Gouvernement du Canada | Government of Canada

Stratégie de cybersécurité du Canada

RENFORCER LE CANADA ET ACCROÎTRE SA PROSPÉRITÉ

Canada

No de cat. : PS4-102/2010F-PDF

ISBN : 978-1-100-95709-8

Imprimé au Canada

Message du Ministre

Les vies personnelle et professionnelle des Canadiens ont pris le tournant numérique : nous vivons, travaillons et jouons dans le cyberespace. Les Canadiens utilisent Internet, ordinateurs, téléphones cellulaires et appareils sans fil tous les jours pour parler et envoyer des courriels, des messages texte et des « tweets » aux membres de leur famille, à leurs amis et à leurs collègues. Chaque jour, nous accédons à Internet pour effectuer des transactions bancaires, magasiner ou utiliser des services gouvernementaux, et nous le faisons à partir de n'importe où. Les infrastructures numériques rendent tout cela possible et assurent le bon fonctionnement des services essentiels en tout temps.

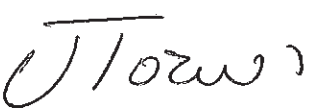
Les Canadiens (individus, industries et gouvernements) sont conscients des nombreux avantages qu'offre le cyberespace pour notre économie et qualité de vie. Notre grande dépendance aux cybertechnologies nous rend toutefois plus vulnérables aux attaques lancées contre nos infrastructures numériques dans le but de déstabiliser notre sécurité nationale, notre prospérité économique et nos modes de vie.

Nos systèmes sont des cibles attrayantes pour les services militaires et du renseignement étrangers ainsi que pour les réseaux criminels et terroristes. Ces groupes s'emparent de nos systèmes informatiques, fouillent dans nos dossiers et provoquent des pannes informatiques. Ils volent nos secrets de sécurité nationale et industriels ainsi que nos identités personnelles.

Nous ne les voyons pas, ne les entendons pas et ne les attrapons pas toujours. Ils ne sont parfois que de simples nuisances, mais peuvent également devenir de véritables menaces pour nos familles, nos entreprises et notre pays.

La *Stratégie de cybersécurité du Canada* est la mesure que nous avons prise pour contrer les cybermenaces. Elle fait suite à l'engagement pris par le gouvernement en 2010, dans le discours du Trône, de collaborer avec les provinces, les territoires et le secteur privé pour mettre en œuvre une stratégie de cybersécurité afin de protéger nos infrastructures numériques. La Stratégie permet de renforcer les partenariats établis dans le cadre de la *Stratégie nationale et le plan d'action sur les infrastructures essentielles*. Elle soutient également les efforts continus déployés par les organismes responsables de l'application de la loi en vue de collaborer avec les partenaires et les alliés internationaux afin de sévir contre ceux qui se servent d'Internet pour participer à des activités criminelles et illégales.

La *Stratégie de cybersécurité du Canada* est une des pierres angulaires de l'engagement du gouvernement d'assurer la sécurité et la prospérité du Canada, notamment de son cyberespace.



L'honorable Vic Toews, c.p., c.r., député
Ministre de la Sécurité publique

Introduction

Le **cyberespace** est le monde électronique créé par des réseaux interconnectés formés de systèmes de technologie de l'information et de l'information qui se trouve sur ses réseaux. Le cyberespace est un bien commun reliant plus de 1,7 milliard de personnes qui échangent des idées et des services et qui tissent des liens d'amitié.

L'économie canadienne repose dans une grande mesure sur Internet :

- En 2007, les ventes en ligne au Canada étaient évaluées à 62,7 milliards de dollars[1];
- En 2007, 87 % des entreprises canadiennes utilisaient Internet[1].

Les entreprises canadiennes s'empressent d'adopter les toutes dernières applications, notamment les technologies mobiles et de la prochaine génération.

Les gouvernements au Canada dépendent aussi de plus en plus d'Internet. Le gouvernement fédéral offre à lui seul plus de 130 services courants en ligne, comme les demandes de remboursement d'impôt, d'assurance-emploi et de prêts étudiants.

Notre utilisation fructueuse du cyberespace représente l'un de nos atouts stratégiques nationaux les plus importants. Pour maintenir cette réussite, nous devons protéger nos

Les Canadiens saisissent les occasions que présente le cyberespace :

- 74 % des foyers canadiens avaient des abonnements Internet en 2008[2] ;
- 59 % des déclarations d'impôt sur le revenu ont été transmises par voie électronique en 2008[3] ;
- 67 % des Canadiens ont effectué des opérations bancaires en ligne en 2009[4].

[1] Statistique Canada – *Le Quotidien*, 24 avril 2008
[2] Conseil de la radiodiffusion et des télécommunications canadiennes – *Rapport de surveillance des communications*, août 2009
[3] Agence du revenu du Canada – *Rapport national sur l'avancement du travail,* septembre 2009
[4] Statistique Canada, *Enquête canadienne sur l'utilisation d'Internet,* 2009

cybersystèmes contre les utilisations malveillantes et les autres attaques destructrices. Il s'agit d'un défi de taille. Il n'existe pas de formule simple pour repérer et identifier les attaquants qui ne sont ni vus, ni entendus, qui ne laissent aucune trace matérielle et qui dissimulent leurs activités en utilisant un réseau complexe d'ordinateurs infiltrés.

