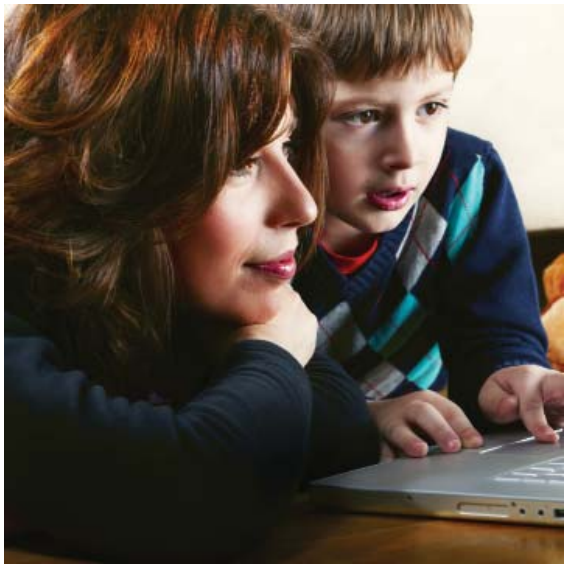
Gouvernement du Canada | Government of Canada



Plan d'action 2010-2015
de la Stratégie de cybersécurité du Canada

Canada

No de cat. : PS9-1/2013F-PDF
ISBN : 978-0-660-20521-2

Introduction

La technologie de l'information est très implantée dans nos vies quotidiennes. En fait, en tant que société, nous avons pris le tournant numérique. Nous jouons, nous apprenons, nous socialisons, nous communiquons et nous faisons des affaires en ligne. Les avantages du cyberespace sont nombreux, mais notre dépendance accrue vis-à-vis de cet environnement contribue tout de même à développer de nouvelles et importantes vulnérabilités.

Conformément à l'engagement qu'a pris le gouvernement du Canada (le gouvernement) d'assurer la sécurité, la protection et la prospérité du pays, nous avons lancé, le 3 octobre 2010, *la Stratégie de cybersécurité du Canada* (la Stratégie) afin d'orienter les efforts du gouvernement visant à assurer la sécurité de tous les Canadiens en ligne.

La Stratégie repose sur trois piliers :

- Sécuriser les systèmes du gouvernement;
- Nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral;
- Aider les Canadiens à se protéger en ligne .

Le présent document, le *Plan d'action 2010-2015 de la Stratégie de cybersécurité du Canada* (le Plan d'action), explique de façon générale comment le gouvernement compte mettre sa stratégie en œuvre et respecter son objectif final visant à sécuriser le cyberespace pour les Canadiens et pour l'économie du pays.

Des progrès considérables ont été réalisés jusqu'à maintenant en ce qui a trait à la mise en œuvre de la Stratégie. Le gouvernement a déjà accompli de nombreuses activités, notamment :

- En 2011, le gouvernement a créé Services partagés Canada (SPC) afin de simplifier sa façon de gérer les télécommunications de la de la technologie de l'information (TI) au fédéral, les centres de données et les points d'accès à Internet. En regroupant ces activités au sein de SPC, nous avons accru la sécurité de nos infrastructures de la TI.

- En 2011, le gouvernement a clarifié les rôles et les mandats du Centre de la sécurité des télécommunications Canada et du Centre canadien de réponse aux incidents cybernétiques (CCRIC), qui relèvent de Sécurité publique Canada (SP), afin d'accroître la capacité du Canada de cerner, de prévenir et d'atténuer les incidents de cybersécurité.

- En 2011, le gouvernement a lancé sa campagne nationale de sensibilisation publique sur la cybersécurité, pensez cybersécurité, afin de fournir aux Canadiens l'information dont ils ont besoin pour se protéger et protéger leur famille en ligne.

- En 2012, le gouvernement a annoncé que des fonds additionnels seraient dégagés afin de renforcer les infrastructures de la TI essentielles à la protection de l'information des Canadiens et de l'information qui sous-tend la sécurité nationale, la sécurité publique et la prospérité économique du Canada. Ces fonds servent à renforcer les infrastructures numériques du Canada qui sont déjà sûres, stables et résilientes.

