISDE), en collaboration avec le Centre de la sécurité des télécommunications (CST), le Conseil canadien des normes (CCN) et des organismes de certification accrédités indépendants du secteur privé.

> *« 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 d'innovation numérique du Canada; elle est devenue une source d'innovation en soi. (La Stratégie) »*

Objectif 2 Un écosystème du cyberespace novateur et adaptable

Programme de stages pratiques en cybersécurité pour étudiants

Ministère	Activités	Date cible	État
Emploi et Développement social Canada (EDSC)	Lancement du Programme d'apprentissage intégré en milieu de travail pour étudiants	2019	Terminé
	Évaluation du Programme d'apprentissage intégré en milieu de travail pour étudiants	2021	Prévu

Évaluation et certification en cybersécurité pour les petites et moyennes entreprises

Ministère	Activités	Date cible	État
Innovation, Sciences et Développement économique (ISDE) en collaboration avec le CST et le CCN	Élaboration de contrôles de sécurité en collaboration avec le CST	2019	Terminé
	Lancement d'un outil d'éducation et de sensibilisation à la cybersécurité	2019	En cours
	Lancement d'un programme de cybercertification	2019	En cours
	Lancement d'une norme nationale sur la cybersécurité	2020	Prévu

Objectif 3

Leadership, gouvernance et collaboration efficaces

En collaboration étroite avec les provinces, les territoires et le secteur privé, le gouvernement jouera un rôle de chef de file pour améliorer la cybersécurité au pays, et, en coordination avec ses alliés, il travaillera à façonner l'environnement de cybersécurité international de manière avantageuse pour le Canada.

Le gouvernement fera preuve de leadership dans la promotion des intérêts du Canada en matière de cybersécurité au pays et à l'étranger, en assurant une collaboration accrue et une meilleure coordination des questions stratégiques de cybersécurité et de cybercriminalité parmi les intervenants, et en préconisant un Internet libre, ouvert et sécure. L'établissement d'un point de liaison pour la cybersécurité au sein du gouvernement, par l'entremise du nouveau Centre canadien

pour la cybersécurité, sera une manifestation de leadership, et le Canada fera en sorte que les partenaires reçoivent des conseils et des directives uniformes sur les questions de cybersécurité et de cybercriminalité. Le gouvernement s'efforcera d'accroître l'échange d'informations parmi les partenaires nationaux et internationaux, et de recueillir des données et des paramètres pertinents à l'appui de la prise de décisions fondées sur des données probantes.

INITIATIVES

Capacité en matière de politiques stratégiques sur la cybersécurité et la cybercriminalité

Avec son équipe améliorée des politiques stratégiques responsable de la cybersécurité et de la cybercriminalité, le ministère de la Sécurité publique et de la Protection civile sera mieux positionné pour appuyer la gamme élargie des fonctions à mettre en œuvre pour la nouvelle Stratégie nationale de cybersécurité. Cette initiative permettra d'assurer une coordination adéquate des questions stratégiques en matière de cybersécurité et de cybercriminalité parmi les intervenants internes et externes, permettra au Ministère d'entreprendre des travaux préliminaires pour combler les lacunes dans les données sur la cybersécurité et la cybercriminalité, et fournira les ressources nécessaires pour appuyer le Programme de coopération en matière de cybersécurité (PCCS) élargi.

En améliorant sa capacité en politiques stratégiques, le Ministère sera en meilleure position pour intégrer les recherches découlant des projets financés par le PCCS. Cela permettra de documenter les travaux prospectifs, d'élaborer des solutions stratégiques proactives pour les enjeux émergents et, pour le gouvernement, d'anticiper les tendances et les développements.

Programme de coopération en matière de cybersécurité

Le Programme de coopération en matière de cybersécurité (PCCS) est le seul programme gouvernemental de subventions et de contributions consacré aux projets de soutien visant à améliorer la sécurité des cybersystèmes du Canada. Il a été lancé à l'origine à titre de programme pilote et le budget de 2018 a prévu des fonds supplémentaires pour son renouvellement et son expansion. Le PCCS élargi sera conforme aux objectifs de la nouvelle Stratégie nationale de cybersécurité, ce qui lui permettra d'obtenir des résultats plus ambitieux à l'appui des trois objectifs de la Stratégie en mettant un accent particulier sur l'innovation et la recherche.