La cybersécurité concerne chacun d'entre nous, puisque même les attaquants possédant seulement des compétences de base peuvent causer de graves dommages. Les attaquants qui s'y connaissent vraiment peuvent troubler les contrôles électroniques des réseaux de distribution d'électricité, des installations de traitement des eaux et des réseaux de télécommunications. Ils nuisent à la production et à la livraison de biens et services essentiels fournis par nos gouvernements et le secteur privé. Ils portent atteinte à notre droit à la vie privée en volant nos renseignements personnels. Il ne suffit pas de lutter séparément contre les différentes cybermenaces. Par l'entremise de la Stratégie, le gouvernement continuera de travailler de manière concertée avec les provinces, les territoires et le secteur privé pour combattre les menaces auxquelles font face le Canada et ses citoyens.

Les cyberattaques comprennent l'accès involontaire ou non autorisé à des renseignements électroniques et/ou des infrastructures électroniques ou matérielles utilisés pour traiter, communiquer ou entreposer cette information, ainsi que leur utilisation, leur manipulation, leur interruption ou leur destruction (par voie électronique). La gravité des cyberattaques détermine le niveau d'intervention et les mesures d'atténuation nécessaires, c'est-à-dire la cybersécurité.

Chaque année, nous détectons un nombre croissant d'attaquants. Chaque année, ceux qui cherchent à infiltrer, à exploiter et à attaquer nos cybersystèmes sont plus compétents et mieux équipés que l'année précédente. Ils investissent afin d'accroître leur capacité. Nous devons aussi investir davantage.

Le gouvernement poursuit ses efforts afin d'assurer la sécurité des cybersystèmes au Canada et de protéger les Canadiens et Canadiennes en ligne. La Stratégie fait partie d'une série d'initiatives mises sur pied pour protéger la population canadienne. Le gouvernement a établi le Centre canadien de réponse aux incidents cybernétiques pour surveiller les cybermenaces et fournir des conseils pour les atténuer; ce centre coordonne également l'intervention au niveau national en cas de cyberincident. Le gouvernement présentera sous peu des projets de loi pour moderniser les pouvoirs d'enquête des organismes d'application de la loi et pour veiller à ce que les criminels ne profitent pas des innovations technologiques pour éviter les interceptions licites de leurs communications.

Bien qu'importantes, ces initiatives ne suffisent plus. La menace est de plus en plus lourde. Les efforts que nous déployons pour assurer la cybersécurité ne doivent pas se limiter aux menaces telles que perçues par le passé. Le Canada doit prévoir et combattre les nouvelles cybermenaces pour que notre utilisation savante du cyberespace demeure un atout. La *Stratégie de cybersécurité du Canada* est notre feuille de route pour accroître la sécurité du cyberespace pour l'ensemble des Canadiens et Canadiennes.

Comprendre les cybermenaces

Il existe plusieurs façons d'accéder à l'information à partir du cyberespace. Les attaquants peuvent exploiter des vulnérabilités dans les logiciels ou le matériel. Ils peuvent exploiter des vulnérabilités sur le plan de la sécurité en amenant par la ruse des personnes à ouvrir des courriels infectés ou à visiter des sites Web corrompus qui leur permettent d'infecter les ordinateurs avec des maliciels. Ils peuvent aussi profiter des personnes qui n'appliquent pas les pratiques de base en matière de cybersécurité, comme changer souvent leurs mots de passe, mettre à jour périodiquement les logiciels antivirus et utiliser seulement des réseaux sans fil protégés.

Dès qu'ils ont accès à un ordinateur, les attaquants peuvent voler ou changer l'information qui s'y trouve, en corrompre les opérations et le programmer pour qu'il attaque d'autres ordinateurs et les systèmes auxquels il est relié. Dans bien des cas, les victimes se font voler leur identité ou des actifs personnels. Selon une étude menée par l'Université McMaster[5], 1,7 million de Canadiens ont été victimes de vol d'identité en 2008. Le coût annuel du vol d'identité au Canada est évalué à près de 1,9 milliard de dollars. Le gouvernement a d'ailleurs modifié le *Code criminel* pour mieux protéger les Canadiens contre le vol d'identité.

Les entreprises canadiennes peuvent se faire devancer dans la course à la mise en marché d'un produit ou encore subir des préjudices sans jamais se rendre compte que les pertes sont causées par des cyberattaques. Récemment, il semblerait que 86 % des grandes organisations canadiennes aient été la cible d'une cyberattaque au cours d'une période récente d'un an. Les pertes de propriété intellectuelle résultant de ces attaques ont doublé de 2006 à 2008[6].

Certains outils et procédés sont plus coûteux et complexes que d'autres. Cependant, la plupart des cyberattaques ont

[5] McMaster University, *Measuring Identity Theft in Canada: 2008 Consumer Survey*

[6] Sondage 2008 de CA Technologies sur la sécurité et la protection de la confidentialité.

en commun quatre caractéristiques qui expliquent, en partie, leur popularité croissante. Les cyberattaques sont dans bien des cas :

- **peu coûteuses :** il est possible de se procurer un grand nombre d'outils d'attaque à bas prix ou de les télécharger gratuitement à partir d'Internet;
- **simples :** les attaquants ayant seulement des connaissances de base peuvent infliger des dommages considérables;
- **efficaces :** même les attaques mineures peuvent causer des dommages importants;
- **à faible risque :** les attaquants peuvent éviter d'être découverts et poursuivis en utilisant un réseau complexe d'ordinateurs pour dissimuler leurs traces et en exploitant les lacunes des régimes juridiques nationaux et étrangers.