- En 2012, le Canada et les États-Unis ont signé un *Plan d'action sur la cybersécurité*, dans le cadre du *Plan d'action Par-delà la frontière*, et ce, dans le but d'accroître le partenariat et la coopération déjà solides entre ces deux pays dans le domaine de la cybersécurité. Ce plan d'action permet de reconnaitre l'importance de protéger les infrastructures numériques essentielles communes au Canada et aux États-Unis et d'accroître notre capacité d'intervenir en cas d'incidents cybernétiques.

- En 2012, le gouvernement a annoncé avoir conclu un nouveau partenariat entre SP et le groupe STOP.THINK. CONNECT.™, une coalition d'entreprises du secteur privé et d'organisations gouvernementales et sans but lucratif, dont le département américain de la Sécurité intérieure. Ce partenariat permettra de faciliter l'harmonisation des campagnes de sensibilisation du public au Canada et aux États-Unis, et de donner des conseils et des outils importants au public pour accroître sa sécurité en ligne.

- Le Canada collabore également avec nos autres partenaires clés en matière de sécurité, à savoir le Royaume-Uni, l'Australie et la Nouvelle-Zélande, pour s'assurer à ce que nos activités nationales et internationales restent complémentaires. Le Canada travaille activement à faire valoir ses intérêts dans le domaine de la cybersécurité dans les principales tribunes internationales, y compris l'OTAN, le G8 ainsi que les Nations Unies et les organismes qui y sont associés. Enfin, le Canada continue de mener des activités d'intervention directe afin d'échanger de l'information et des connaissances dans le but de renforcer les capacités de ses partenaires étrangers en matière de cybersécurité.

- De façon continue, le gouvernement mobilise les secteurs des infrastructures essentielles (p. ex. les finances, les transports et l'énergie), qui sont interreliés et géographiquement dispersés dans toute l'Amérique du Nord. Pour aller de l'avant avec une approche intégrée dans cette grande communauté d'intervenants, en 2010, SP et les partenaires provinciaux et territoriaux ont lancé la *Stratégie nationale et le plan d'action sur les infrastructures essentielles*. De pair avec la Stratégie, cette stratégie définit un plan national pour s'assurer que les secteurs des infrastructures essentielles du Canada peuvent réagir et se rétablir rapidement en cas d'attaques et de perturbations, y compris les incidents cybernétiques.

- Enfin, le gouvernement a aussi pris des mesures afin d'améliorer la collaboration entre les ministères et les organismes qui travaillent activement à l'amélioration de la cybersécurité. Sous la direction de SP, de nouveaux instruments de gouvernance ont été mis en place grâce à un certain nombre de comités interministériels composés de cadres supérieurs.

Par ce plan d'action, le gouvernement démontre sa détermination à faire pleinement face aux cybermenaces en prenant des mesures ciblées visant à produire des résultats considérables et concrets.

Le gouvernement continue de travailler avec ses partenaires des provinces et des territoires, du secteur privé et du reste du monde afin d'améliorer la cybersécurité collective de ses citoyens. Il s'agit là d'une question d'envergure nationale pour laquelle nous avons tous une part de responsabilité, étant donné la nature interreliée de nos systèmes et réseaux.

Améliorer la gouvernance

De nombreux ministères et organismes ont travaillé ensemble pour élaborer la Stratégie. Considérant que gouvernement collabore avec des partenaires clés à la mise en œuvre de la Stratégie, il doit s'assurer que les ministères et les organismes travaillent de manière efficace et efficiente au renforcement de la cybersécurité au Canada.

Parmi les ministères et organismes concernés, notons :

- Forces canadiennes;
- Service canadien du renseignement de sécurité;
- Conseil de la radiodiffusion et des télécommunications canadiennes;
- Centre de la sécurité des télécommunications Canada;
- Recherche et développement pour la Défense Canada;
- Affaires étrangères et Commerce international Canada;
- Défense nationale;
- Industrie Canada;
- Ministère de la Justice Canada;
- Bureau du Conseil privé;
- Sécurité publique Canada;
- Gendarmerie royale du Canada;
- Services partagés Canada;
- Secrétariat du Conseil du Trésor.