Le programme appuiera différents types d'intervenants, comme des établissements d'enseignement et de recherche, des petites et des moyennes entreprises et d'autres partenaires du secteur privé. Les projets financés dans le cadre du PCCS produiront des résultats considérables qui aideront les gouvernements, les entreprises et les citoyens canadiens à mieux prévoir les tendances, à s'adapter à un environnement en évolution et à demeurer à la fine pointe de l'innovation au chapitre de la cybersécurité. En appuyant les efforts de recherche canadiens, le PCCS contribuera à améliorer la compréhension collective du cyberespace et à améliorer la position économique du Canada.

Centre canadien pour la cybersécurité

Jusqu'à tout récemment, les capacités opérationnelles du gouvernement en cybersécurité étaient réparties entre différents ministères et organismes. Même si des mesures existaient pour optimiser la communication et la coordination, l'ambiguïté entourant les rôles et les responsabilités et la difficulté inhérente à la coordination des multiples décideurs constituaient un obstacle à la prestation de directives techniques rapides, efficaces, claires et fiables que les Canadiens attendent de leur gouvernement. Par conséquent, en octobre 2018, le gouvernement a créé le nouveau Centre canadien pour la cybersécurité (le cybercentre) en tant que composante du Centre de la sécurité des télécommunications (CST). Il s'agit d'une équipe gouvernementale unifiée d'experts techniques en cybersécurité qui constituera une source officielle et unique de conseils techniques, de directives, de services, de messagerie et de soutien pour les questions opérationnelles de cybersécurité pour le gouvernement, les propriétaires et exploitants d'infrastructures essentielles, le secteur privé et le public canadien. Les Canadiens disposeront donc d'un endroit stable et fiable vers lequel se tourner pour toutes les questions opérationnelles relatives à la cybersécurité. Le cybercentre fournira également une expertise en cybersécurité pour aider les organismes responsables à s'acquitter de leurs fonctions de base, notamment en collaborant avec l'UNCLC de la GRC et ses services policiers pour lutter contre la cybercriminalité.

Cadre stratégique international pour le cyberespace

Jusqu'à présent, la dimension internationale de la cybersécurité n'a pas été au centre des préoccupations au Canada, malgré le fait que de nombreuses menaces proviennent de l'étranger et que la cybersécurité soit un enjeu intrinsèquement transnational. Les États-Unis, le plus important partenaire économique et commercial du Canada, sont à l'avant-garde des efforts déployés contre les aspects internationaux de la cybersécurité et cherchent des alliés pour une collaboration étroite et significative à ces efforts. Le Cadre stratégique international pour le cyberespace d'Affaires mondiales

Canada (AMC) permettra au Canada de renforcer sa collaboration avec les États-Unis à mesure qu'il poursuivra la mise en œuvre de sa stratégie de cybersécurité, notamment en mettant du personnel en place à Washington. AMC créera aussi un groupe de travail international sur la cybercollaboration afin d'améliorer l'échange d'information et la coordination entre les organismes gouvernementaux qui se consacrent à la cybersécurité internationale. Cette initiative appuie le mandat d'AMC qui consiste à améliorer et à promouvoir le leadership du Canada dans un contexte mondial en évolution, notamment en faisant progresser les efforts visant à remplir plus efficacement les engagements du Canada au sein de l'Organisation du Traité de l'Atlantique Nord (OTAN) et d'autres organisations régionales, comme l'Organisation pour la sécurité et la coopération en Europe, l'Organisation des États américains et le Forum régional de l'ASEAN.