Les cibles et les méthodes des cyberattaquants se ressemblent quelque peu, mais la nature de la menace que pose chacun d'entre eux varie en fonction de leurs motifs et intentions. Il existe trois types de menaces, lesquels sont décrits dans les prochains paragraphes.

CYBERESPIONNAGE ET ACTIVITÉS MILITAIRES PARRAINÉS PAR DES ÉTATS

Les services militaires et du renseignement étrangers sont à l'origine des cybermenaces les plus évoluées. Dans la plupart des cas, ces attaquants sont patients et persistants, et ils ont d'importantes ressources à leur disposition. Leur but est d'obtenir des avantages politiques, économiques, commerciaux ou militaires.

Tous les gouvernements et toutes les entreprises à la fine pointe de la technologie peuvent être la cible d'activités de cyberespionnage parrainées par des États. Des rapports produits au Canada et ailleurs dans le monde confirment que les auteurs de ces attaques ont réussi à voler des secrets industriels et des secrets d'État, des données privées et d'autres renseignements à valeur stratégique.

Certains États étrangers ont déclaré publiquement que les cyberattaques représentaient un élément central de leur stratégie militaire. Certains ont été largement accusés de mener des cyberattaques parallèlement à des opérations militaires traditionnelles pour accentuer les conséquences de ces dernières. Les programmes de cyberattaques de ces États sont habituellement conçus pour saboter les infrastructures et les communications d'un adversaire, ou appuyer des attaques électroniques contre le matériel et les opérations militaires d'un adversaire. Les cyberattaques qui perturbent les systèmes d'intervention d'urgence et de santé publique peuvent mettre des vies en danger.

Le Canada et ses alliés savent qu'ils doivent moderniser leur doctrine militaire pour affronter ces risques. Pour cette raison, l'Organisation du Traité de l'Atlantique Nord (OTAN) a adopté plusieurs documents stratégiques sur la cyberdéfense. Comme les forces militaires de nos plus étroits alliés, le ministère de la Défense nationale et les Forces canadiennes étudient les mesures que peut prendre le Canada pour réagir de manière optimale aux cyberattaques futures.

UTILISATION D'INTERNET PAR LES TERRORISTES

Les réseaux terroristes ont également commencé à intégrer les cyberopérations à leur doctrine stratégique. Ils utilisent entre autres Internet pour recruter des membres, recueillir des fonds et faire de la propagande.

Les terroristes sont conscients que la dépendance des pays occidentaux à l'égard des cybersystèmes constitue une vulnérabilité à exploiter. Par exemple, des ressources en ligne contiennent des conseils à l'intention des terroristes sur la façon de défendre leurs propres sites Web tout en lançant des cyberattaques contre leurs ennemis. De plus, certains organismes terroristes, dont Al Qaïda, ont signalé leur intention de diriger des cyberattaques contre des pays occidentaux. Les spécialistes soupçonnent que les terroristes n'ont pas actuellement la capacité de causer de graves dommages aux moyens de cyberattaques; ils reconnaissent cependant que ces organismes augmenteront leur capacité au fil du temps.

CYBERCRIMINALITÉ

Tout comme les États, les groupes criminels organisés ont étendu leurs activités au cyberespace. Les groupes les mieux avisés se tournent vers des cyberattaquants qualifiés pour mener nombre de leurs activités traditionnelles, comme le vol d'identité, le blanchiment d'argent et l'extorsion.

Les criminels vendent sur Internet des renseignements volés, comme des numéros de carte de crédit et de débit, des mots de passe donnant accès à des serveurs et des maliciels conçus pour infiltrer ou endommager des systèmes ciblés. Même les personnes qui protègent avec diligence leurs renseignements personnels en ligne sont susceptibles de se faire voler ceux détenus par des tiers à qui ils ont été communiqués.

Certaines organisations criminelles développent maintenant des logiciels d'attaque sur mesure. Ils utilisent de nouvelles technologies de cryptage pour protéger leurs propres actifs et secrets professionnels. Certains organismes du milieu de l'application de la loi et du renseignement affirment que les moyens dont disposent certains cybercriminels rivalisent maintenant avec ceux de pays développés.

LES MENACES ÉVOLUENT

Tout comme les bactéries qui deviennent résistantes aux antibiotiques, les virus informatiques et codes malveillants évoluent sans cesse afin d'échapper à nos défenses et aux logiciels antivirus. Le rythme auquel changent les outils et techniques utilisés pour commettre des cyberattaques a dangereusement accéléré au cours des dernières années. Selon des données compilées par deux entreprises connues de sécurité Internet, Akamai et Symantec, de nos jours, les maliciels proviennent de plus de 190 pays[7]. Plus de 60 % des codes malveillants détectés jusqu'à maintenant ont été introduits dans le cyberespace en 2008[8].

Il n'y a aucun doute que la fréquence et la gravité des cybermenaces vont en augmentant. Protéger les Canadiens dans le cyberespace représente donc un défi constant. Pour venir à bout des menaces, il faudra mettre en place un large éventail de mesures, investir constamment des fonds et demeurer vigilants à long terme.