Mesure	Calendrier	Résultats escomptés	État	Responsable
Améliorer la gouvernance				
Assurer un leadership et la coordination dans l'ensemble du gouvernement afin de concentrer les programmes et les ressources en matière de cybersécurité.	Début : 2010	Présenter la *Stratégie de cybersécurité du Canada*.	Terminé	Sécurité publique Canada
		Mettre en œuvre la *Stratégie de cybersécurité du Canada*.	En cours	Sécurité publique Canada

Mesure	Calendrier	Résultats escomptés	État	Responsable
Améliorer la gouvernance (suite)				
Améliorer la gouvernance dans le domaine de la cybersécurité au sein du gouvernement.	Début : 2010	Mettre en place des mécanismes interministériels de gouvernance de la cybersécurité.	Terminé	Sécurité publique Canada
		Appuyer ces mécanismes interministériels de gouvernance.	En cours	Sécurité publique Canada
	Début : 2011	Établir une structure de gouvernance de la sécurité du gouvernement du Canada qui consiste en un Comité directeur des organismes de sécurité et de divers groupes de travail.	Terminé	Secrétariat du Conseil du Trésor
		Appuyer la structure de gouvernance de la sécurité du gouvernement du Canada.	En cours	Secrétariat du Conseil du Trésor
Améliorer la collaboration au sein de la collectivité juridique fédérale à propos de la cybersécurité.	Début : 2011	Mettre en place et assurer le fonctionnement d'un Groupe de pratique sur la cybersécurité au ministère de la Justice.	En cours	Ministère de la Justice Canada
Fournir au gouvernement des méthodes opportunes et pertinentes pour mesurer l'efficacité des efforts déployés dans le cadre de la *Stratégie de cybersécurité du Canada*.	Début : 2012	Élaborer une stratégie horizontale de mesure du rendement.	Terminé	Sécurité publique Canada
		Évaluer la *Stratégie de cybersécurité du Canada*.	En bonne voie pour 2015	Sécurité publique Canada

Pilier 1
Protéger les systèmes gouvernementaux

Le gouvernement est chargé d'assurer la sécurité de l'information des personnes et des entreprises qui est contenue dans ses bases de données informatiques. Il fournit des services aux Canadiens et au secteur privé par l'entremise de ses sites Web et de ses systèmes électroniques de traitement, et il transmet de l'information hautement classifiée qui est essentielle à nos opérations militaires et à la sécurité nationale.

Les cyberattaques visent toute une gamme de réseaux informatiques, dont les systèmes du gouvernement. De plus, les auteurs de ces attaques testent régulièrement les systèmes pour en détecter les vulnérabilités. Par conséquent, la protection de ces systèmes et des données qu'ils contiennent relève de la sécurité nationale et la souveraineté de notre pays.

Le gouvernement considère comme prioritaire la protection des renseignements privés des Canadiens en ligne et de ses infrastructures de la TI. Il a donc mis en place des mesures visant à assurer aux Canadiens un accès sécuritaire en ligne pour ses services, qui deviennent de plus en plus nombreux. Il travaille également à consolider ses infrastructures de la TI afin d'en accroître davantage la sécurité.

Enfin, le gouvernement s'efforce de renforcer sa capacité à déceler et à empêcher les incidents cybernétiques, ainsi qu'à se défendre contre ceux-ci, tout en déployant des technologies cybernétiques visant à faire avancer les intérêts du Canada en matière d'économie et de sécurité nationale.