Collaboration bilatérale sur la cybersécurité et l'énergie

En prenant appui sur les forces et l'expertise actuelles, Ressources naturelles Canada (RNCan) améliorera sa capacité de collaborer avec les intervenants du secteur de l'énergie (p. ex. ministères fédéraux, provinces et territoires, industrie privée, États-Unis) en matière de cybersécurité et de protection des infrastructures énergétiques essentielles. Conçue comme un ensemble d'activités bilatérales, cette initiative facilitera l'amélioration de la communication et de la coopération bilatérales face à un environnement de cybermenaces de plus en plus envahissant et sophistiqué. Plus particulièrement, RNCan entend poursuivre des activités conjointes avec les États-Unis afin de renforcer la sécurité et la résilience du réseau électrique nord-américain intégré et des pipelines transfrontaliers. À cette fin, ces activités s'appuieront sur les piliers de la gestion des urgences – prévention, préparation, intervention et rétablissement – en contribuant à rendre les systèmes énergétiques plus sûrs et plus résilients, en développant et en renforçant les capacités de préparation aux cyberattaques du secteur énergétique et en établissant des mécanismes mixtes pour renforcer les capacités d'intervention et de rétablissement des entités gouvernementales et du secteur énergétique. En fin de compte, cette initiative permettra au Canada de mieux faire face aux menaces nationales et internationales qui pèsent sur les infrastructures énergétiques essentielles de notre pays et de les neutraliser.

Objectif 3 Leadership, gouvernance et collaboration efficaces

Capacité en matière de politiques stratégiques sur la cybersécurité et la cybercriminalité

Ministère	Activités	Date cible	État
Sécurité publique Canada (SP)	Recruter une équipe de politiques stratégiques	2022	En cours
	Procéder à un examen annuel de l'état d'avancement	2021-2024	Prévu
	Procéder à un examen de la gouvernance	2021	Prévu

Programme de coopération en matière de cybersécurité (PCCS)

Ministère	Activités	Date cible	État
Sécurité publique Canada (SP)	Procéder au lancement du PCCS renouvelé	2019	Prévu
	Effectuer le marketing du programme	2019	Prévu
	Lancer l'appel de propositions	2019	Prévu
	Décaisser les fonds du projet	2019	Prévu

Centre canadien pour la cybersécurité

Ministère	Activités	Date cible	État
Centre de la sécurité des télé-communications (CST)	Procéder au lancement virtuel du Centre canadien pour la cybersécurité (le cybercentre)	2018	Terminé
	Réaliser la capacité opérationnelle de base	2022	En cours
	Réaliser la pleine capacité opérationnelle	2023	En cours

Cadre stratégique international pour le cyberespace

Ministère	Activités	Date cible	État
Affaires mondiales Canada (AMC)	Procéder au lancement d'un groupe de travail international sur la cybercollaboration	2018	Terminé
	Créer une équipe cybernétique à Affaires mondiales Canada	2019	Terminé
	Élaborer une cyberstratégie internationale	2019	En cours
	Travailler au renforcement des capacités liées à la cybersécurité	2019	En cours
	Élaborer une politique d'attribution	2019	Terminé
	Créer et pourvoir des postes à la mission de Washington	2020	En cours
	Tenir des réunions pertinentes sur la cybersécurité	2024	En cours
	Soutenir les participants internationaux dans les négociations en cybersécurité	2024	En cours
	Promouvoir les valeurs et les intérêts canadiens en ce qui a trait aux enjeux liés au cyberespace dans les instances internationales	2024	En cours

Collaboration bilatérale sur la cybersécurité et l'énergie

Ministère	Activités	Date cible	État
Ressources naturelles Canada (RNCan)	Recruter du personnel de base pour l'équipe de collaboration bilatérale	2019	En cours
	Lancer un premier appel à déclarations d'intérêt et à propositions de projets	2019	Terminé
	Signer des accords de contribution et décaisser des fonds pour les projets de première ronde	2019	En cours
	Au besoin, lancer un deuxième appel à déclarations d'intérêt et à propositions de projets	2020	Prévu
	Signer des accords de contribution et décaisser des fonds pour les projets de deuxième ronde (le cas échéant)	2020	Prévu
	Participer à des activités clés d'échange de renseignements, à des ateliers et à des séances d'information avec le gouvernement des États-Unis	2023	En cours
	Faire progresser des initiatives conjointes avec les partenaires américains sur la cybersécurité et l'énergie (p. ex. exercices de simulation, R-D, échange de renseignements)	2023	En cours

CONCLUSION

Le Plan d'action est un plan de mise en œuvre détaillé de la Stratégie. La cybersécurité est une responsabilité partagée, et nous sommes déterminés à travailler en étroite collaboration avec d'autres ordres de gouvernement, le secteur privé, des partenaires internationaux et les citoyens canadiens pour nous adapter au cyberespace au fur et à mesure de son évolution. En travaillant ensemble, nous serons mieux à même de bâtir un Canada sûr et prospère à l'ère numérique.