[7] Akamai, « State of the Internet Report », mars 2009
[8] Symantec, « Global Internet Security Threat Report », avril 2009

Stratégie de cybersécurité du Canada

Les chercheurs canadiens ont joué un rôle de premier plan pour faire du cyberespace une réalité. Il faut maintenant continuer à faire preuve de la même ingéniosité pour prédire, détecter et éliminer les futures cybermenaces et exploiter le cyberespace de manière à promouvoir les intérêts canadiens.

La *Stratégie de cybersécurité du Canada* constitue notre plan pour combattre les cybermenaces. La Stratégie repose sur trois piliers :

1. **Protéger les systèmes gouvernementaux** – Les Canadiens confient au gouvernement leurs renseignements personnels et organisationnels, et ils comptent également sur lui pour leur fournir des services. Ils s'en remettent au gouvernement pour défendre la souveraineté cybernétique du Canada de même que pour assurer la sécurité nationale et promouvoir nos intérêts économiques. Le gouvernement mettra en place les structures, les outils et le personnel nécessaires pour satisfaire ses obligations en matière de cybersécurité.

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. En collaboration avec les gouvernements provinciaux et territoriaux ainsi que le secteur privé, le gouvernement appuiera des initiatives et prendra des mesures pour renforcer la résilience cybernétique du Canada, y compris celles des secteurs d'infrastructures essentielles.

3. **Aider les Canadiens à se protéger en ligne** – Le gouvernement aidera les citoyens canadiens à obtenir l'information dont ils ont besoin pour se protéger et protéger leur famille en ligne et pour accroître la capacité des organismes d'application de la loi de lutter contre les cybercrimes.

La *Stratégie de cybersécurité du Canada* contribuera à renforcer nos cybersystèmes et nos secteurs d'infrastructures essentielles, à favoriser la croissance économique et à protéger les Canadiens et Canadiennes lorsqu'ils se branchent entre eux et avec le reste du monde. Tout en profitant pleinement des avantages que procure le cyberespace, nous avons tous un rôle à jouer pour bâtir un Canada sécuritaire, résilient et novateur.

La Stratégie :

- traduit les valeurs canadiennes, comme la primauté du droit, la responsabilisation et le droit à la vie privée;
- permet d'apporter des améliorations constantes pour faire face aux nouvelles menaces;
- intègre les activités à l'échelle du gouvernement du Canada;
- met l'accent sur les partenariats avec les Canadiens, les provinces et les territoires, les entreprises et les universités;
- prend appui sur les relations étroites avec nos alliés.

Le gouvernement a demandé aux intervenants leurs points de vue au sujet d'un vaste éventail de cybermenaces et de pratiques de sécurité. La collaboration, particulièrement à l'échelle internationale, est essentielle pour protéger le cyberespace. Le Canada gagnera à être perçu à l'échelle nationale et internationale comme un partenaire fiable qui contribue à assurer la sécurité du cyberespace.

Trois de nos partenaires les plus proches en matière de sécurité et du renseignement, soit les États-Unis, le Royaume-Uni et l'Australie, ont publié récemment leurs propres plans sur la protection du cyberespace. Un grand nombre des principes directeurs et des priorités opérationnelles énoncés dans ces rapports ressemblent aux nôtres. En adoptant des mesures complémentaires qui font ressortir nos expériences communes en matière de cybersécurité, nous montrons que nous sommes déterminés à améliorer la sécurité collective en s'appuyant sur les régimes de cybersécurité de chacun.

Tout comme le Canada, nos alliés ont l'intention d'examiner et de mettre à jour leurs plans périodiquement pour tenir compte de l'avancement des technologies et pratiques en matière de cybersécurité et de l'évolution des cybermenaces.

Le Canada mettra également à profit sa participation à des discussions sur la cybersécurité dans le cadre de forums internationaux importants, comme les Nations Unies, l'OTAN et le Groupe des huit. Le Canada est l'un des États non européens signataires de la Convention sur la cybercriminalité du Conseil de l'Europe, et le gouvernement prépare un projet de loi pour en permettre la ratification.

Le Canada appuie les efforts internationaux visant à élaborer et à mettre en place un régime de gouvernance global pour la cybersécurité qui renforcera la sécurité. Dans la mesure du possible, le Canada appuiera les efforts visant à accroître la capacité de cybersécurité de pays moins développés et de partenaires à l'étranger. Il pourra ainsi empêcher ses adversaires d'exploiter les faiblesses dans les cyberdéfenses mondiales.

TRAVAILLER EN COLLABORATION

La Stratégie sera mise en œuvre par les ministères et organismes les plus directement responsables de la protection des cybersystèmes du gouvernement. Nous travaillerons également en collaboration avec nos partenaires provinciaux et territoriaux, qui partagent la responsabilité de protéger nombre d'infrastructures essentielles au Canada.

Le milieu universitaire, les organismes non gouvernementaux et le secteur privé au Canada doivent unir leurs efforts à ceux du gouvernement pour assurer la sécurité des cybersystèmes au pays. Ils ont tous des capacités technologiques et analytiques particulières et une bonne raison de protéger leurs propres systèmes. Leur collaboration est essentielle à notre réussite commune afin de sécuriser le Canada et d'accroître notre productivité et prospérité.