Mesure	Calendrier	Résultats escomptés	État	Responsable
Secure Government Systems				
Consolider l'architecture du gouvernement en matière de sécurité de la TI afin d'accroître la sécurité de ses réseaux.	Début : 2011	Créer Services partagés Canada pour consolider le réseau numérique du gouvernement.	Terminé	Travaux publics et Services gouvernementaux Canada
		Élaborer et appliquer de nouvelles normes de sécurité visant l'acquisition, pour le gouvernement, de nouveaux produits et services de la TI.	Terminé	Services partagés Canada, Travaux publics et Services gouvernementaux Canada, et Centre de la sécurité des télécommunications Canada
Mettre en place un mécanisme visant à prévenir les attaques complexes contre les réseaux du gouvernement, et à les aborder.	Début : 2011	Créer et assurer le fonctionnement d'un Centre d'évaluation des cybermenaces au Centre de la sécurité des télécommunications Canada.	Pleinement fonctionnel	Centre de la sécurité des télécommunications Canada
Réaliser des investissements afin d'accroître les capacités du gouvernement en matière de cybersécurité.	Début : 2011	Investir 155 millions de dollars sur quatre ans pour engager de nouveaux employés et améliorer l'équipement.	En bonne voie pour l'hiver 2016	Divers ministères
	Début : 2012	Élaborer une conception d'architecture d'entreprise pour la sécurité de la TI afin de s'assurer que les éléments de base de la sécurité seront présents quand l'infrastructure de la TI du gouvernement sera renouvelée.	En cours	Secrétariat du Conseil du Trésor (en collaboration avec Services partagés Canada et le Centre de la sécurité des télécommunications Canada)
	Début : 2012	Doter l'ensemble du gouvernement d'une nouvelle capacité de rétablissement en cas d'incident touchant la sécurité de la TI afin de veiller à ce qu'il soit en mesure de faire face à ces incidents et de se rétablir après coup.	En cours	Secrétariat du Conseil du Trésor, Services partagés Canada, Centre de la sécurité des télécommunications Canada
	Début : 2012	Accroître la capacité de recueillir et d'analyser du renseignement.	En cours	Centre de la sécurité des télécommunications Canada
	Début : 2012	Améliorer la capacité de détecter les cybermenaces et de se défendre contre ces menaces.	En cours	Centre de la sécurité des télécommunications Canada
Renforcer les aspects militaires de la cybersécurité.	Début : 2010	Renforcer la capacité de défendre les réseaux des Forces canadiennes et du ministère de la Défense nationale.	En cours	Ministère de la Défense nationale, Forces canadiennes
		Créer un Groupe de travail sur la cybernétique des Forces canadiennes et une organisation cybernétique des directeurs généraux.	Terminé	Ministère de la Défense nationale, Forces canadiennes
		Échanger de l'information sur les pratiques cybernétiques exemplaires avec les forces armées alliées.	En cours	Ministère de la Défense nationale, Forces canadiennes
Améliorer le plan du gouvernement visant à intervenir efficacement en cas d'incident cybernétique majeur.	Début : 2009	Passer en revue le Plan de gestion des incidents en matière de technologie de l'information du gouvernement.	Terminé	Secrétariat du Conseil du Trésor
Améliorer la formation et les mesures de sensibilisation sur la sécurité dans l'ensemble de la collectivité gouvernementale du domaine de la sécurité.	Début : 2010	Diriger et animer, pour la collectivité gouvernementale du domaine de la sécurité , diverses activités, tribunes et initiatives relative à de la formation.	En cours	Secrétariat du Conseil du Trésor

Pilier 2
Nouer des partenariats pour protéger les cybersystèmes essentiels à l'extérieur du gouvernement fédéral

La prospérité économique du Canada et la sécurité des Canadiens dépendent du bon fonctionnement de systèmes qui ne relèvent pas du gouvernement fédéral. Le secteur privé du Canada exploite un grand nombre de ces systèmes, et il est le gardien de renseignements de nature délicate et de systèmes de contrôle industriel desquels dépendent la sécurité nationale et publique du Canada.

De plus, pour assurer la viabilité de son succès, le secteur privé se fie en grande partie à sa capacité de commercialiser ses travaux de recherches de pointe et sa propriété intellectuelle, ses opérations commerciales et ses données financières. L'incapacité des entreprises concernées d'assurer la sécurité de cette information numérique essentielle et des systèmes dans lesquels elle est conservée se solderait inévitablement en une perte de parts de marché et de clients, et en l'échec des entreprise en question. À une échelle nationale, le vol de secrets industriels, de propriété intellectuelle et de renseignements confidentiels des entreprise pourrait entraîner des pertes d'emploi et un recul de la prospérité du Canada et des Canadiens.

Les risques et conséquences liés aux cyberattaques sont en grande partie les mêmes pour le gouvernement et le secteur privé. Heureusement, les secteurs public et privé du Canada collaborent depuis longtemps à la réalisation des objectifs communs en matière de sécurité économique et nationale. Cette coopération doit être encore plus renforcée.

Il est particulièrement important de solidifier les partenariats entre tous les paliers de gouvernement pour offrir au Canada et aux Canadiens une stratégie complète de cybersécurité. Nos homologues provinciaux et territoriaux fournissent toute une gamme de services essentiels dont la livraison dépend d'un bon fonctionnement, en toute sécurité, de leurs systèmes cybernétiques.

La perturbation des infrastructures essentielles et des systèmes cybernétiques peut avoir des répercussions directes sur les entreprises et les collectivités de partout dans le monde. Une attaque lancée contre des réseaux cybernétiques interreliés peut avoir un effet en cascade dans les secteurs industriels et ce, sans considération des frontières nationales. En même temps, le Canada doit rester actif dans les forums internationaux qui portent sur la protection des infrastructures essentielles et la cybersécurité.

Mesure	Calendrier	Résultats escomptés	État	Responsable
Collaborer avec des partenaires à l'extérieur du gouvernement du Canada				
Élaborer un nouveau processus de coordination d'intervention à l'échelle nationale en cas d'incident cybernétique majeur.	Début : 2012	Élaborer un Cadre de gestion des incidents cybernétiques.	En bonne voie pour l'automne 2013	Sécurité publique Canada
Mobiliser les propriétaires et exploitants des infrastructures essentielles du Canada au moyen des mécanismes établis dans le cadre de la Stratégie nationale et du plan d'action sur les infrastructures essentielles.	Début : 2010	Fournir des séances d'information sur la cybersécurité à tous les réseaux sectoriels.	En cours	Sécurité publique Canada
	Début : 2013	Élaborer et mettre en œuvre une stratégie visant à mobiliser les premiers dirigeants dans le domaine de la cybersécurité.	En bonne voie pour le printemps 2013	Sécurité publique Canada
Mobiliser les provinces et les territoires afin qu'ils participent activement à l'amélioration de la cybersécurité de leurs systèmes et des systèmes essentiels qui relèvent de leur compétence.	Début : 2011	Créer le Comité des sous-ministres adjoints fédéraux, provinciaux, territoriaux sur la cybersécurité.	Terminé	Sécurité publique Canada
		Obtenir des habilitations de sécurité pour le Sous-comité des dirigeants principaux de l'information sur la protection de l'information auquel participent des représentants des provinces et des municipalités, et fournir à ces personnes des séances d'information classifiées.	Terminé	Sécurité publique Canada
		Élaborer et mettre en œuvre des arrangements et des protocoles d'échange de l'information.	En cours	Sécurité publique Canada
	Début : 2001	Assurer le fonctionnement d'un comité FPT de coordination du Groupe de travail des cadres supérieurs sur la cybercriminalité	En cours	Ministère de la Justice Canada
Élaborer un Programme de partenariat en matière de cybersécurité relatif aux cybersystèmes essentiels à l'extérieur du gouvernement fédéral afin d'offrir un soutien concret à leurs propriétaires et exploitants.	Début : 2010	Organiser des ateliers partout au pays pour accroître la sensibilisation et la compréhension sur les menaces contre les systèmes de contrôle industriel.	En cours	Sécurité publique Canada et Gendarmerie royale du Canada
		Établir un programme et un environnement de mise à l'essai pour les systèmes de contrôle industriel – Centre d'essai national sur l'infrastructure énergétique.	Terminé	Sécurité publique Canada, Ressources naturelles Canada, Gendarmerie royale du Canada et Recherche et développement pour la défense Canada
		Assurer le fonctionnement du programme et de l'environnement de mise à l'essai des systèmes de contrôle industriel.	En cours	Sécurité publique Canada, Ressources naturelles Canada et Recherche et développement pour la défense Canada
		Élaborer et appliquer un programme de subvention et de contribution.	En bonne voie pour le printemps 2013	Sécurité publique Canada
		Concevoir et mettre en œuvre d'autres éléments de programme en consultation avec les propriétaires et les exploitants des systèmes essentiels.	En cours	Sécurité publique Canada