Les Canadiens et Canadiennes ont également un rôle important à jouer pour protéger l'avenir cybernétique de notre pays. Le gouvernement peut lancer et appuyer d'importantes initiatives axées sur la cybersécurité, mais il ne peut pas protéger chacun d'entre nous contre toutes les menaces lorsque nous nous branchons à Internet. Les Canadiens doivent être sensibilisés aux menaces et informés des outils disponibles pour les reconnaître et les éviter. Plus important encore, ils doivent utiliser ces outils pour se protéger et protéger leur famille.

La cybersécurité est l'affaire de tous, au quotidien. Elle contribue à rendre le Canada plus sécuritaire et plus prospère.

Initiatives

La *Stratégie de cybersécurité du Canada* repose sur trois piliers :

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

PROTÉGER LES SYSTÈMES GOUVERNEMENTAUX

Contrairement au monde physique, aucun régime de loi et d'ordre ne gouverne le monde cybernétique où vivent, travaillent et jouent les Canadiens et Canadiennes. Le gouvernement est chargé de protéger nos renseignements les plus personnels et l'information de nature délicate contenue dans ses bases de données électroniques. Il fournit des services aux Canadiens et au secteur privé par l'entremise de ses sites Web et de ses systèmes de traitement électronique. Il transmet à l'aide de systèmes de communications sécurisés des renseignements hautement classifiés qui sont essentiels à nos opérations militaires et de sécurité nationale.

Les systèmes gouvernementaux ont été la cible d'un grand nombre de cyberattaques. Les cyberattaquants sondent périodiquement ces systèmes afin de découvrir des vulnérabilités. Il importe de protéger ces systèmes non seulement pour des raisons d'efficacité opérationnelle, mais aussi pour assurer la sécurité nationale et la souveraineté de notre pays, pour sauvegarder les vies des membres du personnel des services extérieurs et des forces militaires, pour assurer l'intégrité de notre économie et pour préserver les renseignements personnels des Canadiens.

Nous devons renforcer la capacité du gouvernement de détecter et d'empêcher les cyberattaques, ainsi que de se défendre le cas échéant, tout en déployant des cybertechnologies pour soutenir les intérêts économiques et la sécurité nationale au Canada. C'est ce que nous allons faire. Pour assurer l'intégrité cybernétique du gouvernement, il faut établir clairement les rôles et les responsabilités, accroître la sécurité des systèmes et sensibiliser les fonctionnaires au sujet des consignes à respecter.

Établir clairement les rôles et responsabilités du gouvernement fédéral

Vu l'importance de la cybersécurité, il ne doit exister aucune ambigüité quant aux rôles et responsabilités de chacun. La Stratégie est claire à ce sujet.

Sécurité publique Canada coordonnera la mise en œuvre de la Stratégie. Il établira une approche pangouvernementale pour en rendre compte, et il coordonnera de manière centrale l'évaluation des nouvelles menaces complexes ainsi que l'élaboration et la promotion d'approches complètes et harmonisées pour faire face aux risques au sein du gouvernement et partout au Canada. Au sein de Sécurité publique Canada, le Centre canadien de réponse aux incidents cybernétiques continuera de servir de point central pour la surveillance des cybermenaces et la communication de conseils sur leur atténuation, et il dirigera l'intervention nationale en cas de cyberincident. Sécurité publique Canada mènera aussi des activités publiques de sensibilisation et de liaison pour informer les Canadiens et les Canadiennes des risques potentiels auxquels ils font face et les actions qu'ils peuvent prendre pour se protéger et pour protéger leur famille dans le cyberespace.

Le Centre de la sécurité des télécommunications Canada est reconnu à l'échelle internationale pour son expertise en matière de lutte contre les cybermenaces et les cyberattaques. Compte tenu de son mandat particulier et de ses connaissances sans pareil, le Centre de la sécurité des télécommunications Canada accroîtra sa capacité de détecter et découvrir les menaces, de fournir des services du renseignement étranger et de cybersécurité, et de faire face aux cybermenaces et cyberattaques contre les réseaux et systèmes de technologie de l'information du gouvernement.

Le Service canadien du renseignement de sécurité analysera les menaces nationales et étrangères mettant en péril la sécurité du Canada et mènera des enquêtes à ce sujet. Conformément à la *Loi sur la Gendarmerie royale du Canada*, la Gendarmerie royale du Canada enquêtera sur les actes criminels d'origine canadienne et étrangère impliquant des réseaux et des infrastructures essentielles d'information au Canada.

Le Secrétariat du Conseil du Trésor renforcera la capacité de gérer les cyberincidents à l'échelle du gouvernement, notamment en élaborant des politiques, des normes et des outils d'évaluation. Il est également responsable de la sécurité de la technologie de l'information au sein du gouvernement du Canada.

Affaires étrangères et Commerce international Canada prodiguera des conseils sur la dimension internationale de la cybersécurité et élaborera une politique étrangère sur la cybersécurité pour renforcer la cohérence des activités liées à la cybersécurité menées à l'étranger par le gouvernement.

Le ministère de la Défense nationale et les Forces canadiennes renforceront leur capacité de défendre leurs propres réseaux et travailleront avec d'autres ministères fédéraux afin de cerner les menaces et de déterminer les interventions possibles. Ils continueront en outre d'échanger avec les forces militaires de nos alliés de l'information sur les pratiques exemplaires en matière de cybersécurité. Le ministère de la Défense nationale et les Forces canadiennes collaboreront avec nos alliés pour établir des cadres stratégiques et juridiques régissant les aspects militaires de la cybersécurité, appuyant ainsi les activités de liaison internationale d'Affaires étrangères et Commerce international Canada.