Mesure	Calendrier	Résultats escomptés	État	Responsable
Améliorer la capacité du Centre canadien de réponse aux incidents cybernétiques (CCRIC) d'offrir un soutien aux systèmes à l'extérieur du gouvernement du Canada				
Accroître la capacité du CCRIC.	Début : 2012	Accroître le nombre d'heures d'exploitation du CCRIC à raison de 15 heures par jour, sept jours par semaine, de façon à ce qu'elles correspondent aux heures de bureau en cours d'un bout à l'autre du pays.	Terminé	Sécurité publique Canada
	Début : 2011	Investir dans les capacités techniques du CCRIC grâce à la formation, à des systèmes et à des processus analytiques, à l'automatisation et à la technologie.	En cours	Sécurité publique Canada
Améliorer les capacités du CCRIC pour aider les propriétaires et les exploitants des systèmes essentiels à améliorer leur posture de cybersécurité.	Début : 2011	Mettre au point et actualiser le mandat du CCRIC de façon à privilégier la distribution de produits et de services aux systèmes essentiels à l'extérieur du gouvernement fédéral.	Terminé	Sécurité publique Canada
		Actualiser les procédures et les politiques du CCRIC de façon à fournir un niveau de soutien élevé et constant aux clients, étant donné l'évolution des activités.	En cours	Sécurité publique Canada
		Lancer le Portail de la communauté du CCRIC au sein du Portail des infrastructures essentielles.	Terminé	Sécurité publique Canada
		Assurer le fonctionnement du Portail de la communauté du CCRIC.	En cours	Sécurité publique Canada
		Mettre en place un programme d'échange d'employés entre le CCRIC et le Centre de la sécurité des télécommunications Canada.	Terminé	Sécurité publique Canada et Centre de la sécurité des télécommunications Canada
		Entreprendre la mise sur pied d'installations d'essais importantes pour améliorer la capacité du CCRIC d'effectuer des recherches et des analyses techniques.	Terminé	Sécurité publique Canada
Cerner et combler les lacunes des politiques en ce qui a trait à la cybersécurité au Canada.	Début : 2011	Fournir des conseils au gouvernement.	En cours	Sécurité publique Canada
Favoriser les activités de recherche et de développement				
Appuyer les activités de recherche et de développement en matière de cybersécurité afin d'améliorer les outils techniques nécessaires pour accroître la cybersécurité.	Début : 2011	Fournir du financement aux organisations du système d'innovation, y compris les établissements universitaires, pour élaborer de nouvelles solutions technologiques dans le domaine de la cybersécurité.	En cours	Recherche et développement pour la défense Canada
Élaborer un programme de mobilisation du milieu universitaire pour la cybersécurité afin de favoriser la création d'une collectivité universitaire forte et unie travaillant dans le domaine de la cybersécurité portant sur les sciences sociales.	Début : 2012	Organiser un atelier de niveau universitaire sur les questions touchant les infrastructures essentielles et la cybersécurité.	Terminé	Sécurité publique Canada
		Mandater des travaux de recherche sur la cybersécurité.	En cours	Sécurité publique Canada

Mesure	Calendrier	Résultats escomptés	État	Responsable
Mobiliser la communauté internationale				
Élaborer un plan d'action canado-américain sur la cybersécurité qui viendra accroître la capacité du Canada et la cybersécurité de nos infrastructures communes.	Début : 2012	Élaborer le plan d'action canado-américain sur la cybersécurité, conformément au Plan d'action Par-delà la frontière.	Terminé	Sécurité publique Canada
	Début : 2010	Mettre en œuvre le plan d'action canado-américain sur la cybersécurité.	En cours	Sécurité publique Canada
Travailler avec nos proches alliés et partenaires afin de promouvoir les intérêts du Canada dans un cyberespace ouvert, interopérable, sûr et fiable.	Début : 2010	Affecter, de façon permanente, des employés diplomatiques canadiens aux bureaux des Nations Unies à Genève pour traiter des questions de cybersécurité.	Terminé	Sécurité publique Canada et ministère des Affaires étrangères et du Commerce international
		Positionner le Canada en tant que l'un des 15 pays travaillant sur une étude majeure des Nations Unies pour le Secrétaire général des Nations Unies.	Terminé	Sécurité publique Canada, ministère des Affaires étrangères et du Commerce international et ministère de la Défense nationale, Forces canadiennes
		Assurer une collaboration régulière sur les questions stratégiques et opérationnelles à l'échelle internationale.	En cours	Sécurité publique Canada, ministère des Affaires étrangères et du Commerce international et ministère de la Défense nationale, Forces canadiennes
Travailler avec des organisations internationales et des gouvernements étrangers afin d'améliorer leurs capacités en matière de cybersécurité, et ainsi améliorer la capacité du Canada d'assurer la sécurité de ses infrastructures communes.	Début : 2012	Entreprendre des activités de renforcement des capacités avec de nombreux partenaires régionaux, parmi lesquels l'Organisation pour la sécurité et la coopération en Europe, le Forum régional de l'Association des nations de l'Asie du Sud Est et l'Organisation des États américains (OEA).	En cours	Ministère des Affaires étrangères et du Commerce international et Sécurité publique Canada
		Organiser un atelier de l'OEA pour y échanger les pratiques exemplaires sur l'élaboration de stratégies nationales en matière de cybersécurité.	Terminé	Sécurité publique Canada
Élaborer un cadre visant à s'assurer que les activités effectuées dans le cyberespace sont conformes aux objectifs généraux sur les politiques étrangères, le commerce international et la sécurité.	Début : 2012	Créer une politique étrangère sur la cybersécurité.	En bonne voie pour l'automne 2013	Ministère des Affaires étrangères et du Commerce international
Améliorer les mesures de communication et de collaboration du gouvernement en ce qui a trait aux questions internationales se rapportant au cyberespace.	Début : 2011	Créer et assurer le fonctionnement du groupe de travail interministériel sur les questions internationales se rapportant au cyberespace.	En cours	Présidence assurée tour à tour par des représentants du ministère des Affaires étrangères et du Commerce international, de Sécurité publique Canada, du ministère de la Justice et d'Industrie Canada
Faire appel à nos partenaires internationaux afin d'étudier les travaux exécutés par les Nations Unies sur la cybercriminalité.	Début : 2010	Collaborer à l'étude sur la cybercriminalité des Nations Unies. Représenter les gouvernements de l'Europe de l'Ouest et d'autres États à titre de rapporteur (ministère de la Justice).	En cours	Ministère de la Justice et ministère des Affaires étrangères et du Commerce international

Pilier 3
Aider les Canadiens à se protéger en ligne

Le troisième pilier de la *Stratégie de cybersécurité du Canada* consiste à fournir aux Canadiens de l'information pour se protéger et protéger leur famille en ligne, et à renforcer la capacité des organismes d'application de la loi à lutter contre la cybercriminalité.