Compte tenu de la vitesse et de la complexité des cyberattaques dans bien des cas, il est essentiel d'éliminer les obstacles à la coopération et à l'échange d'information entre les partenaires fédéraux. La Stratégie englobe des mesures à l'appui de cet objectif, et prévoit des ressources financières et humaines supplémentaires pour permettre au gouvernement de satisfaire ses obligations en matière de cybersécurité.

Accroître la sécurité des cybersystèmes fédéraux

Chaque fois qu'une nouvelle technologie ou pratique est adoptée pour accroître la cybersécurité, une autre est mise au point pour l'éluder. Nous continuerons d'investir pour mettre en place l'expertise, les systèmes et les cadres nécessaires afin de rester à la hauteur des nouvelles menaces. Nous étudierons également les options à notre disposition pour accroître les risques et les conséquences pour les attaquants qui ciblent nos cybersystèmes.

Le gouvernement resserrera la sécurité de son architecture cybernétique. Il continuera de réduire le nombre de passerelles Internet donnant accès à ses systèmes informatiques et prendra d'autres mesures pour protéger les systèmes.

En 2009, le gouvernement a apporté des modifications importantes à la Politique sur la sécurité du gouvernement. Administrée par le Secrétariat du Conseil du Trésor, cette politique prévoit des mesures de protection pour assurer la prestation de services gouvernementaux à la population. Puisque le gouvernement compte beaucoup sur la technologie de l'information pour offrir ses services, la politique insiste sur le fait que les ministères et organismes doivent surveiller et protéger leurs opérations électroniques.

Compte tenu de la mondialisation de l'industrie de la technologie, il est difficile de déterminer et d'évaluer si les fournisseurs sont fiables. Les cyberattaquants sont bien au courant des possibilités qu'offrent les lacunes en matière de sécurité dans la chaîne d'approvisionnement mondiale. Certains groupes criminels organisés et services du renseignement étrangers exploitent déjà ces vulnérabilités afin de disséminer des technologies exploitables. Le gouvernement renforcera ses processus pour réduire les risques associés aux technologies compromises.

Sensibiliser les fonctionnaires fédéraux aux questions de cybersécurité

Il est important d'établir clairement les rôles et responsabilités et de renforcer les systèmes pour assurer la cybersécurité, mais pour réussir à protéger ses cybersystèmes, le gouvernement dépend en large partie de ses employés. Comme l'ont montré d'innombrables incidents survenus dans tous les secteurs de la société, même les systèmes de sécurité les plus complexes peuvent être ébranlés par de simples erreurs humaines. Au gouvernement comme ailleurs, les employés peuvent ne pas appliquer les pratiques de base en cybersécurité, comme :

- ne pas changer périodiquement leurs mots de passe;
- se tromper en supposant qu'un système de courriel est sécuritaire;
- importer des maliciels au travail en visitant des sites Web corrompus.

NOUER DES PARTENARIATS POUR PROTÉGER LES CYBERSYSTÈMES ESSENTIELS À L'EXTÉRIEUR DU GOUVERNEMENT FÉDÉRAL

Le succès financier du secteur privé au Canada dépend en grande partie de sa capacité de protéger ses projets de recherche à la fine pointe et la propriété intellectuelle, ses opérations commerciales et ses données financières. À défaut de protéger ces actifs, les entreprises perdent une part du marché et des clients, et peuvent s'effondrer.

De même, notre bien-être personnel repose sur l'accès à des services sûrs et fiables qui sont assurés par les réseaux de transport et de communication et les institutions financières. Il est donc de plus en plus important de protéger contre les cybermenaces les deux principaux garants de notre qualité de vie, soit les entreprises privées qui contribuent à notre prospérité économique et les systèmes d'infrastructure à l'appui de nos activités quotidiennes. Le défaut d'agir sur ce plan aurait des conséquences négatives sur l'économie et minerait la confiance des consommateurs.

Une étude menée en 2008 par l'Université McMaster[9] sur le vol d'identité a révélé que 20 % des consommateurs avaient cessé de faire des achats en ligne ou en avaient réduit le nombre, et que 9 % des consommateurs avaient cessé d'effectuer des opérations bancaires en ligne ou en avait réduit le nombre en raison des risques qu'ils estiment associés aux activités en ligne. En bâtissant un environnement opérationnel sûr et fiable, nous favoriserons la productivité et l'innovation de manière à contribuer à la prospérité économique de notre pays.

Le public doit être plus conscient des vulnérabilités inhérentes aux cybersystèmes qu'utilisent ces industries pour offrir leurs services. S'ils sont mieux informés, les Canadiens pourront éviter de devenir victimes de vol d'identité ou de subir des pertes financières. Le gouvernement travaillera en partenariat avec les provinces, les territoires et le secteur privé pour améliorer la posture de cybersécurité du Canada et des Canadiens.

[9] McMaster University, *Measuring Identity Theft in Canada: 2008 Consumer Survey*

Le gouvernement misera sur des programmes existants et l'expertise en place, comme le Programme technique de sécurité publique de Recherche et développement pour la défense Canada, pour favoriser les activités de recherche et de développement sur la cybersécurité. Nous collaborerons également avec le secteur privé et les partenaires universitaires pour accroître l'échange d'information.