Mesure	Calendrier	Résultats escomptés	État	Responsable
Mieux sensibiliser la population				
Aider les Canadiens à naviguer en toute sécurité en ligne.	Début : 2011	Élaborer une stratégie qui repose sur les campagnes publicitaires, les partenariats, Internet, les médias sociaux, les relations proactives avec les médias, la publicité gratuite, la mobilisation des parlementaires, les expositions et activités spéciales et les plans internes de communication.	Terminé	Sécurité publique Canada
		Mettre en œuvre la stratégie de communication.	En cours	Sécurité publique Canada
	Début : 2011	Effectuer des sondages de l'opinion publique afin d'évaluer la connaissance, les attitudes et les comportements des Canadiens en ce qui a trait à la cybersécurité.	Terminé	Sécurité publique Canada
	Début : 2011	Mettre sur pied une campagne de sensibilisation publique, Pensez cybersécurité, qui repose sur Internet, les médias sociaux et des activités médiatiques et ayant pour plaque centrale le site Web pensezcybersécurité.ca.	En cours	Sécurité publique Canada

Mesure	Calendrier	Résultats escomptés	État	Responsable
Mieux sensibiliser la population (suite)				
Aider les Canadiens à naviguer en toute sécurité en ligne. *(suite)*	Début : 2011	Créer des partenariats avec d'autres organismes fédéraux, ainsi qu'avec des intervenants canadiens et étrangers afin d'accroître la portée et la fréquence des messages ainsi que leur incidence sur les auditoires cibles.	En cours	Sécurité publique Canada
	Début : 2011	Travailler en partenariat avec STOP. THINK.CONNECT.™ (une coalition d'entreprises du secteur privé et d'organisations gouvernementales et sans but lucratif, dont le département américain de la Sécurité intérieure, et ayant pour objectif d'informer le public sur les façons d'assurer sa sécurité en ligne).	En cours	Sécurité publique Canada
	Début : 2012	Effectuer des analyses secondaires de l'environnement de la menace contre la cybersécurité pour les besoins de la campagne de sensibilisation publique.	En cours	Sécurité publique Canada
Cybercriminalité				
Créer un Centre intégré d'expertise sur les cybercrimes afin d'améliorer la connaissance de la situation et d'analyser les tendances en matière de cybercriminalité, et dans le cadre duquel de nouvelles méthodes de mesure du rendement et de collecte de données statistiques sont utilisées.	Début : 2011	Mettre sur pied le Centre intégré d'expertise sur les cybercrimes.	Terminé	Gendarmerie royale du Canada
		Préparer le premier rapport en analysant les tendances et les méthodes se rapportant à la cybercriminalité.	En bonne voie pour l'automne 2013	Gendarmerie royale du Canada
Élaborer une stratégie de lutte contre la cybercriminalité.	Début : 2012	Élaborer une stratégie de lutte contre la cybercriminalité pour traiter tous les aspects de la cybercriminalité, dont la fraude, le crime organisé et le vol d'identité.	En cours	Gendarmerie royale du Canada
Améliorer les outils législatifs afin de mieux protéger les Canadiens en ligne.	Début : 2010	Projet de loi C-28, *Loi visant l'élimination des pourriels sur les réseaux Internet et sans fil*.	Terminé (sanction royale obtenu, mais la Loi n'est pas encore en application)	Industrie Canada
	Début : 2011	Le projet de loi C-12, Loi sur la protection des renseignements personnels et les documents électroniques, ce qui comprend les exigences relatives à la notification de violation pour les organisations.	En bonne voie (en attente de la deuxième lecture)	Industrie Canada

Conclusion

La cybersécurité est une responsabilité partagée, et le gouvernement fédéral, le secteur privé, d'autres niveaux du gouvernements et les Canadiens doivent travailler ensemble afin d'assurer la sécurité des cybersystèmes essentiels et de pouvoir continuer à se protéger en ligne. La Stratégie et le Plan d'action tiennent compte de cette responsabilité partagée. À l'avenir, en collaboration avec les partenaires du gouvernement fédéral et à l'extérieur de celui-ci, ce plan d'action sera révisé et mis à jour de façon périodique pour s'assurer que les progrès se poursuivent.