Partenariats avec les provinces et les territoires

Renforcer les partenariats parmi les différents ordres de gouvernement est un élément essentiel de la mise en œuvre d'une stratégie globale de cybersécurité pour le Canada et sa population. Les gouvernements provinciaux et territoriaux offrent toute une gamme de services essentiels dont la prestation repose sur le fonctionnement sécuritaire de leurs cybersystèmes. Par exemple, ils détiennent des renseignements très personnels dans leurs bases de données, notamment des dossiers médicaux, des licences de mariage, des permis de conduire et des renseignements sur les déclarations d'impôt provinciales. Les provinces et territoires ont un rôle important à jouer afin de sensibiliser les Canadiens et Canadiennes, et plus particulièrement les jeunes au sein du système d'éducation où ils sont souvent exposés pour la première fois à Internet. Ce n'est que lorsque tous les ordres de gouvernement travaillent ensemble que les renseignements personnels des Canadiens et les services dont ils dépendent sont assurés.

Partenariat avec le secteur privé et les secteurs d'infrastructures essentielles

Les risques et conséquences liés aux cyberattaques sont en grande partie les mêmes pour le gouvernement et le secteur privé. Par exemple, les technologies douteuses causent des dommages au gouvernement et à l'industrie. Il est donc important de travailler en partenariat pour cerner ces risques.

Heureusement, les secteurs public et privé au Canada collaborent ensemble depuis longtemps afin d'atteindre des objectifs communs touchant l'économie et la sécurité nationale. Il importe de resserrer cette collaboration. Chaque partenaire doit échanger en temps opportun des renseignements exacts sur la cybersécurité, notamment sur les menaces existantes et nouvelles, sur les techniques de défense et les pratiques exemplaires.

Pour renforcer les partenariats publics-privés, le gouvernement misera sur les structures et organisations existantes, comme les réseaux sectoriels d'infrastructures essentielles. Des mécanismes intersectoriels seront établis pour permettre aux gouvernements et à l'industrie de collaborer sur diverses questions relatives aux infrastructures essentielles, y compris la cybersécurité.

Les partenaires des secteurs publics et privés devront également collaborer pour assurer la sécurité des systèmes de contrôle des processus, qui gouvernent tout, que ce soit la machinerie, les usines ou nos infrastructures essentielles. Ces systèmes empêchent les barrages de céder, les réseaux électriques de s'effondrer et les réseaux de transport de faire défaut. La sécurité de ces systèmes est indispensable pour assurer des services et des biens dont dépendent les Canadiens. Des initiatives conjointes entre les secteurs public et privé seront lancées pour recenser et communiquer les pratiques exemplaires de manière à lutter contre les menaces touchant ces systèmes.

Nous améliorerons les mesures prises collectivement pour assurer la cybersécurité grâce à des programmes de formation et d'exercices. Les résultats de ces exercices, dont certains sont en cours, permettront de mieux comprendre la dynamique entre les partenaires de la cybersécurité. La participation à ces exercices permettra d'améliorer les procédures visant à prévenir les manquements à la sécurité.

Les perturbations touchant les infrastructures essentielles et les cybersystèmes peuvent avoir une incidence directe sur les activités et les collectivités de part et d'autre de la frontière entre le Canada et les États-Unis. Les attaques contre des réseaux cybernétiques interreliés peuvent avoir un effet en cascade dans tous les secteurs de l'industrie et sur la frontière. Pour cette raison, le Canada jouera un rôle actif dans le cadre de forums internationaux afin de promouvoir la protection des infrastructures essentielles et la cybersécurité.

AIDER LES CANADIENS À SE PROTÉGER EN LIGNE

Notre capacité d'exploiter le cyberespace nous a permis d'accroître plus que jamais notre productivité et notre prospérité personnelle. Cependant, des criminels de toutes les régions du monde peuvent commettre des variantes de crimes traditionnels en recourant aux technologies du 21e siècle. Le gouvernement prend des mesures pour que le cyberespace ne devienne pas un refuge pour les criminels. Nous briserons l'anonymat recherché par les cybercriminels tout en protégeant le droit à la vie privée des Canadiens et Canadiennes.

Combattre la cybercriminalité

Les criminels ont rapidement appris qu'il est profitable ainsi que peu coûteux et peu risqué de commettre des crimes à partir du cyberespace. Pour donner un exemple connu[10], en 2007, plus de 45 millions de dossiers de clients ont été volés chez un détaillant nord-américain bien en vue. Sur une période de trois ans, des criminels ont surveillé les signaux sans fil des terminaux de cartes de crédit des points de vente. Ces attaques ont coûté au détaillant plus de 130 millions de dollars et ont causé aux victimes des préjudices financiers dont on ignore l'ampleur.

Également en 2008, 11 personnes dans cinq pays différents ont été accusées[11] d'avoir infiltré les bases de données de neuf grands détaillants américains; ils ont volé quelque 40 millions de numéros de carte de crédit et de débit et les ont vendus (sur Internet) à d'autres criminels.

Les organismes d'application de la loi au Canada ne peuvent pas lutter contre les cybercrimes transnationaux en s'appuyant sur des pouvoirs et des outils qui ne sont plus à jour. Pour donner aux services de police les moyens de nous protéger dans le cyberespace, nous devons leur accorder de nouveaux pouvoirs dans la loi et leur octroyer les ressources financières nécessaires.

Par conséquent, le gouvernement donnera à la Gendarmerie royale du Canada les ressources dont elle a besoin pour établir un centre intégré d'expertise sur les cybercrimes. Cette équipe permettra d'accroître la capacité de la Gendarmerie de répondre, en appliquant une approche axée sur l'analyse du risque, aux demandes du Centre canadien de réponse aux incidents cybernétiques concernant des cyberattaques contre le gouvernement ou des infrastructures essentielles du Canada.

Le gouvernement a déjà adopté une loi pour combattre le vol d'identité. Il présentera de nouveau une série de projets de loi qui contribueront à accroître la capacité des organismes d'application de la loi de mener des enquêtes et des poursuites en cas de cybercrimes. Ces projets de loi visent entre autres à :

- ériger en infraction le fait d'utiliser un système informatique pour exploiter un enfant;
- obliger les fournisseurs de services Internet à doter leurs systèmes d'une capacité d'interception afin de permettre aux organismes d'application de la loi d'effectuer des interceptions autorisées par les tribunaux;
- obliger les fournisseurs de services Internet à fournir aux services de police des données de base sur l'identité des clients puisque cette information est essentielle pour combattre les crimes en ligne qui se déroulent en temps réel, comme la violence sexuelle à l'endroit d'enfants;
- élargir le type d'aide que le Canada peut fournir à ses partenaires signataires de traités pour combattre les crimes graves.

Protéger les Canadiens en ligne

Les familles canadiennes veulent que leur vie privée, identité et bien-être soient à l'abri des prédateurs en ligne. D'ailleurs, les Canadiens sont conscients des risques. Selon une étude récente de Decima Research[12] :

- Seulement 35 % des Canadiens estiment que leur ordinateur est très bien protégé contre les menaces en ligne.

[10] *SC Magazine*, « FTC Settles with TJX Over Breach », mars 2008
[11] *Wired Magazine*, « Feds Charge 11 in Breaches at TJ Maxx, OfficeMax, DSW, Others », août 2008
[12] Decima Research, *Cyber Security Practices in Canada*, Final Report, février 2008

- 77 % s'inquiètent de la sécurité de leurs renseignements personnels. Malgré tout, 63 % utilisent Internet pour effectuer des transactions à caractère confidentiel, et 57 % conservent des renseignements de nature délicate sur leur ordinateur.

Dans la mesure où ils savent quoi faire, les Canadiens et Canadiennes renforceront leur propre cybersécurité et celle de notre pays en général. Nous devons tous appliquer les pratiques de base en matière de cybersécurité, comme changer souvent nos mots de passe, mettre à jour les logiciels antivirus et utiliser uniquement des réseaux sans fil protégés.

Le gouvernement sensibilisera davantage la population canadienne aux crimes couramment commis en ligne et les informera des bonnes pratiques de cybersécurité en affichant des renseignements sur des sites Web, en produisant du matériel original et en menant des activités de liaison.

Le but du gouvernement est de créer une culture de cybersécurité, pour que les Canadiens soient informés des menaces et des mesures à prendre pour utiliser en toute sécurité le cyberespace. Or, pour favoriser cette culture, le gouvernement devra soutenir ses efforts pendant plusieurs années. C'est maintenant qu'il faut commencer.

Voie à suivre

Avec le temps, les Canadiens et Canadiennes dépendent de plus en plus du cyberespace. Il n'est pas question de faire marche arrière et de se passer d'Internet. Tout comme les générations passées qui ont profité des nouveaux modes de communication sans cesse plus utiles et complexes, nous avons adopté Internet.

Tout en tirant avantage du cyberespace, nous sommes conscients que la nouvelle technologie nous menace de différentes façons. Ceux qui ont décidé d'abuser d'Internet sont de plus en plus perfectionnés et dangereux. Nous devons investir dès aujourd'hui dans la cybersécurité pour protéger notre prospérité économique, notre sécurité nationale et notre qualité de vie.

La *Stratégie de cybersécurité du Canada* est le plan mis de l'avant par le Canada pour protéger nos cybersystèmes. La Stratégie permettra de protéger l'intégrité des systèmes gouvernementaux et des actifs essentiels de notre pays. Elle contribuera à combattre la cybercriminalité et à protéger les Canadiens et Canadiennes qui utilisent le cyberespace dans leur quotidien. En insistant sur l'importance de la cybersécurité, la Stratégie encourage les Canadiens et Canadiennes, l'industrie et les différents ordres de gouvernement à changer leur comportement et à mettre en place la technologie requise pour lutter contre les menaces qui ne cessent d'évoluer.

Le gouvernement commencera à mettre en œuvre de nouvelles initiatives de la Stratégie au cours de l'année 2010. Les initiatives mentionnées dans la Stratégie représentent une première étape importante. Elles seront modifiées et renforcées au besoin.

La cybersécurité est une responsabilité que nous partageons tous. Les Canadiens, les gouvernements, le secteur privé et les partenaires internationaux ont tous un rôle à jouer. La Stratégie traduit ce partage des responsabilités. Il faudra concerter nos efforts pour la mettre en application. Sa réussite dépendra de notre capacité de travailler ensemble.

Chacun a un rôle à jouer.